

This appendix contains some acronyms that do not actually appear in this manual. They have been included to present a comprehensive list that pertains to this series of publications.

## A

<b>AA&amp;E</b>	Arms, Ammunition, and Explosives
<b>AAR</b>	After Action Report
<b>ACL</b>	Access Control List
<b>ACP</b>	access control point
<b>ACS</b>	Access Control System
<b>ADA</b>	Americans with Disabilities Act
<b>ADAAG</b>	Americans with Disabilities Act Accessibility Guidelines
<b>AECS</b>	Automated Entry Control System
<b>AFJMAN</b>	Air Force Joint Manual, also may be known as AFMAN (I) for Air Force Manual
<b>AFMAN</b>	Air Force Manual
<b>ALERT</b>	Automated Local Evaluation in Real Time
<b>AMS</b>	Aerial Measuring System
<b>ANS</b>	Alert and Notification System
<b>ANSI</b>	American National Standards Institute
<b>ANSIR</b>	Awareness of National Security Issues and Response Program
<b>AOR</b>	Area of Responsibility

<b>AP</b>	armor piercing
<b>APHL</b>	Agency for Public Health Laboratories
<b>ARAC</b>	Atmospheric Release Advisory Capability
<b>ARC</b>	American Red Cross
<b>ARG</b>	Accident Response Group
<b>ARS</b>	Agriculture Research Service
<b>ASCE</b>	American Society of Civil Engineers
<b>ASHRAE</b>	American Society of Heating, Refrigerating, and Air-Conditioning Engineers
<b>ASTHO</b>	Association for State and Territorial Health Officials
<b>ASTM</b>	American Society for Testing and Materials
<b>ASZM-TEDA</b>	copper-silver-zinc-molybdenum-triethylenediamine
<b>AT</b>	Antiterrorism
<b>ATC</b>	Air Traffic Control
<b>ATF</b>	Bureau of Alcohol, Tobacco, and Firearms
<b>ATSD(CS)</b>	Assistant to the Secretary of Defense for Civil Support
<b>ATSDR</b>	Agency for Toxic Substances and Disease Registry
<b>AWG</b>	American wire gauge

## B

<b>BCA</b>	Benefit/Cost Analysis
<b>BCC</b>	Backup Control Center
<b>BCP</b>	Business Continuity Plan
<b>BDC</b>	Bomb Data Center

<b>BLASTOP</b>	Blast-Resistant Window Program
<b>BMS</b>	balanced magnetic switch
<b>BW</b>	biological warfare



<b>CAMEO</b>	Computer-Aided Management of Emergency Operations
<b>CB</b>	Citizens Band
<b>CBIAC</b>	Chemical and Biological Defense Information and Analysis Center
<b>CBR</b>	chemical, biological, or radiological
<b>CBRNE</b>	chemical, biological, radiological, nuclear, or explosive
<b>CCTV</b>	closed circuit television
<b>CDC</b>	Centers for Disease Control and Prevention
<b>CDR</b>	Call Detail Report
<b>CDRG</b>	Catastrophic Disaster Response Group
<b>CEO</b>	Chief Executive Officer
<b>CEPPO</b>	Chemical Emergency Preparedness and Prevention Office
<b>CERCLA</b>	Comprehensive Environmental Response, Compensation, and Liability Act
<b>CERT</b>	Community Emergency Response Team
<b>CFD</b>	Computational Fluid Dynamics
<b>CFO</b>	Chief Financial Officer
<b>CFR</b>	Code of Federal Regulations

<b>CHEMTREC</b>	Chemical Manufacturers' Association Chemical Transportation Emergency Center
<b>CHPPM</b>	Center for Health Promotion and Preventive Medicine
<b>CIAO</b>	Chief Infrastructure Assurance Office
<b>CIAO</b>	Critical Infrastructure Assurance Officer
<b>CICG</b>	Critical Infrastructure Coordination Group
<b>CIO</b>	Chief Information Officer
<b>CIP</b>	Critical Infrastructure Protection
<b>CIRG</b>	Crisis Incident Response Group
<b>CJCS</b>	Chairman of the Joint Chiefs of Staff
<b>CM</b>	Consequence Management
<b>CM</b>	Crisis Management
<b>CMS</b>	Call Management System
<b>CMU</b>	concrete masonry unit
<b>CMU</b>	Crisis Management Unit (CIRG)
<b>COB</b>	Continuity of Business
<b>COBIT™</b>	Control Objectives for Information Technology
<b>CO/DO</b>	Central Office/Direct Outdial
<b>CONEX</b>	Container Express
<b>CONOPS</b>	Concept of Operations
<b>COO</b>	Chief Operating Officer
<b>COOP</b>	Continuity of Operations Plan
<b>COR</b>	Class of Restriction
<b>COS</b>	Class of Service
<b>CPG</b>	Civil Preparedness Guide

<b>CPTED</b>	Crime Prevention Through Environmental Design
<b>CPX</b>	Command Post Exercise
<b>CRU</b>	Crisis Response Unit
<b>CSEPP</b>	Chemical Stockpile Emergency Preparedness Program
<b>CSI</b>	Construction Specifications Institute
<b>CSREES</b>	Cooperative State Research, Education, and Extension Service
<b>CST</b>	Civil Support Team
<b>CSTE</b>	Council of State and Territorial Epidemiologists
<b>CT</b>	Counterterrorism
<b>CW/CBD</b>	Chemical Warfare/Contraband Detection

## D

<b>DBMS</b>	Database Management System
<b>DBT</b>	Design Basis Threat
<b>DBU</b>	dial backup
<b>DD</b>	Data Dictionary
<b>DES</b>	Data Encryption Standard
<b>DEST</b>	Domestic Emergency Support Team
<b>DFO</b>	Disaster Field Office
<b>DHS</b>	Department of Homeland Security
<b>DISA</b>	Direct Inward System Access
<b>DMA</b>	Disaster Mitigation Act of 2000
<b>DMAT</b>	Disaster Medical Assistance Team

<b>DMCR</b>	Disaster Management Central Resource
<b>DMORT</b>	Disaster Mortuary Operational Response Team
<b>DOC</b>	Department of Commerce
<b>DoD</b>	Department of Defense
<b>DOE</b>	Department of Energy
<b>DOJ</b>	Department of Justice
<b>DOS</b>	Department of State
<b>DOT</b>	Department of Transportation
<b>DPP</b>	Domestic Preparedness Program
<b>DRC</b>	Disaster Recovery Center
<b>DTCTPS</b>	Domestic Terrorism/Counterterrorism Planning Section (FBI HQ)
<b>DTIC</b>	Defense Technical Information Center
<b>DTM</b>	data-transmission media
<b>DWI</b>	Disaster Welfare Information

## **E**

<b>EAS</b>	Emergency Alert System
<b>ECL</b>	Emergency Classification Level
<b>EECS</b>	Electronic Entry Control System
<b>EFR</b>	Emergency First Responder
<b>EM</b>	Emergency Management
<b>EMAC</b>	Emergency Medical Assistance Compact
<b>EMI</b>	Emergency Management Institute
<b>EMP</b>	electromagnetic pulse

<b>EMS</b>	Emergency Medical Services
<b>EOC</b>	Emergency Operations Center
<b>EOD</b>	Explosive Ordnance Disposal
<b>EOP</b>	Emergency Operating Plan
<b>EOP</b>	Emergency Operations Plan
<b>EPA</b>	Environmental Protection Agency
<b>EPCRA</b>	Emergency Planning and Community Right-to-Know Act
<b>EPG</b>	Emergency Planning Guide
<b>EPI</b>	Emergency Public Information
<b>EP&amp;R</b>	Directorate of Emergency Preparedness and Response (DHS)
<b>EPZ</b>	Emergency Planning Zone
<b>ERP</b>	Emergency Response Plan
<b>ERT</b>	Emergency Response Team
<b>ERT-A</b>	Emergency Response Team Advance Element
<b>ERT-N</b>	Emergency Response Team National
<b>ERTU</b>	Evidence Response Team Unit
<b>ESC</b>	Expandable Shelter Container
<b>ESF</b>	Emergency Support Function
<b>ESS</b>	Electronic Security System
<b>EST</b>	Emergency Support Team
<b>ETL</b>	Engineering Technical Letter
<b>EU</b>	explosives unit

# F

<b>FAST</b>	Field Assessment Team
<b>FBI</b>	Federal Bureau of Investigation
<b>FCC</b>	Federal Communications Commission
<b>FCC</b>	Fire Control Center
<b>FCO</b>	Federal Coordinating Officer
<b>FEM</b>	finite element
<b>FEMA</b>	Federal Emergency Management Agency
<b>FEST</b>	Foreign Emergency Support Team
<b>FHBM</b>	Flood Hazard Boundary Map
<b>FIA</b>	Federal Insurance Administration
<b>FIPS</b>	Federal Information Processing Standard
<b>FIRM</b>	Flood Insurance Rate Map
<b>FIS</b>	Flood Insurance Study
<b>FISCAM</b>	Federal Information Systems Control Audit Manual
<b>FMFIA</b>	Federal Manager's Financial Integrity Act
<b>FNS</b>	Food and Nutrition Service
<b>FOIA</b>	Freedom of Information Act
<b>FOUO</b>	For Official Use Only
<b>FPEIS</b>	Final Programmatic Environmental Impact Statement
<b>FRERP</b>	Federal Radiological Emergency Response Plan
<b>FRF</b>	fragment retention film
<b>FRL</b>	Facility Restriction Level



<b>FRMAC</b>	Federal Radiological Monitoring and Assessment Center
<b>FRP</b>	Federal Response Plan
<b>FS</b>	Forest Service
<b>FSTFS</b>	Frame-Supported Tensioned Fabric Structure
<b>FTP</b>	File Transfer Protocol
<b>FTX</b>	Functional Training Exercise

## G

<b>GAO</b>	General Accounting Office
<b>GAR</b>	Governor's Authorized Representative
<b>GC/MS</b>	gas chromatograph/mass spectrometer
<b>GIS</b>	Geographic Information System
<b>GP</b>	General Purpose
<b>GPS</b>	Global Positioning System
<b>GSA</b>	General Services Administration

## H

<b>HazMat</b>	hazardous material
<b>HAZUS</b>	Hazards U.S.
<b>HEPA</b>	high efficiency particulate air
<b>HEU</b>	highly enriched uranium
<b>HF</b>	high frequency
<b>HHS</b>	Department of Health and Human Services

<b>HIRA</b>	Hazard Identification and Risk Assessment
<b>HMRU</b>	Hazardous Materials Response Unit
<b>HQ</b>	Headquarters
<b>HRCQ</b>	Highway Route Controlled Quantity
<b>HRT</b>	Hostage Rescue Team (CIRG)
<b>HTIS</b>	Hazardous Technical Information Services (DoD)
<b>HVAC</b>	heating, ventilation, and air conditioning



<b>IC</b>	Incident Commander
<b>ICDDC</b>	Interstate Civil Defense and Disaster Compact
<b>ICP</b>	Incident Command Post
<b>ICS</b>	Incident Command System
<b>ID</b>	identification
<b>IDS</b>	Intrusion Detection System
<b>IED</b>	Improvised Explosive Device
<b>IEMS</b>	Integrated Emergency Management System
<b>IESNA</b>	Illuminating Engineering Society of North America
<b>IID</b>	Improvised Incendiary Device
<b>IMS</b>	ion mobility spectrometry
<b>IND</b>	Improvised Nuclear Device
<b>IPL</b>	Initial Program Load
<b>IR</b>	infrared
<b>IRZ</b>	Immediate Response Zone

<b>IS</b>	Information System
<b>ISACF</b>	Information Systems Audit and Control Foundation
<b>ISC</b>	Interagency Security Committee
<b>ISO</b>	International Organization for Standardization
<b>ISP</b>	Internet Service Provider
<b>IT</b>	Information Technology

## J

<b>JIC</b>	Joint Information Center
<b>JIISE</b>	Joint Interagency Intelligence Support Element
<b>JIS</b>	Joint Information System
<b>JNACC</b>	Joint Nuclear Accident Coordinating Center
<b>JOC</b>	Joint Operations Center
<b>JSMG</b>	Joint Service Materiel Group
<b>JTF-CS</b>	Joint Task Force for Civil Support
<b>JTTF</b>	Joint Terrorism Task Force
<b>JTWG</b>	Joint Terrorism Working Group

## K

<b>kHz</b>	kilohertz
<b>kPa</b>	kilo Pascal

## L

<b>LAN</b>	Local Area Network
<b>LAW</b>	Light Antitank Weapon
<b>LBNL</b>	Lawrence Berkley National Lab
<b>LCM</b>	Life-cycle Management
<b>LED</b>	light-emitting diode
<b>LEED</b>	Leadership in Energy and Environmental Design
<b>LEPC</b>	Local Emergency Planning Committee
<b>LF</b>	low frequency
<b>LFA</b>	Lead Federal Agency
<b>LLNL</b>	Lawrence Livermore National Laboratory
<b>LOP</b>	level of protection
<b>LOS</b>	line of sight
<b>LPHA</b>	Local Public Health Agency
<b>LPHS</b>	Local Public Health System


## M

<b>MAC</b>	Moves, Adds, Changes
<b>MEDCOM</b>	Medical Command
<b>MEI</b>	Minimum Essential Infrastructure
<b>M/E/P</b>	Mechanical/Electrical/Plumbing
<b>MEP</b>	Mission Essential Process
<b>MERV</b>	minimum efficiency reporting value
<b>MMRS</b>	Metropolitan Medical Response System

<b>MOU/A</b>	Memorandum of Understanding/Agreement
<b>mph</b>	miles per hour
<b>MPOP</b>	Minimum-Points-of-Presence
<b>ms</b>	millisecond
<b>MSCA</b>	Military Support to Civil Authorities
<b>MSDS</b>	Material Safety Data Sheet
<b>MSS</b>	Medium Shelter System
<b>MW</b>	medium wave

## N

<b>NACCHO</b>	National Association for County and City Health Officials
<b>NAP</b>	Nuclear Assessment Program
<b>NAVFAC</b>	Naval Facilities Command
<b>NBC</b>	nuclear, biological, and chemical
<b>NCJ</b>	National Criminal Justice
<b>NCP</b>	National Contingency Plan (also known as National Oil and Hazardous Substances Pollution Contingency Plan)
<b>NDA</b>	National Defense Area
<b>NDMS</b>	National Disaster Medical System
<b>NDPO</b>	National Domestic Preparedness Office
<b>NEST</b>	Nuclear Emergency Search Team
<b>NETC</b>	National Emergency Training Center
<b>NFA</b>	National Fire Academy
<b>NFIP</b>	National Flood Insurance Program

<b>NFPA</b>	National Fire Protection Association
<b>NFPC</b>	National Fire Protection Code
<b>NIJ</b>	National Institute of Justice
<b>NIOSH</b>	National Institute for Occupational Safety and Health
<b>NMRT</b>	National Medical Response Team
<b>NMS</b>	Network Management System
<b>NOAA</b>	National Oceanic and Atmospheric Administration
<b>NRC</b>	National Response Center
<b>NRC</b>	Nuclear Regulatory Commission
<b>NRT</b>	National Response Team
<b>NSC</b>	National Security Council
<b>NTIS</b>	National Technical Information Service
<b>NUREG</b>	Nuclear Regulation
<b>NWS</b>	National Weather Service
	
<b>OCC</b>	Operational Control Center
<b>ODP</b>	Office of Disaster Preparedness
<b>OEP</b>	Office of Emergency Preparedness
<b>OES</b>	Office of Emergency Services
<b>OFCM</b>	Office of the Federal Coordinator for Meteorology
<b>OHS</b>	Office of Homeland Security
<b>OJP</b>	Office of Justice Programs

<b>O&amp;M</b>	operations and maintenance
<b>OMB</b>	Office of Management and Budget
<b>OPA</b>	Oil Pollution Act
<b>OSC</b>	On-scene Coordinator
<b>OSD</b>	Office of Secretary of Defense
<b>OSHA</b>	Occupational Safety and Health Administration
<b>OSLDPS</b>	Office for State and Local Domestic Preparedness Support

## P

<b>Pa</b>	Pascal
<b>PA</b>	public address
<b>PAZ</b>	Protective Action Zone
<b>PBX</b>	Public Branch Exchange
<b>PC</b>	personal computer
<b>PCC</b>	Policy Coordinating Committee
<b>PCCIP</b>	President's Commission on Critical Infrastructure Protection
<b>PCM</b>	Procedures Control Manual
<b>PDA</b>	personal data assistant
<b>PDA</b>	Preliminary Damage Assessment
<b>PDD</b>	Presidential Decision Directive
<b>PHS</b>	Public Health Service
<b>PIN</b>	Personal Identification Number
<b>PIO</b>	Public Information Officer

<b>PL</b>	Public Law
<b>POC</b>	Point of Contact
<b>POD</b>	probability of detection
<b>POI</b>	probability of intrusion
<b>POL</b>	Petroleum, Oils, and Lubricants
<b>POV</b>	privately owned vehicle
<b>PPA</b>	Performance Partnership Agreement
<b>ppm</b>	parts per million
<b>PSE</b>	particle size efficiency
<b>psi</b>	pounds per square inch
<b>PT</b>	Preparedness, Training, and Exercises Directorate (FEMA)
<b>PTE</b>	Potential Threat Element
<b>PTZ</b>	pan-tilt-zoom (camera)
<b>PVB</b>	polyvinyl butyral
<b>PZ</b>	Precautionary Zone

## R

<b>RACES</b>	Radio Amateur Civil Emergency Service
<b>RAP</b>	Radiological Assistance Program
<b>RCRA</b>	Research Conservation and Recovery Act
<b>RDD</b>	Radiological Dispersal Device
<b>RDT&amp;E</b>	Research, Development, Test, and Evaluation
<b>REACT</b>	Radio Emergency Associated Communications Team



<b>REAC/TS</b>	Radiation Emergency Assistance Center/Training Site
<b>REM</b>	Roentgen Man Equivalent
<b>REP</b>	Radiological Emergency Preparedness Program
<b>RF</b>	radio frequency
<b>ROC</b>	Regional Operations Center
<b>ROD</b>	Record of Decision
<b>RPG</b>	Rocket Propelled Grenade
<b>RRIS</b>	Rapid Response Information System (FEMA)
<b>RRP</b>	Regional Response Plan
<b>RRT</b>	Regional Response Team

## S

<b>SAA</b>	State Administrative Agency
<b>SAC</b>	Special Agent in Charge (FBI)
<b>SAFEVU</b>	Safety Viewport Analysis Code
<b>SAME</b>	Specific Area Message Encoder
<b>SARA</b>	Superfund Amendments and Reauthorization Act
<b>SATCOM</b>	satellite communications
<b>SAW</b>	surface acoustic wave
<b>SBCCOM</b>	Soldier and Biological Chemical Command (U.S. Army)
<b>SCADA</b>	Supervisory, Control, and Data Acquisition
<b>SCBA</b>	Self-Contained Breathing Apparatus
<b>SCC</b>	Security Control Center

<b>SCO</b>	State Coordinating Officer
<b>SDOF</b>	single-degree-of-freedom
<b>SEA</b>	Southeast Asia
<b>SEB</b>	State Emergency Board
<b>SEL</b>	Standardized Equipment List
<b>SEMA</b>	State Emergency Management Agency
<b>SERC</b>	State Emergency Response Commission
<b>SFO</b>	Senior FEMA Official
<b>SIOC</b>	Strategic Information and Operations Center (FBI HQ)
<b>SLA</b>	Service Level Agreement
<b>SLG</b>	State and Local Guide
<b>SNM</b>	Special Nuclear Material
<b>SOP</b>	Standard Operating Procedure
<b>SPCA</b>	Society for the Prevention of Cruelty to Animals
<b>SPSA</b>	Super Power Small Arms
<b>SSS</b>	Small Shelter System
<b>STC</b>	Sound Transmission Class
<b>SWAT</b>	Special Weapons and Tactics

## T

<b>TAC</b>	Trunk Access Codes
<b>TDR</b>	transferable development right
<b>TEA</b>	Threat Environment Assessment
<b>TEMPER</b>	Tent, Extendable, Modular, Personnel

<b>TERC</b>	Tribal Emergency Response Commission
<b>TIA</b>	Terrorist Incident Appendix
<b>TIM</b>	toxic industrial material
<b>TM</b>	Technical Manual
<b>TNT</b>	trinitrotoluene
<b>TRIS</b>	Toxic Release Inventory System
<b>TSC</b>	triple-standard concertina
<b>TSO</b>	Time Share Option
<b>TTG</b>	thermally tempered glass

## U

<b>UC</b>	Unified Command
<b>UCS</b>	Unified Command System
<b>UFAS</b>	Uniform Federal Accessibility Standards
<b>UFC</b>	Unified Facilities Criteria
<b>UL</b>	Underwriters Laboratories
<b>ULPA</b>	ultra low penetration air
<b>UPS</b>	uninterrupted power supply
<b>URV</b>	UVGI Rating Values
<b>U.S.</b>	United States
<b>USA</b>	United States Army
<b>USAF</b>	United States Air Force
<b>USC</b>	U.S. Code
<b>USDA</b>	U.S. Department of Agriculture
<b>USFA</b>	U.S. Fire Administration

<b>USGBC</b>	U.S. Green Building Council
<b>USGS</b>	U.S. Geological Survey
<b>US&amp;R</b>	Urban Search and Rescue
<b>UV</b>	ultraviolet
<b>UVGI</b>	ultraviolet germicidal irradiation

## V

<b>VA</b>	Department of Veterans Affairs
<b>VAP</b>	Vulnerability Assessment Plan
<b>VAV</b>	Variable Air Volume
<b>VDN</b>	Vector Directory Number
<b>VHF</b>	very high frequency
<b>VRU</b>	Voice Response Unit

## W

<b>WAN</b>	Wide Area Network
<b>wg</b>	water gauge
<b>WINGARD</b>	Window Glazing Analysis Response and Design
<b>WINLAC</b>	Window Lite Analysis Code
<b>WMD</b>	Weapons of Mass Destruction
<b>WMD-CST</b>	WMD Civil Support Team

This appendix contains some terms that do not actually appear in this manual. They have been included to present a comprehensive list that pertains to this series of publications.

## A

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

**Access control point (ACP).** A station at an entrance to a building or a portion of a building where identification is checked and people and hand-carried items are searched.

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

**Access Control System (ACS).** Also referred to as an Electronic Entry Control Systems; an electronic system that controls entry and egress from a building or area.

**Access Control System elements.** Detection measures used to control vehicle or personnel entry into a protected area. Access Control System elements include locks, Electronic Entry Control Systems, and guards.

**Access group.** A software configuration of an Access Control System that groups together access points or authorized users for easier arrangement and maintenance of the system.

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

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

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

**Active vehicle barrier.** An impediment placed at an access control point that may be manually or automatically deployed in response to detection of a threat.

**Aerosol.** Fine liquid or solid particles suspended in a gas (e.g., fog or smoke).

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

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

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

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

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

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

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

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

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

**Area lighting.** Lighting that illuminates a large exterior area.

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

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

**Assessment System elements.** Detection measures used to assist guards in visual verification of Intrusion Detection System Alarms and Access Control System functions and to assist in visual detection by guards. Assessment System elements include closed circuit television and protective lighting.

**Asset.** A resource of value requiring protection. An asset can be tangible (e.g., people, buildings, facilities, equipment, activities, operations, and information) or intangible (e.g., processes or a company's information and reputation).

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

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

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

**Audible alarm device.** An alarm device that produces an audible announcement (e.g., bell, horn, siren, etc.) of an alarm condition.

## B

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

**Ballistics attack.** An attack in which small arms (e.g., pistols, submachine guns, shotguns, and rifles) are fired from a distance and rely on the flight of the projectile to damage the target.

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

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

**Barcode.** A black bar printed on white paper or tape that can be easily read with an optical scanner.

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

**Biometric reader.** A device that gathers and analyzes biometric features.

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

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

**Blast-resistant glazing.** Window opening glazing that is resistant to blast effects because of the interrelated function of the frame and



glazing material properties frequently dependent upon tempered glass, polycarbonate, or laminated glazing.

**Blast vulnerability envelope.** The geographical area in which an explosive device will cause damage to assets.

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

**Boundary penetration sensor.** An interior intrusion detection sensor that detects attempts by individuals to penetrate or enter a building.

**Building hardening.** Enhanced construction that reduces vulnerability to external blast and ballistic attacks.

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

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



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

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

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

**Chemical agent.** A chemical substance that is intended to kill, seriously injure, or incapacitate people through physiological effects. Generally separated by severity of effect (e.g., lethal, blister, and incapacitating).

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

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

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

**CCTV pan-tilt-zoom camera (PTZ).** A CCTV camera that can move side to side, up and down, and zoom in or out.

**CCTV pan-tilt-zoom control.** The method of controlling the PTZ functions of a camera.

**CCTV pan-tilt-zoom controller.** The operator interface for performing PTZ control.

**CCTV switcher.** A piece of equipment capable of presenting multiple video images to various monitors, recorders, etc.

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

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

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

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

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

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

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

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

**Control center.** A centrally located room or facility staffed by personnel charged with the oversight of specific situations and/or equipment.

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

**Controlled lighting.** Illumination of specific areas or sections.

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

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

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

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

**Counterterrorism (CT).** Offensive measures taken to prevent, deter, and respond to terrorism.

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

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

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

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

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

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

## D

**Damage assessment.** The process used to appraise or determine the number of injuries and deaths, damage to public and private property, and the status of key facilities and services (e.g., hospitals and other health care facilities, fire and police stations, communications networks, water and sanitation systems, utilities, and transportation networks) resulting from a manmade or natural disaster.

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

**Data transmission equipment.** A path for transmitting data between two or more components (e.g., a sensor and alarm reporting system, a card reader and controller, a CCTV camera and monitor, or a transmitter and receiver).

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

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

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

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

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

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

**Design opportunity.** Anything that enhances protection, reduces requirements for protective measures, or solves a design problem.

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

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

**Detection measures.** Protective measures that detect intruders, weapons, or explosives; assist in assessing the validity of detection; control access to protected areas; and communicate the appropriate information to the response force. Detection measures include Detection Systems, Assessment Systems, and Access Control System elements.

**Detection System elements.** Detection measures that detect the presence of intruders, weapons, or explosives. Detection System elements include Intrusion Detection Systems, weapons and explosives detectors, and guards.

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

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

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

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

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

**Door strike, electronic.** An electromechanical lock that releases a door plunger to unlock the door. Typically, an electronic door strike is mounted in place of or near a normal door strike plate.

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

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

**Dual technology sensor.** A sensor that combines two different technologies in one unit.

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

# E

**Effective stand-off distance.** A stand-off distance at which the required level of protection can be shown to be achieved through analysis or can be achieved through building hardening or other mitigating construction or retrofit.

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

**Electronic emanations.** Electromagnetic emissions from computers, communications, electronics, wiring, and related equipment.

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

**Electronic Entry Control Systems (EECS).** Electronic devices that automatically verify authorization for a person to enter or exit a controlled area.

**Electronic Security System (ESS).** An integrated system that encompasses interior and exterior sensors, closed circuit television systems for assessment of alarm conditions, Electronic Entry Control Systems, data transmission media, and alarm reporting systems for monitoring, control, and display of various alarm and system information.

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

**Emergency Alert System (EAS).** A communications system of broadcast stations and interconnecting facilities authorized by the Federal Communications Commission (FCC). The system provides the President and other national, state, and local



officials the means to broadcast emergency information to the public before, during, and after disasters.

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

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

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

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

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

**Emergency Planning Zones (EPZ).** Areas around a facility for which planning is needed to ensure prompt and effective actions are taken to protect the health and safety of the public

if an accident or disaster occurs. In the Radiological Emergency Preparedness Program, the two EPZs are:

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

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

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

**Immediate Response Zone (IRZ).** A circular zone ranging from 10 to 15 kilometers (6 to 9 miles) from the potential chemical event source, depending on the stockpile location on-post. Emergency response plans developed for the IRZ must provide for the most rapid and effective protective actions possible, because the IRZ will have the highest concentration of agent and the least amount of warning time.

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

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

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

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

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

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

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

or because of the specialized or unique nature of the assistance required. ESF missions are designed to supplement state and local response efforts.

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

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

**Entry control point.** A continuously or intermittently manned station at which entry to sensitive or restricted areas is controlled.

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

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

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

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

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

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

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

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

**Exclusion zone.** An area around an asset that has controlled entry with highly restrictive access. See controlled area.

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

## F

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

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

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

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

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

**Fence sensor.** An exterior intrusion detection sensor that detects aggressors as they attempt to climb over, cut through, or otherwise disturb a fence.

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

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

**Field of view.** The visible area in a video picture.

**First responder.** Local police, fire, and emergency medical personnel who first arrive on the scene of an incident and take action to save lives, protect property, and meet basic human needs.

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

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

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

**Fragment retention film (FRF).** A thin, optically clear film applied to glass to minimize the spread of glass fragments when the glass is shattered.

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

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



**Glare security lighting.** Illumination projected from a secure perimeter into the surrounding area, making it possible to see potential intruders at a considerable distance while making it difficult to observe activities within the secure perimeter.

**Glass-break detector.** An intrusion detection sensor that is designed to detect breaking glass either through vibration or acoustics.

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

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

**Grid wire sensor.** An intrusion detection sensor that uses a grid of wires to cover a wall or fence. An alarm is sounded if the wires are cut.



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

**Hazard.** A source of potential danger or adverse condition.

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

**Hazardous material (HazMat).** Any substance or material that, when involved in an accident and released in sufficient quantities, poses a risk to people's health, safety, and/or property. These substances and materials include explosives, radioactive materials,


flammable liquids or solids, combustible liquids or solids, poisons, oxidizers, toxins, and corrosive materials.

**High-hazard areas.** Geographic locations that, for planning purposes, have been determined through historical experience and vulnerability analysis to be likely to experience the effects of a specific hazard (e.g., hurricane, earthquake, hazardous materials accident, etc.), resulting in vast property damage and loss of life.

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

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

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



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

**Incident Command System (ICS).** A standardized organizational structure used to command, control, and coordinate the use of resources and personnel that have responded to the scene of an emergency. The concepts and principles for ICS include common



terminology, modular organization, integrated communication, unified command structure, consolidated action plan, manageable span of control, designated incident facilities, and comprehensive resource management.

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

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

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

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

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

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

**Intrusion Detection Sensor.** A device that initiates alarm signals by sensing the stimulus, change, or condition for which it was designed.

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

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

## J

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

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

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

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

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

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



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

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

**Laser card.** A card technology that uses a laser reflected off of a card for uniquely identifying the card.

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

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

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

**Level of protection (LOP).** The degree to which an asset is protected against injury or damage from an attack.

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

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

**Line of sight (LOS).** Direct observation between two points with the naked eye or hand-held optics.

**Line-of-sight sensor.** A pair of devices used as an intrusion detection sensor that monitor any movement through the field between the sensors.

**Line supervision.** A data integrity strategy that monitors the communications link for connectivity and tampering. In Intrusion Detection System sensors, line supervision is often referred to as two-state, three-state, or four-state in respect to the number of conditions monitored. The frequency of sampling the link also plays a big part in the supervision of the line.

**Local government.** Any county, city, village, town, district, or political subdivision of any state, and Indian tribe or authorized tribal organization, or Alaska Native village or organization, including any rural community or unincorporated town or village or any other public entity.

## M

**Magnetic lock.** An electromagnetic lock that unlocks a door when power is removed.

**Magnetic stripe.** A card technology that uses a magnetic stripe on the card to encode data used for unique identification of the card.

**Mail-bomb delivery.** Bombs or incendiary devices delivered to the target in letters or packages.

**Man-trap.** An access control strategy that uses a pair of interlocking doors to prevent tailgating. Only one door can be unlocked at a time.

**Mass care.** The actions that are taken to protect evacuees and other disaster victims from the effects of the disaster. Activities include providing temporary shelter, food, medical care, clothing, and other essential life support needs to those people who have been displaced from their homes because of a disaster or threatened disaster.

**Mass notification.** Capability to provide real-time information to all building occupants or personnel in the immediate vicinity of a building during emergency situations.

**Microwave motion sensor.** An intrusion detection sensor that uses microwave energy to sense movement within the sensor's field of view. These sensors work similar to radar by using the Doppler effect to measure a shift in frequency.

**Military installations.** Army, Navy, Air Force, and Marine Corps bases, posts, stations, and annexes (both contractor and government operated), hospitals, terminals, and other special mission facilities, as well as those used primarily for military purposes.

**Minimum essential infrastructure resource elements.** The broad categories of resources, all or portions of which constitute the minimal essential infrastructure necessary for a department, agency, or organization to conduct its core mission(s).

**Minimum measures.** Protective measures that can be applied to all buildings regardless of the identified threat. These measures offer defense or detection opportunities for minimal cost, facilitate future upgrades, and may deter acts of aggression.

**Mitigation.** Those actions taken to reduce the exposure to and impact of an attack or disaster.

**Motion detector.** An intrusion detection sensor that changes state based on movement in the sensor's field of view.

**Moving vehicle bomb.** An explosive-laden car or truck driven into or near a building and detonated.

**Mutual Aid Agreement.** A pre-arranged agreement developed between two or more entities to render assistance to the parties of the agreement.

## N

**Natural hazard.** Naturally-occurring events such as floods, earthquakes, tornadoes, tsunamis, coastal storms, landslides, and wildfires that strike populated areas. A natural event is a hazard when it has the potential to harm people or property (FEMA 386-2, *Understanding Your Risks*). The risks of natural hazards may be increased or decreased as a result of human activity; however, they are not inherently human-induced.

**Natural protective barriers.** Natural protective barriers are mountains and deserts, cliffs and ditches, water obstacles, or other terrain features that are difficult to traverse.

**Non-exclusive zone.** An area around an asset that has controlled entry, but shared or less restrictive access than an exclusive zone.

**Non-persistent agent.** An agent that, upon release, loses its ability to cause casualties after 10 to 15 minutes. It has a high evaporation rate, is lighter than air, and will disperse rapidly. It is considered to be a short-term hazard; however, in small, unventilated areas, the agent will be more persistent.

**Nuclear, biological, or chemical weapons.** Also called Weapons of Mass Destruction (WMD). Weapons that are characterized by their capability to produce mass casualties.

**Nuclear detonation.** An explosion resulting from fission and/or fusion reactions in nuclear material, such as that from a nuclear weapon.



**On-Scene Coordinator (OSC).** The federal official pre-designated by the EPA and U.S. Coast Guard to coordinate and direct response and removals under the National Oil and Hazardous Substances Pollution Contingency Plan.

**Open systems architecture.** A term borrowed from the IT industry to claim that systems are capable of interfacing with other systems from any vendor, which also uses open system architecture. The opposite would be a proprietary system.

**Operator interface.** The part of a security management system that provides that user interface to humans.

**Organizational areas of control.** Controls consist of the policies, procedures, practices, and organization structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.

## P

**Passive infrared motion sensor.** A device that detects a change in the thermal energy pattern caused by a moving intruder and initiates an alarm when the change in energy satisfies the detector's alarm-criteria.

**Passive vehicle barrier.** A vehicle barrier that is permanently deployed and does not require response to be effective.

**Patch panel.** A concentrated termination point that separates backbone cabling from devices cabling for easy maintenance and troubleshooting.

**Perimeter barrier.** A fence, wall, vehicle barrier, landform, or line of vegetation applied along an exterior perimeter used to obscure vision, hinder personnel access, or hinder or prevent vehicle access.

**Persistent agent.** An agent that, upon release, retains its casualty-producing effects for an extended period of time, usually anywhere from 30 minutes to several days. A persistent agent usually has a low evaporation rate and its vapor is heavier than air; therefore, its vapor cloud tends to hug the ground. It is considered to be a long-term hazard. Although inhalation hazards are still a concern, extreme caution should be taken to avoid skin contact as well.

**Physical security.** The part of security concerned with measures/concepts designed to safeguard personnel; to prevent unauthorized access to equipment, installations, materiel, and documents; and to safeguard them against espionage, sabotage, damage, and theft.

**Planter barrier.** A passive vehicle barrier, usually constructed of concrete and filled with dirt (and flowers for aesthetics). Planters, along with bollards, are the usual street furniture used to keep vehicles away from existing buildings. Overall size and the depth of installation below grade determine the vehicle stopping capability of the individual planter.

**Plume.** Airborne material spreading from a particular source; the dispersal of particles, gases, vapors, and aerosols into the atmosphere.

**Polycarbonate glazing.** A plastic glazing material with enhanced resistance to ballistics or blast effects.

**Predetonation screen.** A fence that causes an anti-tank round to detonate or prevents it from arming before it reaches its target.

**Preliminary Damage Assessment (PDA).** A mechanism used to determine the impact and magnitude of damage and the resulting unmet needs of individuals, businesses, the public sector, and the community as a whole. Information collected is used by the state as a basis for the Governor's request for a Presidential declaration, and by FEMA to document the recommendation made to the President in response to the Governor's request. PDAs are made by at least one state and one federal representative. A local government representative familiar with the extent and location of damage in the community



often participates; other state and federal agencies and voluntary relief organizations also may be asked to participate, as needed.

**Preparedness.** Establishing the plans, training, exercises, and resources necessary to enhance mitigation of and achieve readiness for response to, and recovery from all hazards, disasters, and emergencies, including WMD incidents.

**Pressure mat.** A mat that generates an alarm when pressure is applied to any part of the mat's surface, such as when someone steps on the mat. Pressure mats can be used to detect an intruder approaching a protected object, or they can be placed by doors and windows to detect entry.

**Primary asset.** An asset that is the ultimate target for compromise by an aggressor.

**Primary gathering building.** Inhabited buildings routinely occupied by 50 or more personnel. This designation applies to the entire portion of a building that meets the population density requirements for an inhabited building.

**Probability of detection (POD).** A measure of an intrusion detection sensor's performance in detecting an intruder within its detection zone.

**Probability of intercept.** The probability that an act of aggression will be detected and that a response force will intercept the aggressor before the asset can be compromised.

**Progressive collapse.** A chain reaction failure of building members to an extent disproportionate to the original localized damage. Such damage may result in upper floors of a building collapsing onto lower floors.

**Protective barriers.** Define the physical limits of a site, activity, or area by restricting, channeling, or impeding access and forming a continuous obstacle around the object.

**Protective measures.** Elements of a protective system that protect an asset against a threat. Protective measures are divided into defensive and detection measures.

**Protective system.** An integration of all of the protective measures required to protect an asset against the range of threats applicable to the asset.

**Proximity sensor.** An intrusion detection sensor that changes state based on the close distance or contact of a human to the sensor. These sensors often measure the change in capacitance as a human body enters the measured field.

**Public Information Officer (PIO).** A federal, state, or local government official responsible for preparing and coordinating the dissemination of emergency public information.

## R

**Radiation.** High-energy particles or gamma rays that are emitted by an atom as the substance undergoes radioactive decay. Particles can be either charged alpha or beta particles or neutral neutron or gamma rays.

**Radiation sickness.** The symptoms characterizing the sickness known as radiation injury, resulting from excessive exposure of the whole body to ionizing radiation.

**Radiological monitoring.** The process of locating and measuring radiation by means of survey instruments that can detect and measure (as exposure rates) ionizing radiation.

**Recovery.** The long-term activities beyond the initial crisis period and emergency response phase of disaster operations that focus on returning all systems in the community to a normal status or to reconstitute these systems to a new condition that is less vulnerable.

**Regional Operations Center (ROC).** The temporary operations facility for the coordination of federal response and recovery activities located at the FEMA Regional Office (or Federal

Regional Center) and led by the FEMA Regional Director or Deputy Director until the DFO becomes operational. After the ERT-A is deployed, the ROC performs a support role for federal staff at the disaster scene.

**Report printers.** A separate, dedicated printer attached to the Electronic Security Systems used for generating reports utilizing information stored by the central computer.

**Request-to-exit device.** Passive infrared motion sensors or push buttons that are used to signal an Electronic Entry Control System that egress is imminent or to unlock a door.

**Resolution.** The level to which video details can be determined in a CCTV scene is referred to as resolving ability or resolution.

**Resource Management.** Those actions taken by a government to: identify sources and obtain resources needed to support disaster response activities; coordinate the supply, allocation, distribution, and delivery of resources so that they arrive where and when most needed; and maintain accountability for the resources used.

**Response.** Executing the plan and resources identified to perform those duties and services to preserve and protect life and property as well as provide services to the surviving population.

**Response force.** The people who respond to an act of aggression. Depending on the nature of the threat, the response force could consist of guards, special reaction teams, military or civilian police, an explosives ordnance disposal team, or a fire department.

**Response time.** The length of time from the instant an attack is detected to the instant a security force arrives on site.

**Restricted area.** Any area with access controls that is subject to these special restrictions or controls for security reasons. See controlled area, limited area, exclusion area, and exclusion zone.

**Retinal pattern.** A biometric technology that is based on features of the human eye.

**RF data transmission.** A communications link using radio frequency to send or receive data.

**Risk.** The potential for loss of, or damage to, an asset. It is measured based upon the value of the asset in relation to the threats and vulnerabilities associated with it.

**Rotating drum or rotating plate vehicle barrier.** An active vehicle barrier used at vehicle entrances to controlled areas based on a drum or plate rotating into the path of the vehicle when signaled.

**Routinely occupied.** For the purposes of these standards, an established or predictable pattern of activity within a building that terrorists could recognize and exploit.

**RS-232 data.** IEEE Recommended Standard 232; a point-to-point serial data protocol with a maximum effective distance of 50 feet.

**RS-422 data.** IEEE Recommended Standard 422; a point-to-point serial data protocol with a maximum effective distance of 4,000 feet.

**RS-485 data.** IEEE Recommended Standard 485; a multi-drop serial data protocol with a maximum effective distance of 4,000 feet.

## S

**Sacrificial roof or wall.** Roofs or walls that can be lost in a blast without damage to the primary asset.

**Safe haven.** Secure areas within the interior of the facility. A safe haven should be designed such that it requires more time to penetrate by aggressors than it takes for the response force to reach the protected area to rescue the occupants. It may be a haven from a physical attack or air-isolated haven from CBR contamination.

**Scramble keypad.** A keypad that uses keys on which the numbers change pattern with each use to enhance security by preventing eavesdropping observation of the entered numbers.

**Secondary asset.** An asset that supports a primary asset and whose compromise would indirectly affect the operation of the primary asset.

**Secondary hazard.** A threat whose potential would be realized as the result of a triggering event that of itself would constitute an emergency (e.g., dam failure might be a secondary hazard associated with earthquakes).

**Secure/access mode.** The state of an area monitored by an intrusion detection system in regards to how alarm conditions are reported.

**Security analysis.** The method of studying the nature of and the relationship between assets, threats, and vulnerabilities.

**Security console.** Specialized furniture, racking, and related apparatus used to house the security equipment required in a control center.

**Security engineering.** The process of identifying practical, risk managed short- and long-term solutions to reduce and/or mitigate dynamic manmade hazards by integrating multiple factors, including construction, equipment, manpower, and procedures.

**Security engineering design process.** The process through which assets requiring protection are identified, the threat to and vulnerability of those assets is determined, and a protective system is designed to protect the assets.

**Security Management System database.** In a Security Management System, a database that is transferred to various nodes or panels throughout the system for faster data processing and protection against communications link downtime.

**Security Management System distributed processing.** In a Security Management System, a method of data processing at various

nodes or panels throughout the system for faster data processing and protection against communications links downtime.

**Segregation of duties.** Policies, procedures, and an organizational structure established so that one individual cannot control key aspects of physical and/or computer-related operations and thereby conduct unauthorized actions or gain unauthorized access to minimum essential infrastructure resource elements.

**Semi-isolated fenced perimeters.** Fence lines where approach areas are clear of obstruction for 60 to 100 feet outside of the fence and where the general public or other personnel seldom have reason to be in the area.

**Senior FEMA Official (SFO).** The official appointed by the Director of FEMA, or his representative, that is responsible for deploying to the JOC to serve as the senior interagency consequence management representative on the Command Group, and to manage and coordinate activities taken by the Consequence Management Group.

**Serial interface.** An integration strategy for data transfer where components are connected in series.

**Shielded wire.** Wire with a conductive wrap used to mitigate electromagnetic emanations.

**Situational crime prevention.** A crime prevention strategy based on reducing the opportunities for crime by increasing the effort required to commit a crime, increasing the risks associated with committing the crime, and reducing the target appeal or vulnerability (whether property or person). This opportunity reduction is achieved by management and use policies such as procedures and training, as well as physical approaches such as alteration of the built environment.

**Smart card.** A newer card technology that allows data to be written, stored, and read on a card typically used for identification and/or access.

**Software level integration.** An integration strategy that uses software to interface systems. An example of this would be digital

video displayed in the same computer application window and linked to events of a security management system.

**Specific threat.** Known or postulated aggressor activity focused on targeting a particular asset.

**Stand-off distance.** A distance maintained between a building or portion thereof and the potential location for an explosive detonation or other threat.

**Stand-off weapons.** Weapons such as anti-tank weapons and mortars that are launched from a distance at a target.

**State Coordinating Officer (SCO).** The person appointed by the Governor to coordinate state, commonwealth, or territorial response and recovery activities with FRP-related activities of the Federal Government, in cooperation with the FCO.

**State Liaison.** A FEMA official assigned to a particular state, who handles initial coordination with the state in the early stages of an emergency.

**Stationary vehicle bomb.** An explosive-laden car or truck stopped or parked near a building.

**Storm surge.** A dome of sea water created by the strong winds and low barometric pressure in a hurricane that causes severe coastal flooding as the hurricane strikes land.

**Strain sensitive cable.** Strain sensitive cables are transducers that are uniformly sensitive along their entire length and generate an analog voltage when subjected to mechanical distortions or stress resulting from fence motion. They are typically attached to a chain-link fence about halfway between the bottom and top of the fence fabric with plastic ties.

**Structural protective barriers.** Manmade devices (e.g., fences, walls, floors, roofs, grills, bars, roadblocks, signs, or other construction) used to restrict, channel, or impede access.

**Superstructure.** The supporting elements of a building above the foundation.

**Supplies-bomb delivery.** Bombs or incendiary devices concealed and delivered to supply or material handling points such as loading docks.

**System events.** Events that occur normally in the operation of a security management system. Examples include access control operations and changes of state in intrusion detection sensors.

**System software.** Controls that limit and monitor access to the powerful programs and sensitive files that control the computer hardware and secure applications supported by the system.

## T

**Tactics.** The specific methods of achieving the aggressor's goals to injure personnel, destroy assets, or steal materiel or information.

**Tamper switch.** Intrusion detection sensor that monitors an equipment enclosure for breach.

**Tangle-foot wire.** Barbed wire or tape suspended on short metal or wooden pickets outside a perimeter fence to create an obstacle to approach.

**Taut wire sensor.** An intrusion detection sensor utilizing a column of uniformly spaced horizontal wires, securely anchored at each end and stretched taut. Each wire is attached to a sensor to indicate movement of the wire.

**Technical assistance.** The provisioning of direct assistance to states and local jurisdictions to improve capabilities for program development, planning, and operational performances related to responses to WMD terrorist incidents.

**Technological hazards.** Incidents that can arise from human activities such as manufacture, transportation, storage, and use of hazardous materials. For the sake of simplicity, it is assumed that technological emergencies are accidental and that their consequences are unintended.



**TEMPEST.** An unclassified short name referring to investigations and studies of compromising emanations. It is sometimes used synonymously for the term “compromising emanations” (e.g., TEMPEST tests, TEMPEST inspections).

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

**Thermally tempered glass (TTG).** Glass that is heat-treated to have a higher tensile strength and resistance to blast pressures, although with a greater susceptibility to airborne debris.

**Threat.** Any indication, circumstance, or event with the potential to cause loss of, or damage to an asset.

**Threat analysis.** A continual process of compiling and examining all available information concerning potential threats and human-caused hazards. A common method to evaluate terrorist groups is to review the factors of existence, capability, intentions, history, and targeting.

**Time/date stamp.** Data inserted into a CCTV video signal with the time and date of the video as it was created.

**TNT equivalent weight.** The weight of TNT (trinitrotoluene) that has an equivalent energetic output to that of a different weight of another explosive compound.

**Tornado.** A local atmospheric storm, generally of short duration, formed by winds rotating at very high speeds, usually in a counter-clockwise direction. The vortex, up to several hundred yards wide, is visible to the observer as a whirlpool-like column of winds rotating about a hollow cavity or funnel. Winds may reach 300 miles per hour or higher.

**Toxic-free area.** An area within a facility in which the air supply is free of toxic chemical or biological agents.

**Toxicity.** A measure of the harmful effects produced by a given amount of a toxin on a living organism.

**Triple-standard concertina (TSC) wire.** This type of fence uses three rolls of stacked concertina. One roll will be stacked on top of two other rolls that run parallel to each other while resting on the ground, forming a pyramid.

**Tsunami.** Sea waves produced by an undersea earthquake. Such sea waves can reach a height of 80 feet and can devastate coastal cities and low-lying coastal areas.

**Twisted pair wire.** Wire that uses pairs of wires twisted together to mitigate electromagnetic interference.

**Two-person rule.** A security strategy that requires two people to be present in or gain access to a secured area to prevent unobserved access by any individual.

## U

**Unobstructed space.** Space around an inhabited building without obstruction large enough to conceal explosive devices 150 mm (6 inches) or greater in height.

**Unshielded wire.** Wire that does not have a conductive wrap.

## V

**Vault.** A reinforced room for securing items.

**Vertical rod.** Typical door hardware often used with a crash bar to lock a door by inserting rods vertically from the door into the doorframe.

**Vibration sensor.** An intrusion detection sensor that changes state when vibration is present.

**Video intercom system.** An intercom system that also incorporates a small CCTV system for verification.

**Video motion detection.** Motion detection technology that looks for changes in the pixels of a video image.

**Video multiplexer.** A device used to connect multiple video signals to a single location for viewing and/or recording.

**Visual displays.** A display or monitor used to inform the operator visually of the status of the electronic security system.

**Visual surveillance.** The aggressor uses ocular and photographic devices (such as binoculars and cameras with telephoto lenses) to monitor facility or installation operations or to see assets.

**Voice recognition.** A biometric technology that is based on nuances of the human voice.

**Volumetric motion sensor.** An interior intrusion detection sensor that is designed to sense aggressor motion within a protected space.

**Vulnerability.** Any weakness that can be exploited by an aggressor or, in a nonterrorist threat environment, make an asset susceptible to hazard damage.

## W

**Warning.** The alerting of emergency response personnel and the public to the threat of extraordinary danger and the related effects that specific hazards may cause.

**Watch.** Indication in a defined area that conditions are favorable for the specified type of severe weather (e.g., flash flood watch, severe thunderstorm watch, tornado watch, tropical storm watch).

**Waterborne contamination.** Chemical, biological, or radiological agent introduced into and fouling a water supply.

**Weapons-grade material.** Nuclear material considered most suitable for a nuclear weapon. It usually connotes uranium enriched to above 90 percent uranium-235 or plutonium with greater than about 90 percent plutonium-239.

**Weapons of Mass Destruction (WMD).** Any device, material, or substance used in a manner, in a quantity or type, or under circumstances showing an intent to cause death or serious injury to persons, or significant damage to property. An explosive, incendiary, or poison gas, bomb, grenade, rocket having a propellant charge of more than 4 ounces, or a missile having an explosive incendiary charge of more than 0.25 ounce, or mine or device similar to the above; poison gas; weapon involving a disease organism; or weapon that is designed to release radiation or radioactivity at a level dangerous to human life.

**Weigand protocol.** A security industry standard data protocol for card readers.

## Z

**Zoom.** The ability of a CCTV camera to close and focus or open and widen the field of view.

This appendix contains some CBR terms that do not actually appear in this manual. They have been included to present a comprehensive list that pertains to this series of publications.

## **CHEMICAL TERMS**

### **A**

**Acetylcholinesterase.** An enzyme that hydrolyzes the neurotransmitter acetylcholine. The action of this enzyme is inhibited by nerve agents.

**Aerosol.** Fine liquid or solid particles suspended in a gas (e.g., fog or smoke).

**Atropine.** A compound used as an antidote for nerve agents.

### **C**

**Casualty (toxic) agents.** Produce incapacitation, serious injury, or death, and can be used to incapacitate or kill victims. They are the blister, blood, choking, and nerve agents.

**Blister agents.** Substances that cause blistering of the skin. Exposure is through liquid or vapor contact with any exposed tissue (eyes, skin, lungs). Examples are distilled mustard (**HD**), nitrogen mustard (**HN**), lewisite (**L**), mustard/lewisite (**HL**), and phenodichloroarsine (**PD**).

**Blood agents.** Substances that injure a person by interfering with cell respiration (the exchange of oxygen and carbon dioxide between blood and tissues). Examples are arsine (**SA**), cyanogens chloride (**CK**), hydrogen chloride (**HCl**), and hydrogen cyanide (**AC**).

**Choking/lung/pulmonary agents.** Substances that cause physical injury to the lungs. Exposure is through inhalation. In extreme cases, membranes swell and lungs become filled with liquid. Death results from lack of oxygen; hence, the victim is “choked.” Examples are chlorine (**CL**), diphosgene (**DP**), cyanide (**KCN**), nitrogen oxide (**NO**), perfluororisobutylene (**PHIB**), phosgene (**CG**), red phosphorous (**RP**), sulfur trioxide-chlorosulfonic acid (**FS**), Teflon and **PHIB**, titanium tetrachloride (**FM**), and zinc oxide (**HC**).

**Nerve agents.** Substances that interfere with the central nervous system. Exposure is primarily through contact with the liquid (skin and eyes) and secondarily through inhalation of the vapor. Three distinct symptoms associated with nerve agents are: pin-point pupils, an extreme headache, and severe tightness in the chest. See also G-series and V-series nerve agents.

**Chemical agents.** Substances that are intended for use in military operations to kill, seriously injure, or incapacitate people through its physiological effects. Excluded from consideration are riot control agents, and smoke and flame materials. The agent may appear as a vapor, aerosol, or liquid; it can be either a casualty/toxic agent or an incapacitating agent.

**Cutaneous.** Pertaining to the skin.

## D

**Decontamination.** The process of making any person, object, or area safe by absorbing, destroying, neutralizing, making harmless, or removing the hazardous material.



**G-series nerve agents.** Chemical agents of moderate to high toxicity developed in the 1930s. Examples are tabun (**GA**), sarin (**GB**), soman (**GD**), phosphonofluoridic acid, ethyl-, 1-methylethyl ester (**GE**), and cyclohexyl sarin (**GF**).

**Incapacitating agents.** Produce temporary physiological and/or mental effects via action on the central nervous system. Effects may persist for hours or days, but victims usually do not require medical treatment; however, such treatment speeds recovery.

**Vomiting agents.** Produce nausea and vomiting effects; can also cause coughing, sneezing, pain in the nose and throat, nasal discharge, and tears. Examples are adamsite (**DM**), diphenylchloroarsine (**DA**), and diphenylcyanoarsine (**DC**).

**Tear (riot control) agents.** Produce irritating or disabling effects that rapidly disappear within minutes after exposure ceases. Examples are bromobenzylcyanide (**CA**), chloroacetophenone (**CN** or commercially known as Mace), chloropicrin (**PS**), **CNB** (CN in benzene and carbon tetrachloride), **CNC** (CN in chloroform), **CNS** (CN and chloropicrin in chloroform), **CR** (dibenz-(b,f)-1,4-oxazepine, a tear gas), **CS** (tear gas), and **Capsaicin** (pepper spray).

**Central nervous system depressants.** Compounds that have the predominant effect of depressing or blocking the activity of the central nervous system. The primary mental effects include the disruption of the ability to think, sedation, and lack of motivation.

**Central nervous system stimulants.** Compounds that have the predominant effect of flooding the brain with too

much information. The primary mental effect is loss of concentration, causing indecisiveness and the inability to act in a sustained, purposeful manner.

Examples of the depressants and stimulants include agent 15 (suspected Iraqi **BZ**), **BZ** (3-quinulidinyle benzilate), cannabinoids, fentanyls, **LSD** (lysergic acid diethylamide), and phenothiazines.

**Industrial agents.** Chemicals developed or manufactured for use in industrial operations or research by industry, government, or academia. These chemicals are not primarily manufactured for the specific purpose of producing human casualties or rendering equipment, facilities, or areas dangerous for use by man. Hydrogen cyanide, cyanogen chloride, phosgene, chloropicrin, and many herbicides and pesticides are industrial chemicals that also can be chemical agents.

## L

**Liquid agents.** Chemical agents that appear to be an oily film or droplets. The color ranges from clear to brownish amber.

## N

**Nonpersistent agents.** Agents that, upon release, lose the ability to cause casualties after 10 to 15 minutes. They have a high evaporation rate and are lighter than air and will disperse rapidly. They are considered to be short-term hazards; however, in small unventilated areas, these agents will be more persistent.





**Organophosphorous compound.** A compound containing the elements phosphorus and carbon, whose physiological effects include inhibition of acetylcholinesterase. Many pesticides (malathione and parathion) and virtually all nerve agents are organophosphorous compounds.



**Percutaneous agents.** Agents that are able to be absorbed by the body through the skin.

**Persistent agents.** Agents that, upon release, retain their casualty-producing effects for an extended period of time, usually anywhere from 30 minutes to several days. A persistent agent usually has a low evaporation rate and its vapor is heavier than air. Therefore, its vapor cloud tends to hug the ground. They are considered to be long-term hazards. Although inhalation hazards are still a concern, extreme caution should be taken to avoid skin contact as well.

**Protection.** Any means by which an individual protects his or her body. Measures include masks, self-contained breathing apparatuses, clothing, structures such as buildings, and vehicles.



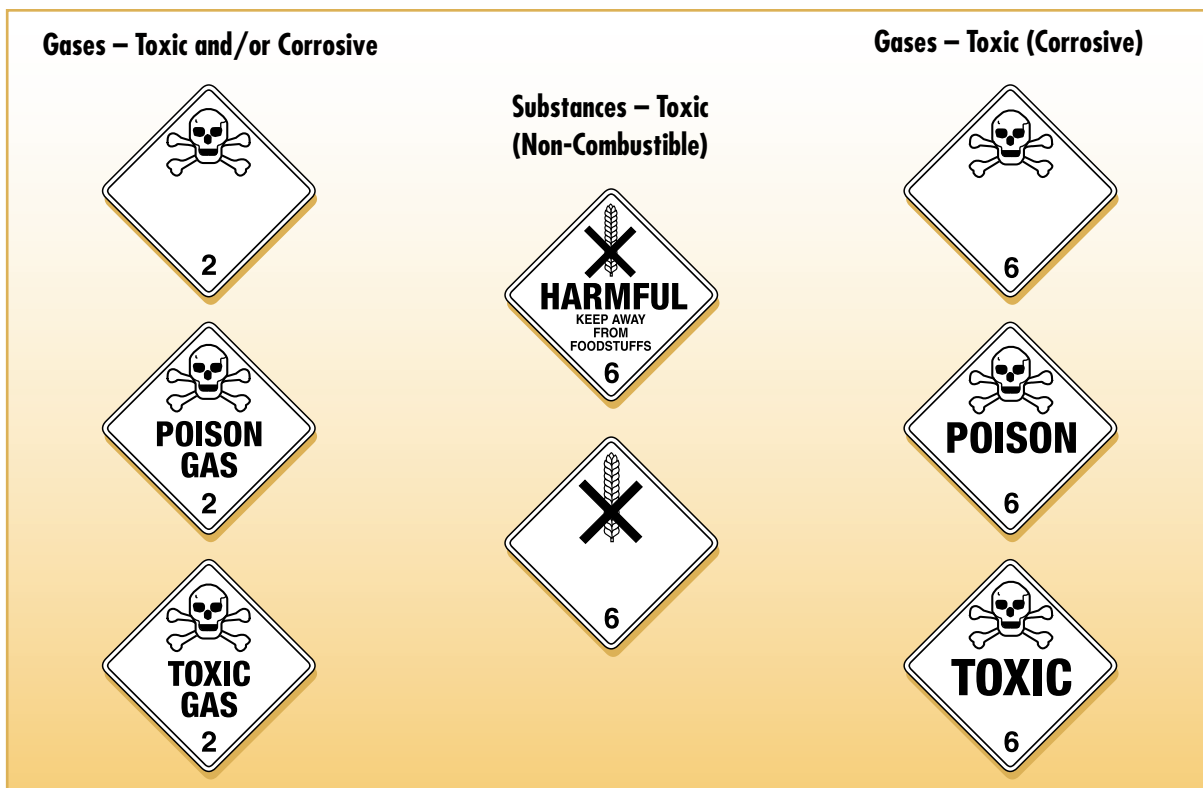
**V-series nerve agents.** Chemical agents of moderate to high toxicity developed in the 1950s. They are generally persistent. Examples are **VE** (phosphonothioic acid, ethyl-, S-[2-(diethylamino)ethyl] O-ethylester), **VG** (phosphorothioic acid, S-[2-(diethylamino)ethyl] O, O-diethyl ester), **VM** (phosphonothioic acid, methyl-, S-[2-(diethylamino)ethyl] O-ethyl ester), **VS** (phosphonothioic acid, ethyl, S-[2-[bis(1-methylethyl)amino]ethyl] O-ethyl

ester), and **VX** (phosphonothioic acid, methyl-, S-[2-[bis(1-methylethyl)amino]ethyl] O-ethyl ester).

**Vapor agents.** A gaseous form of a chemical agent. If heavier than air, the cloud will be close to the ground. If lighter than air, the cloud will rise and disperse more quickly.

**Volatility.** A measure of how readily a substance will vaporize.

### Placards Associated with Chemical Incidents



## BIOLOGICAL TERMS

### A

**Aerosol.** Fine liquid or solid particles suspended in a gas (e.g., fog or smoke).

**Antibiotic.** A substance that inhibits the growth of or kills microorganisms.

**Antisera.** The liquid part of blood containing antibodies that react against disease-causing agents such as those used in biological warfare.

### B

**Bacteria.** Single-celled organisms that multiply by cell division and that can cause disease in humans, plants, or animals.

**Biochemicals.** The chemicals that make up or are produced by living things.

**Biological warfare.** The intentional use of biological agents as weapons to kill or injure humans, animals, or plants, or to damage equipment.

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

**Bioregulators.** Biochemicals that regulate bodily functions. Bioregulators that are produced by the body are termed “endogenous.” Some of these same bioregulators can be chemically synthesized.

## C

**Causative agents.** The organism or toxin that is responsible for causing a specific disease or harmful effect.

**Contagious.** Capable of being transmitted from one person to another.

**Culture.** A population of microorganisms grown in a medium.

## D

**Decontamination.** The process of making people, objects, or areas safe by absorbing, destroying, neutralizing, making harmless, or removing the hazardous material.

## F

**Fungi.** Any of a group of plants mainly characterized by the absence of chlorophyll, the green colored compound found in other plants. Fungi range from microscopic single-celled plants (such as molds and mildews) to large plants (such as mushrooms).

## H

**Host.** An animal or plant that harbors or nourishes another organism.

## I

**Incapacitating agents.** Agents that produce physical or psychological effects, or both, that may persist for hours or days after exposure, rendering victims incapable of performing normal physical and mental tasks.

**Infectious agents.** Biological agents capable of causing disease in a susceptible host.

**Infectivity.** (1) The ability of an organism to spread. (2) The number of organisms required to cause an infection to secondary hosts. (3) The capability of an organism to spread out from the site of infection and cause disease in the host organism. Infectivity also can be viewed as the number of organisms required to cause an infection.

## L

**Line-source delivery system.** A delivery system in which the biological agent is dispersed from a moving ground or air vehicle in a line perpendicular to the direction of the prevailing wind. (See also “point-source delivery system.”)

## M

**Microorganism.** Any organism, such as bacteria, viruses, and some fungi, that can be seen only with a microscope.

**Mycotoxin.** A toxin produced by fungi.

## N

**Nebulizer.** A device for producing a fine spray or aerosol.

## O

**Organism.** Any individual living thing, whether animal or plant.

## P

**Parasite.** Any organism that lives in or on another organism without providing benefit in return.

**Pathogen.** Any organism (usually living), such as bacteria, fungi, and viruses, capable of producing serious disease or death.

**Pathogenic agents.** Biological agents capable of causing serious disease.

**Point-source delivery system.** A delivery system in which the biological agent is dispersed from a stationary position. This delivery method results in coverage over a smaller area than with the line-source system. See also line-source delivery system.

## R

**Route of exposure (entry).** The path by which a person comes into contact with an agent or organism (e.g., through breathing, digestion, or skin contact).

## S

**Single-cell protein.** Protein-rich material obtained from cultured algae, fungi, protein, and bacteria, and often used as food or animal feed.

**Spore.** A reproductive form some microorganisms can take to become resistant to environmental conditions, such as extreme heat or cold, while in a “resting stage.”

## T

**Toxicity.** A measure of the harmful effect produced by a given amount of a toxin on a living organism. The relative toxicity of

an agent can be expressed in milligrams of toxin needed per kilogram of body weight to kill experimental animals.

**Toxins.** Poisonous substances produced by living organisms.

## V

**Vaccine.** A preparation of killed or weakened microorganism products used to artificially induce immunity against a disease.

**Vector.** An agent, such as an insect or rat, capable of transferring a pathogen from one organism to another.

**Venom.** A poison produced in the glands of some animals (e.g., snakes, scorpions, or bees).

**Virus.** An infectious microorganism that exists as a particle rather than as a complete cell. Particle sizes range from 20 to 400 nanometers (one-billionth of a meter). Viruses are not capable of reproducing outside of a host cell.

### Placards Associated with Biological Incidents



## RADIOLOGICAL TERMS

### A

**Acute radiation syndrome.** Consists of three levels of effects: hematopoietic (blood cells, most sensitive); gastrointestinal (GI cells, very sensitive); and central nervous system (brain/muscle cells, insensitive). The initial signs and symptoms are nausea, vomiting, fatigue, and loss of appetite. Below about 200 rems, these symptoms may be the only indication of radiation exposure.

**Alpha particles ( $\alpha$ ).** Alpha particles have a very short range in air and a very low ability to penetrate other materials, but also have a strong ability to ionize materials. Alpha particles are unable to penetrate even the thin layer of dead cells of human skin and consequently are not an external radiation hazard. Alpha-emitting nuclides inside the body as a result of inhalation or ingestion are a considerable internal radiation hazard.

### B

**Beta particles ( $\beta$ ).** High-energy electrons emitted from the nucleus of an atom during radioactive decay. They normally can be stopped by the skin or a very thin sheet of metal.

### C

**Cesium-137 (Cs-137).** A strong gamma ray source and can contaminate property, entailing extensive cleanup. It is commonly used in industrial measurement gauges and for irradiation of material. Its half-life is 30.2 years.

**Cobalt-60 (Co-60).** A strong gamma ray source, and is extensively used as a radiotherapeutic for treating cancer, food and material irradiation, gamma radiography, and industrial measurement gauges. Its half-life is 5.27 years.



**Curie (Ci).** A unit of radioactive decay rate defined as  $3.7 \times 10^{10}$  disintegrations per second.

## D

**Decay.** The process by which an unstable element is changed to another isotope or another element by the spontaneous emission of radiation from its nucleus. This process can be measured by using radiation detectors such as Geiger counters.

**Decontamination.** The process of making people, objects, or areas safe by absorbing, destroying, neutralizing, making harmless, or removing the hazardous material.

**Dose.** A general term for the amount of radiation absorbed over a period of time.

**Dosimeter.** A portable instrument for measuring and registering the total accumulated dose to ionizing radiation.

## G

**Gamma ray ( $\gamma$ ).** A high-energy photon emitted from the nucleus of atoms; similar to an x-ray. It can penetrate deeply into body tissue and many materials. Cobalt-60 and Cesium-137 are both strong gamma-emitters. Shielding against gamma radiation requires thick layers of dense materials, such as lead. Gamma rays are potentially lethal to humans.

## H

**Half-life.** The amount of time needed for half of the atoms of a radioactive material to decay.

**Highly enriched uranium (HEU).** Uranium that is enriched to above 20 percent Uranium-235 (U-235). Weapons-grade HEU is enriched to above 90 percent in U-235.

**Ionize.** To split off one or more electrons from an atom, thus leaving it with a positive electric charge. The electrons usually attach to one of the atoms or molecules, giving them a negative charge.

**Iridium-192.** A gamma ray emitting radioisotope used for gamma radiography. Its half-life is 73.83 days.

**Isotope.** A specific element always has the same number of protons in the nucleus. That same element may, however, appear in forms that have different numbers of neutrons in the nucleus. These different forms are referred to as “isotopes” of the element; for example, deuterium (**2H**) and tritium (**3H**) are isotopes of ordinary hydrogen (**H**).

**Lethal dose (50/30).** The dose of radiation expected to cause death within 30 days to 50 percent of those exposed without medical treatment. The generally accepted range is from 400-500 rem received over a short period of time.

**Nuclear reactor.** A device in which a controlled, self-sustaining nuclear chain reaction can be maintained with the use of cooling to remove generated heat.

## P

**Plutonium-239 (Pu-239).** A metallic element used for nuclear weapons. Its half-life is 24,110 years.

## R

**Rad.** A unit of absorbed dose of radiation defined as deposition of 100 ergs of energy per gram of tissue. A rad amounts to approximately one ionization per cubic micron.

**Radiation.** High energy alpha or beta particles or gamma rays that are emitted by an atom as the substance undergoes radioactive decay.

**Radiation sickness.** Symptoms resulting from excessive exposure to radiation of the body.

**Radioactive waste.** Disposable, radioactive materials resulting from nuclear operations. Wastes are generally classified into two categories, high-level and low-level.

**Radiological Dispersal Device (RDD).** A device (weapon or equipment), other than a nuclear explosive device, designed to disseminate radioactive material in order to cause destruction, damage, or injury by means of the radiation produced by the decay of such material.

**Radioluminescence.** The luminescence produced by particles emitted during radioactive decay.

**Roentgen Equivalent Man (REM or rem).** A unit of absorbed dose that takes into account the relative effectiveness of radiation that harms human health.

## S

**Shielding.** Materials (lead, concrete, etc.) used to block or attenuate radiation for protection of equipment, materials, or people.

**Special Nuclear Material (SNM).** Plutonium and uranium enriched in the isotopes Uranium-233 or Uranium-235.

## U

**Uranium 235 (U-235).** Naturally-occurring U-235 is found at 0.72 percent enrichment. U-235 is used as a reactor fuel or for weapons; however, weapons typically use U-235 enriched to 90 percent. Its half-life is  $7.04 \times 10^8$  years.

## X

**X-ray.** An invisible, highly penetrating electromagnetic radiation of much shorter wavelength (higher frequency) than visible light. Very similar to gamma rays.

### Placards Associated with Radiological Incidents



The following web sites are available for further clarification or for terms not used in this manual:

Chemical, Biological, Radiological (CBR)  
[Formerly NBC (Nuclear, Biological, Chemical)]

<http://www.nbc-med.org/SiteContent/glossary.asp?B>

<http://www.nbcprotect.com/new/glossary.htm>







# SELECTED BIOLOGICAL AGENT CHARACTERISTICS

Agent Type	Disease/Condition of Pathogen	Description of Agent	Transmissibility	Infectivity	Incubation Period	Duration of Illness	Persistability	Mortality/ Morbidity	Rate of Action	Symptoms	Treatment	Possible Route of Delivery
A	Botulism (paralytic)	Non-spore gram-positive, aerobic, rod-shaped bacteria (1-10µm x 2-5µm) with flagella. Produces a potent neurotoxin (BoTx) that blocks acetylcholine release at the neuromuscular junction.	No	High/Low	1-7 days	3-4 days	Stable in soil, resistant to heat and sunlight.	Yes	24-36 hrs after symptoms	Fever, fatigue, drooping eyelids, and constipation. No systemic symptoms.	Antitoxin. Supportive care. No specific treatment for the toxin itself.	Antitoxin. Supportive care. No systemic symptoms.
B	Brucella (Brucella abortus, Brucella melitensis, Brucella abortus)	Small, curved, motile, gram-negative, non-spore-forming rod-shaped bacteria (0.5-1.5µm x 0.5-1.5µm).	No	High/Low	Days to months	Weeks to months	Stable in soil, resistant to heat and sunlight.	Yes	2-30 days	Flu-like symptoms, fever, sweats, weight loss, and joint pain.	Antibiotics (doxycycline and rifampin). Supportive care.	Antitoxin. Supportive care. No systemic symptoms.
C	Cholera	Short, curved, motile, gram-negative, non-spore-forming rod-shaped bacteria (3µm x 0.5µm) with flagella. Produces a potent enterotoxin (EPEC) that causes watery diarrhea.	High	High/Low	1-5 days	1 or more weeks	Stable in soil, resistant to heat and sunlight.	Yes	1-2 days	Watery diarrhea, vomiting, dehydration, and muscle cramps.	Rehydration. Supportive care. No specific treatment for the toxin itself.	Antitoxin. Supportive care. No systemic symptoms.
D	Cholera (Vibrio cholerae)	Comma-shaped, motile, gram-negative, non-spore-forming rod-shaped bacteria (3µm x 0.5µm) with flagella. Produces a potent enterotoxin (EPEC) that causes watery diarrhea.	High	High/Low	1-5 days	1 or more weeks	Stable in soil, resistant to heat and sunlight.	Yes	1-2 days	Watery diarrhea, vomiting, dehydration, and muscle cramps.	Rehydration. Supportive care. No specific treatment for the toxin itself.	Antitoxin. Supportive care. No systemic symptoms.
E	Diphtheria	Gram-positive, rod-shaped, non-motile, non-spore-forming bacteria (2-10µm x 0.5-1µm). Produces a potent exotoxin (Dtx) that causes a thick, white membrane in the throat.	No	High/Low	2-5 days	2-4 weeks	Stable in soil, resistant to heat and sunlight.	Yes	2-5 days	Sore throat, fever, and a thick, white membrane in the throat.	Antitoxin. Supportive care. No specific treatment for the toxin itself.	Antitoxin. Supportive care. No systemic symptoms.
F	Ebola (Ebola virus)	Non-enveloped, rod-shaped, filamentous virus (100-1400nm x 10-15nm). Produces a potent hemorrhagic fever.	No	High/Low	2-21 days	2-6 weeks	Stable in soil, resistant to heat and sunlight.	Yes	2-21 days	Fever, fatigue, muscle pain, and hemorrhagic fever.	Supportive care. No specific treatment for the virus itself.	Antitoxin. Supportive care. No systemic symptoms.
G	Q Fever	Gram-negative, rod-shaped, non-motile, non-spore-forming bacteria (0.5-1µm x 0.5-1µm). Produces a potent fever.	No	High/Low	1-30 days	2-6 weeks	Stable in soil, resistant to heat and sunlight.	Yes	1-30 days	Fever, fatigue, and muscle pain.	Antibiotics (doxycycline and rifampin). Supportive care.	Antitoxin. Supportive care. No systemic symptoms.
H	Rocky Mountain spotted fever	Gram-negative, rod-shaped, non-motile, non-spore-forming bacteria (0.5-1µm x 0.5-1µm). Produces a potent fever.	No	High/Low	1-14 days	2-6 weeks	Stable in soil, resistant to heat and sunlight.	Yes	1-14 days	Fever, fatigue, and muscle pain.	Antibiotics (doxycycline and rifampin). Supportive care.	Antitoxin. Supportive care. No systemic symptoms.
I	Typhoid (Salmonella typhi)	Gram-negative, rod-shaped, motile, non-spore-forming bacteria (2-12µm x 0.5-1µm). Produces a potent fever.	High	High/Low	1-30 days	2-6 weeks	Stable in soil, resistant to heat and sunlight.	Yes	1-30 days	Fever, fatigue, and muscle pain.	Antibiotics (ciprofloxacin and rifampin). Supportive care.	Antitoxin. Supportive care. No systemic symptoms.
J	Typhoid (Salmonella typhi)	Gram-negative, rod-shaped, motile, non-spore-forming bacteria (2-12µm x 0.5-1µm). Produces a potent fever.	High	High/Low	1-30 days	2-6 weeks	Stable in soil, resistant to heat and sunlight.	Yes	1-30 days	Fever, fatigue, and muscle pain.	Antibiotics (ciprofloxacin and rifampin). Supportive care.	Antitoxin. Supportive care. No systemic symptoms.
K	Yersinia (Yersinia enterocolitica)	Gram-negative, rod-shaped, motile, non-spore-forming bacteria (3-10µm x 0.5-1µm). Produces a potent fever.	No	High/Low	1-10 days	2-6 weeks	Stable in soil, resistant to heat and sunlight.	Yes	1-10 days	Fever, fatigue, and muscle pain.	Antibiotics (doxycycline and rifampin). Supportive care.	Antitoxin. Supportive care. No systemic symptoms.
L	Yersinia (Yersinia enterocolitica)	Gram-negative, rod-shaped, motile, non-spore-forming bacteria (3-10µm x 0.5-1µm). Produces a potent fever.	No	High/Low	1-10 days	2-6 weeks	Stable in soil, resistant to heat and sunlight.	Yes	1-10 days	Fever, fatigue, and muscle pain.	Antibiotics (doxycycline and rifampin). Supportive care.	Antitoxin. Supportive care. No systemic symptoms.
M	Yersinia (Yersinia enterocolitica)	Gram-negative, rod-shaped, motile, non-spore-forming bacteria (3-10µm x 0.5-1µm). Produces a potent fever.	No	High/Low	1-10 days	2-6 weeks	Stable in soil, resistant to heat and sunlight.	Yes	1-10 days	Fever, fatigue, and muscle pain.	Antibiotics (doxycycline and rifampin). Supportive care.	Antitoxin. Supportive care. No systemic symptoms.
N	Yersinia (Yersinia enterocolitica)	Gram-negative, rod-shaped, motile, non-spore-forming bacteria (3-10µm x 0.5-1µm). Produces a potent fever.	No	High/Low	1-10 days	2-6 weeks	Stable in soil, resistant to heat and sunlight.	Yes	1-10 days	Fever, fatigue, and muscle pain.	Antibiotics (doxycycline and rifampin). Supportive care.	Antitoxin. Supportive care. No systemic symptoms.
O	Yersinia (Yersinia enterocolitica)	Gram-negative, rod-shaped, motile, non-spore-forming bacteria (3-10µm x 0.5-1µm). Produces a potent fever.	No	High/Low	1-10 days	2-6 weeks	Stable in soil, resistant to heat and sunlight.	Yes	1-10 days	Fever, fatigue, and muscle pain.	Antibiotics (doxycycline and rifampin). Supportive care.	Antitoxin. Supportive care. No systemic symptoms.
P	Yersinia (Yersinia enterocolitica)	Gram-negative, rod-shaped, motile, non-spore-forming bacteria (3-10µm x 0.5-1µm). Produces a potent fever.	No	High/Low	1-10 days	2-6 weeks	Stable in soil, resistant to heat and sunlight.	Yes	1-10 days	Fever, fatigue, and muscle pain.	Antibiotics (doxycycline and rifampin). Supportive care.	Antitoxin. Supportive care. No systemic symptoms.
Q	Yersinia (Yersinia enterocolitica)	Gram-negative, rod-shaped, motile, non-spore-forming bacteria (3-10µm x 0.5-1µm). Produces a potent fever.	No	High/Low	1-10 days	2-6 weeks	Stable in soil, resistant to heat and sunlight.	Yes	1-10 days	Fever, fatigue, and muscle pain.	Antibiotics (doxycycline and rifampin). Supportive care.	Antitoxin. Supportive care. No systemic symptoms.
R	Yersinia (Yersinia enterocolitica)	Gram-negative, rod-shaped, motile, non-spore-forming bacteria (3-10µm x 0.5-1µm). Produces a potent fever.	No	High/Low	1-10 days	2-6 weeks	Stable in soil, resistant to heat and sunlight.	Yes	1-10 days	Fever, fatigue, and muscle pain.	Antibiotics (doxycycline and rifampin). Supportive care.	Antitoxin. Supportive care. No systemic symptoms.
S	Yersinia (Yersinia enterocolitica)	Gram-negative, rod-shaped, motile, non-spore-forming bacteria (3-10µm x 0.5-1µm). Produces a potent fever.	No	High/Low	1-10 days	2-6 weeks	Stable in soil, resistant to heat and sunlight.	Yes	1-10 days	Fever, fatigue, and muscle pain.	Antibiotics (doxycycline and rifampin). Supportive care.	Antitoxin. Supportive care. No systemic symptoms.
T	Yersinia (Yersinia enterocolitica)	Gram-negative, rod-shaped, motile, non-spore-forming bacteria (3-10µm x 0.5-1µm). Produces a potent fever.	No	High/Low	1-10 days	2-6 weeks	Stable in soil, resistant to heat and sunlight.	Yes	1-10 days	Fever, fatigue, and muscle pain.	Antibiotics (doxycycline and rifampin). Supportive care.	Antitoxin. Supportive care. No systemic symptoms.
U	Yersinia (Yersinia enterocolitica)	Gram-negative, rod-shaped, motile, non-spore-forming bacteria (3-10µm x 0.5-1µm). Produces a potent fever.	No	High/Low	1-10 days	2-6 weeks	Stable in soil, resistant to heat and sunlight.	Yes	1-10 days	Fever, fatigue, and muscle pain.	Antibiotics (doxycycline and rifampin). Supportive care.	Antitoxin. Supportive care. No systemic symptoms.
V	Yersinia (Yersinia enterocolitica)	Gram-negative, rod-shaped, motile, non-spore-forming bacteria (3-10µm x 0.5-1µm). Produces a potent fever.	No	High/Low	1-10 days	2-6 weeks	Stable in soil, resistant to heat and sunlight.	Yes	1-10 days	Fever, fatigue, and muscle pain.	Antibiotics (doxycycline and rifampin). Supportive care.	Antitoxin. Supportive care. No systemic symptoms.
W	Yersinia (Yersinia enterocolitica)	Gram-negative, rod-shaped, motile, non-spore-forming bacteria (3-10µm x 0.5-1µm). Produces a potent fever.	No	High/Low	1-10 days	2-6 weeks	Stable in soil, resistant to heat and sunlight.	Yes	1-10 days	Fever, fatigue, and muscle pain.	Antibiotics (doxycycline and rifampin). Supportive care.	Antitoxin. Supportive care. No systemic symptoms.
X	Yersinia (Yersinia enterocolitica)	Gram-negative, rod-shaped, motile, non-spore-forming bacteria (3-10µm x 0.5-1µm). Produces a potent fever.	No	High/Low	1-10 days	2-6 weeks	Stable in soil, resistant to heat and sunlight.	Yes	1-10 days	Fever, fatigue, and muscle pain.	Antibiotics (doxycycline and rifampin). Supportive care.	Antitoxin. Supportive care. No systemic symptoms.
Y	Yersinia (Yersinia enterocolitica)	Gram-negative, rod-shaped, motile, non-spore-forming bacteria (3-10µm x 0.5-1µm). Produces a potent fever.	No	High/Low	1-10 days	2-6 weeks	Stable in soil, resistant to heat and sunlight.	Yes	1-10 days	Fever, fatigue, and muscle pain.	Antibiotics (doxycycline and rifampin). Supportive care.	Antitoxin. Supportive care. No systemic symptoms.
Z	Yersinia (Yersinia enterocolitica)	Gram-negative, rod-shaped, motile, non-spore-forming bacteria (3-10µm x 0.5-1µm). Produces a potent fever.	No	High/Low	1-10 days	2-6 weeks	Stable in soil, resistant to heat and sunlight.	Yes	1-10 days	Fever, fatigue, and muscle pain.	Antibiotics (doxycycline and rifampin). Supportive care.	Antitoxin. Supportive care. No systemic symptoms.

This appendix contains some CBR terms that do not actually appear in this manual. They have been included to present a comprehensive list that pertains to this series of publications.

## CHEMICAL TERMS

### A

**Acetylcholinesterase.** An enzyme that hydrolyzes the neurotransmitter acetylcholine. The action of this enzyme is inhibited by nerve agents.

**Aerosol.** Fine liquid or solid particles suspended in a gas (e.g., fog or smoke).

**Atropine.** A compound used as an antidote for nerve agents.

### C

**Casualty (toxic) agents.** Produce incapacitation, serious injury, or death, and can be used to incapacitate or kill victims. They are the blister, blood, choking, and nerve agents.

**Blister agents.** Substances that cause blistering of the skin. Exposure is through liquid or vapor contact with any exposed tissue (eyes, skin, lungs). Examples are distilled mustard (**HD**), nitrogen mustard (**HN**), lewisite (**L**), mustard/lewisite (**HL**), and phenodichloroarsine (**PD**).

**Blood agents.** Substances that injure a person by interfering with cell respiration (the exchange of oxygen and carbon dioxide between blood and tissues). Examples are arsine (**SA**), cyanogens chloride (**CK**), hydrogen chloride (**HCl**), and hydrogen cyanide (**AC**).

**Choking/lung/pulmonary agents.** Substances that cause physical injury to the lungs. Exposure is through inhalation. In extreme cases, membranes swell and



**A**n overall site-security system is composed of three major subelements: detection, delay, and response. The detection subelement includes intrusion detection, assessment, and entry control. The purpose of this appendix is to introduce the basic concepts of site security systems, including the use of Electronic Security Systems (ESSs), boundary-penetration sensors, volumetric motion sensors, exterior intrusion detection sensors, microwave sensors, infrared sensors, video motion sensors, electronic entry control, and monitoring designated restricted areas.

## USE OF ESS

An ESS is an integrated system that encompasses interior and exterior sensors; closed circuit television (CCTV) systems for assessing alarm conditions; Electronic Entry Control Systems (EECSs); data-transmission media (DTM); and alarm reporting systems for monitoring, controlling, and displaying various alarm and system information. Interior and exterior sensors and their associated communication and display subsystems are collectively called IDSs.

An ESS is used to provide early warning of an intruder. This system consists of hardware and software elements operated by trained security personnel.

A system is configured to provide one or more layers of detection around an asset. Each layer is made up of a series of contiguous detection zones designed to isolate the asset and to control the entry and exit of authorized personnel and materials.

## General ESS Description

An ESS consists of sensors interfaced with electronic entry control devices, CCTV, alarm reporting displays (both visual and audible), and security lighting. The situation is assessed by sending guards

to the alarm point or by using CCTV. Alarm reporting devices and video monitors are located in the security center. The asset's importance will determine whether multiple or redundant security centers are required and, ultimately, the required sophistication of all elements in the ESS. Digital and analog data are transmitted from local (field) interior and exterior locations to the security center for processing. Reliability and accuracy are important functional requirements of the data-transmission system.

### **ESS Design Considerations**

A facility may require interior and exterior ESS elements, depending on the level of protection required. The applicable regulations, threat, and design criteria will define the ESS's general requirements. For an existing ESS, hardware and software may need to be supplemented, upgraded, or completely replaced. A site layout (in which all assets are identified and located) is required. It is a useful design tool for such tasks as configuring the DTM.

The exterior and interior IDSs should be configured as layers of unbroken rings concentrically surrounding the asset. These rings should correspond to defensive layers that constitute the delay system. The first detection layer is located at the outermost defensive layer necessary to provide the required delay. Detection layers can be on a defensive layer, in the area between two defensive layers, or on the asset itself, depending on the delay required. For example, if a wall of an interior room provides sufficient delay for effective response to aggression, detection layers could be between the facility exterior and interior-room wall or on the interior-room wall. They would detect the intruder before penetration of the interior wall is possible.

### **PERIMETER LAYOUT AND ZONING SENSORS**

A protected area's perimeter is usually defined by an enclosing wall or fence or a natural barrier such as water. For exterior sensors to be effective, the perimeter around which they are to be deployed must be precisely defined. In most applications, a dual

chain-link-fence configuration will be established around the perimeter (see Chapter 2.4.1 for additional information). Typically, fences should be between 30 and 50 feet apart; as the distance increases, it is harder for an intruder to bridge the fences. If fence separation is less than 30 feet, some microwave and ported coax sensors cannot be used. The area between fences (called the controlled area or isolation zone) may need to be cleared of vegetation and graded, depending on the type of sensor used. Proper drainage is required to preclude standing water and to prevent the formation of gullies caused by running water after a heavy rain or melting snow. Cleared areas are required inside and outside of the controlled area. These areas enhance routine observation, as well as sensor-alarm assessment, and minimize the protective cover available to a would-be intruder.

After the perimeter has been defined, the next step is to divide it into specific detection zones. The length of each detection zone is determined by evaluating the contour, the existing terrain, and the operational activities along the perimeter. Detection zones should be long and straight to minimize the number of sensors or cameras necessary and to aid guard assessment if cameras are not used. It may be more economical to straighten an existing fence line than to create numerous detection zones in accommodating a crooked fence line. If the perimeter is hilly and line of sight (LOS) sensors or CCTV assessment are used, the length of individual detection zones will be commensurate with sensor limitations. Entry points for personnel and vehicles must be configured as independent zones. This enables deactivation of the sensors in these zones; that is, placing them in the access mode during customary working hours (assuming the entry points are manned) without having to deactivate adjacent areas.

The specific length of individual zones can vary around the perimeter. Although specific manufacturers may advertise maximum zone lengths exceeding 1,000 feet, it is not practical to exceed a zone length of 300 feet. If the zone is longer, it will be difficult for an operator using CCTV assessment or for the response force to identify the location of an intrusion or the cause of a false alarm.

When establishing zones using multiple sensors, the designer should establish coincident zones where the length and location of each individual sensor will be identical for all sensors within a given zone. If an alarm occurs in a specific zone, the operator can readily determine its approximate location by referring to a map of the perimeter. This also minimizes the number of CCTV cameras required for assessment and simplifies the interface between the alarm-annunciation system and the CCTV switching system.

## **BOUNDARY-PENETRATION SENSORS**

Boundary-penetration sensors are designed to detect penetration or attempted penetration through perimeter barriers. These barriers include walls, ceilings, duct openings, doors, and windows.

- **Structural-vibration sensors.** Structural-vibration sensors detect low-frequency energy generated in an attempted penetration of a physical barrier (such as a wall or a ceiling) by hammering, drilling, cutting, detonating explosives, or employing other forcible methods of entry. A piezoelectric transducer senses mechanical energy and converts it into electrical signals proportional in magnitude to the vibrations.
- **Glass-breakage sensors.** Glass-breakage sensors detect the breaking of glass. The noise from breaking glass consists of frequencies in both the audible and ultrasonic range. Glass-breakage sensors use microphone transducers to detect the glass breakage. The sensors are designed to respond to specific frequencies only, thus minimizing such false alarms as may be caused by banging on the glass.
- **Passive ultrasonic sensors.** Passive ultrasonic sensors detect acoustical energy in the ultrasonic frequency range, typically between 20 and 30 kilohertz (kHz). They are used to detect an attempted penetration through rigid barriers (such as metal or masonry walls, ceilings, and floors). They also detect penetration through windows and vents covered by metal grilles, shutters, or bars if these openings are properly sealed against outside sounds.

- **Balanced magnetic switches.** Balanced magnetic switches (BMSs) are typically used to detect the opening of a door. These sensors can also be used on windows, hatches, gates, or other structural devices that can be opened to gain entry. When using a BMS, mount the switch mechanism on the doorframe and the actuating magnet on the door. Typically, the BMS has a three-position reed switch and an additional magnet (called the bias magnet) located adjacent to the switch. When the door is closed, the reed switch is held in the balanced or center position by interacting magnetic fields. If the door is opened or an external magnet is brought near the sensor in an attempt to defeat it, the switch becomes unbalanced and generates an alarm. A BMS must be mounted so that the magnet receives maximum movement when the door or window is opened.
- **Grid wire sensors.** The grid wire sensor consists of a continuous electrical wire arranged in a grid pattern. The wire maintains an electrical current. An alarm is generated when the wire is broken. The sensor detects forced entry through walls, floors, ceilings, doors, windows, and other barriers. An enamel-coated number 24 or 26 American wire gauge (AWG) solid-copper wire typically forms the grid. The grid's maximum size is determined by the spacing between the wires, the wire's resistance, and the electrical characteristics of the source providing the current. The grid wire can be installed directly on the barrier, in a grille or screen that is mounted on the barrier, or over an opening that requires protection.

## **VOLUMETRIC MOTION SENSORS**

Volumetric motion sensors are designed to detect intruder motion within the interior of a protected volume. Volumetric sensors may be active or passive. Active sensors (such as microwave) fill the volume to be protected with an energy pattern and recognize a disturbance in the pattern when anything moves within the detection zone. Whereas active sensors generate their own energy pattern to detect an intruder, passive sensors (such as infrared

(IR)) detect energy generated by an intruder. Some sensors, known as dual technology sensors, use a combination of two different technologies, usually one active and one passive, within the same unit. If CCTV assessment or surveillance cameras are installed, video motion sensors can be used to detect intruder movement within the area. Because ultrasonic motion sensors are seldom used, they will not be discussed herein.

- **Microwave motion sensors.** With microwave motion sensors, high-frequency electromagnetic energy is used to detect an intruder's motion within the protected area. Interior or sophisticated microwave motion sensors are normally used.
  - **Interior microwave motion sensors.** Interior microwave motion sensors are typically monostatic; the transmitter and the receiver are housed in the same enclosure (transceiver).
  - **Sophisticated microwave motion sensors.** Sophisticated microwave motion sensors may be equipped with electronic range gating. This feature allows the sensor to ignore the signals reflected beyond the settable detection range. Range gating may be used to effectively minimize unwanted alarms from activity outside the protected area.
- **Passive infrared (PIR) motion sensors.** PIR motion sensors detect a change in the thermal energy pattern caused by a moving intruder and initiate an alarm when the change in energy satisfies the detector's alarm criteria. These sensors are passive devices because they do not transmit energy; they monitor the energy radiated by the surrounding environment.
- **Dual technology sensors.** To minimize the generation of alarms caused by sources other than intruders, dual-technology sensors combine two different technologies in one unit. Ideally, this is achieved by combining two sensors that individually have a high probability of detection (POD) and do not respond to common sources of false alarms. Available dual-

technology sensors combine an active ultrasonic or microwave sensor with a PIR sensor. The alarms from each sensor are logically combined in an “and” configuration (i.e., nearly simultaneous alarms from both active and passive sensors are needed to produce a valid alarm).

- **Video motion sensors.** A video motion sensor generates an alarm when an intruder enters a selected portion of a CCTV camera’s field of view. The sensor processes and compares successive images between the images against predefined alarm criteria. There are two categories of video motion detectors, analog and digital. Analog detectors generate an alarm in response to changes in a picture’s contrast. Digital devices convert selected portions of the analog video signal into digital data that are compared with data converted previously; if differences exceed preset limits, an alarm is generated. The signal processor usually provides an adjustable window that can be positioned anywhere on the video image. Available adjustments permit changing horizontal and vertical window size, window position, and window sensitivity. More sophisticated units provide several adjustable windows that can be individually sized and positioned. Multiple windows permit concentrating on several specific areas of an image while ignoring others. For example, in a scene containing six doorways leading into a long hallway, the sensor can be set to monitor only two critical doorways.
  
- **Point sensors.** Point sensors are used to protect specific objects within a facility. These sensors (sometimes referred to as proximity sensors) detect an intruder coming in close proximity to, touching, or lifting an object. Several different types are available, including capacitance sensors, pressure mats, and pressure switches. Other types of sensors can also be used for object protection.
  
- **Capacitance sensors.** Capacitance sensors detect an intruder approaching or touching a metal object by sensing a change in capacitance between the object and the ground. A capacitor

consists of two metallic plates separated by a dielectric medium. A change in the dielectric medium or electrical charge results in a change in capacitance. In practice, the metal object to be protected forms one plate of the capacitor and the ground plane surrounding the object forms the second plate. The sensor processor measures the capacitance between the metal object and the ground plane. An approaching intruder alters the dielectric value, thus changing the capacitance. If the net capacitance change satisfies the alarm criteria, an alarm is generated.

- Pressure mats. Pressure mats generate an alarm when pressure is applied to any part of the mat's surface, such as when someone steps on the mat. One type of construction uses two layers of copper screening separated by soft-sponge rubber insulation with large holes in it. Another type uses parallel strips of ribbon switches made from two strips of metal separated by an insulating material and spaced several inches apart. When enough pressure is applied to the mat, either the screening or the metal strips make contact, generating an alarm. Pressure mats can be used to detect an intruder approaching a protected object, or they can be placed by doors or windows to detect entry. Because pressure mats are easy to bridge, they should be well concealed, such as placing them under a carpet.
  
- **Pressure switches.** Mechanically activated contact switches or single ribbon switches can be used as pressure switches. Objects that require protection can be placed on top of the switch. When the object is moved, the switch actuates and generates an alarm. In this usage, the switch must be well concealed. The interface between the switch and the protected object should be designed so that an adversary cannot slide a thin piece of material under the object to override the switch while the object is removed.



## EXTERIOR INTRUSION DETECTION SENSORS

Exterior intrusion detection sensors are customarily used to detect an intruder crossing the boundary of a protected area. They can also be used in clear zones between fences or around buildings, for protecting materials and equipment stored outdoors within a protected boundary, or in estimating the POD for buildings and other facilities.

Because of the nature of the outdoor environment, exterior sensors are also more susceptible to nuisance and environmental alarms than interior sensors. Inclement weather conditions (e.g., heavy rain, hail, and high wind), vegetation, the natural variation of the temperature of objects in the detection zone, blowing debris, and animals are major sources of unwanted alarms.

Due to this vulnerability, it is extremely important that enclosures are located and installed properly and that adequate physical protection is provided. Several different types of exterior intrusion detection sensors are available:

- Fence sensors
- Buried line sensors
- Video motion sensors

## FENCE SENSORS

Fence sensors detect attempts to penetrate a fence around a protected area. Penetration attempts (e.g., climbing, cutting, or lifting) generate mechanical vibrations and stresses in fence fabric and posts that are usually different than those caused by natural phenomena like wind and rain. The basic types of sensors used to detect these vibrations and stresses are strain sensitive cable, taut wire, fiber optics, and capacitance.

- **Strain sensitive cables.** Strain sensitive cables are transducers that are uniformly sensitive along their entire length. They generate an analog voltage when subject to mechanical

distortions or stress resulting from fence motion. Strain sensitive cables are sensitive to both low and high frequencies. Because the cable acts like a microphone, some manufacturers offer an option that allows the operator to listen to fence noises causing the alarm. Operators can then determine whether the noises are naturally occurring sounds from wind or rain or are from an actual intrusion attempt.

- **Taut wire sensors.** Taut wire sensors combine a physically taut-wire barrier with an intrusion detection sensor network. The taut wire sensor consists of a column of uniformly spaced horizontal wires up to several hundred feet in length and securely anchored at each end. Typically, the wires are spaced 4 to 8 inches apart. Each is individually tensioned and attached to a detector located in a sensor post. Two types of detectors are commonly used, mechanical switches and strain gauges.
- **Fiber optic cable sensors.** Fiber optic cable sensors are functionally equivalent to the strain-sensitive cable sensors previously discussed. However, rather than electrical signals, modulated light is transmitted down the cable and the resulting received signals are processed to determine whether an alarm should be initiated. Because the cable contains no metal and no electrical signal is present, fiber optic sensors are generally less susceptible to electrical interference from lightning or other sources.
- **Capacitance proximity sensors.** Capacitance proximity sensors measure the electrical capacitance between the ground and an array of sense wires. Any variations in capacitance, such as that caused by an intruder approaching or touching one of the sense wires, initiates an alarm. These sensors usually consist of two or three wires attached to outriggers along the top of an existing fence, wall, or roof edge.

## **BURIED LINE SENSORS**

A buried line sensor system consists of detection probes or cable buried in the ground, typically between two fences that form an

isolation zone. These devices are wired to an electronic processing unit. The processing unit generates an alarm if an intruder passes through the detection field. Buried line sensors have several significant features:

- They are hidden, making them difficult to detect and circumvent.
- They follow the terrain's natural contour.
- They do not physically interfere with human activity, such as grass mowing or snow removal.
- They are affected by certain environmental conditions, such as running water and ground freeze/thaw cycles. (Seismic, seismic/magnetic, magnetic, and balanced pressure sensors are seldom used and will not be discussed herein.)

## **MICROWAVE SENSORS**

Microwave intrusion detection sensors are categorized as bistatic or monostatic. Bistatic sensors use transmitting and receiving antennas located at opposite ends of the microwave link, whereas monostatic sensors use the same antenna.

- A bistatic system uses a transmitter and a receiver that are typically separated by 100 to 1,200 feet and that are within direct LOS of each other.
- Monostatic microwave sensors use the same antenna or virtually coincident antenna arrays for the transmitter and receiver, which are usually combined into a single package.

## **INFRARED (IR) SENSORS**

The IR sensors are available in both active and passive models. An active sensor generates one or more near-IR beams that generate an alarm when interrupted. A passive sensor detects changes in thermal IR radiation from objects located within its field of view.

Active sensors consist of transmitter/receiver pairs. The transmitter contains an IR light source (such as a gallium arsenide light-emitting diode [LED]) that generates an IR beam. The light source is usually modulated to reduce the sensor's susceptibility to unwanted alarms resulting from sunlight or other IR light sources. The receiver detects changes in the signal power of the received beam. To minimize nuisance alarms from birds or blowing debris, the alarm criteria usually require that a high percentage of the beam be blocked for a specific interval of time.

## **VIDEO MOTION SENSORS**

Video motion sensors are available on most digital video recorders used in security applications. They can be programmed to activate alarms, initiate recording, or 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 in order 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.

## **ELECTRONIC ENTRY CONTROL**

The function of an entry control system is to ensure that only authorized personnel are permitted into or out of a controlled area. Entry can be controlled by locked fence gates, locked doors to a building or rooms within a building, or specially designed portals.

These means of entry control can be applied manually by guards or automatically by using entry control devices. In a manual system, guards verify that a person is authorized to enter an area, usually by comparing the photograph and personal characteristics of the individual requesting entry. In an automated system, the entry control device verifies that a person is authorized to enter or exit. The automated system usually interfaces with locking mechanisms on doors or gates that open momentarily to permit passage.

Mechanical hardware (e.g., locking mechanisms, electric door strikes, and specially designed portal hardware) and equipment used to detect contraband material (e.g., metal detectors, X-ray baggage-search systems, explosives detectors, and special nuclear-material monitors) are described in other documentation.

All entry control systems control passage by using one or more of three basic techniques (e.g., something a person knows, something a person has, or something a person is or does). Automated entry control devices based on these techniques are grouped into three categories: coded, credential, and biometric devices.

## **CODED DEVICES**

Coded devices operate on the principle that a person has been issued a code to enter into an entry control device. This code will match the code stored in the device and permit entry. Depending on the application, a single code can be used by all persons authorized to enter the controlled area or each authorized person can be assigned a unique code. Group codes are useful when the group is small and controls are primarily for keeping out the general public. Individual codes are usually required for control of entry to more critical areas. Coded devices verify the entered code's authenticity, and any person entering a correct code is authorized to enter the controlled area. Electronically coded devices include electronic and computer-controlled keypads.

**Electronic Keypad Devices.** The common telephone keypad (12 keys) is an example of an electronic keypad. This type of keypad consists of simple push-button switches that, when depressed, are decoded by digital logic circuits. When the correct sequence of buttons is pushed, an electric signal unlocks the door for a few seconds.

**Computer-controlled Keypad Devices.** These devices are similar to electronic keypad devices, except they are equipped with a microprocessor in the keypad or in a separate enclosure at a different location. The microprocessor monitors the sequence in which the

keys are depressed and may provide additional functions such as personal ID and digit scrambling. When the correct code is entered and all conditions are satisfied, an electric signal unlocks the door.

## **CREDENTIAL DEVICES**

A credential device identifies a person having legitimate authority to enter a controlled area. A coded credential (e.g., plastic card or key) contains a prerecorded, machine-readable code. An electric signal unlocks the door if the prerecorded code matches the code stored in the system when the card is read. Like coded devices, credential devices only authenticate the credential; it assumes a user with an acceptable credential is authorized to enter. The most commonly used types of cards are described as follows:

**Magnetic-stripe Card.** A strip of magnetic material located along one edge of the card is encoded with data (sometimes encrypted). The data is read by moving the card past a magnetic read head.

**Wiegand-effect Card.** The Wiegand-effect card contains a series of small-diameter, parallel wires approximately ½-inch long, embedded in the bottom half of the card. The wires are manufactured from ferromagnetic materials that produce a sharp change in magnetic flux when exposed to a slowly changing magnetic field. This type of card is impervious to accidental erasure. The card reader contains a small read head and a tiny magnet to supply the applied magnetic field. It usually does not require external power.

**Proximity Card.** A proximity card is not physically inserted into a reader; the coded pattern on the card is sensed when it is brought within several inches of the reader. Several techniques are used to code cards. One technique uses a number of electrically tuned circuits embedded in the card. Data are encoded by varying resonant frequencies of the tuned circuits. The reader contains a transmitter that continually sweeps through a specified range of frequencies and a receiver that senses the pattern of resonant frequencies contained in the card. Another technique uses an

integrated circuit embedded in the card to generate a code that can be magnetically or electro-statically coupled to the reader. The power required to activate embedded circuitry can be provided by a small battery embedded in the card or by magnetically coupling power from the reader.

**Smart Card.** A smart card is embedded with a microprocessor, memory, communication circuitry, and a battery. The card contains edge contacts that enable a reader to communicate with the microprocessor. Entry control information and other data may be stored in the microprocessor's memory.

**Bar Code.** A bar code consists of black bars printed on white paper or tape that can be easily read with an optical scanner. This type of coding is not widely used for entry control applications because it can be easily duplicated. It is possible to conceal the code by applying an opaque mask over it. In this approach, an IR scanner is used to interpret the printed code. For low-level security areas, the use of bar codes can provide a cost-effective solution for entry control. Coded strips and opaque masks can be attached to existing ID badges, alleviating the need for complete badge replacement.

## **BIOMETRIC DEVICES**

The third basic technique used to control entry is based on the measurement of one or more physical or personal characteristics of an individual. Because most entry control devices based on this technique rely on measurements of biological characteristics, they have become commonly known as biometric devices. Characteristics such as fingerprints, hand geometry, voiceprints, handwriting, and retinal blood-vessel patterns have been used for controlling entry. Typically, in enrolling individuals, several reference measurements are made of the selected characteristic and then stored in the device's memory or on a card. From then on, when that person attempts entry, a scan of the characteristic is compared with the reference data template. If a match is found, entry is granted. Rather than verifying an artifact, such as a code

or a credential, biometric devices verify a person's physical characteristic, thus providing a form of identity verification. Because of this, biometric devices are sometimes referred to as personnel identity verification devices. The most common biometric devices are discussed below.

**Fingerprints.** Fingerprint-verification devices use one of two approaches. One is pattern recognition of the whorls, loops, and tilts of the referenced fingerprint, which is stored in a digitized representation of the image and compared with the fingerprint of the prospective entrant. The second approach is minutiae comparison, which means that the endings and branching points of ridges and valleys of the referenced fingerprint are compared with the fingerprint of the prospective entrant.

**Hand Geometry.** Several devices are available that use hand geometry for personnel verification. These devices use a variety of physical measurements of the hand, such as finger length, finger curvature, hand width, webbing between fingers, and light transmissivity through the skin to verify identity. Both two- and three-dimensional units are available.

**Retinal Patterns.** This type of technique is based on the premise that the pattern of blood vessels on the human eye's retina is unique to an individual. While the eye is focused on a visual target, a low-intensity IR light beam scans a circular area of the retina. The amount of light reflected from the eye is recorded as the beam progresses around the circular path. Reflected light is modulated by the difference in reflectivity between blood-vessel pattern and adjacent tissue. This information is processed and converted to a digital template that is stored as the eye's signature. Users are allowed to wear contact lenses; however, glasses should be removed.



## MONITORING OF DESIGNATED RESTRICTED AREAS

A restricted area is any area that can be monitored by electronic devices and that is subject to special restrictions or controls for security reasons. Restricted areas may be established for the following:

- The enforcement of security measures and the exclusion of unauthorized personnel.
- Intensified controls in areas requiring special protection.
- The protection of classified information or critical equipment or materials.

## DEGREE OF SECURITY

The degree of security and control required depends on the nature, sensitivity, or importance of the security interest. Restricted areas are classified as controlled, limited, or exclusion areas:

**Controlled Area.** A controlled area is that portion of a restricted area usually near or surrounding a limited or exclusion area. Entry to the controlled area is restricted to personnel with a need for access. Movement of authorized personnel within this area is not necessarily controlled because mere entry to the area does not provide access to the security interest. The controlled area is provided for administrative control, for safety, or as a buffer zone for in-depth security for the limited or exclusion area.

**Limited Area .** A limited area is a restricted area within close proximity of a security interest. Uncontrolled movement may permit access to the item. Escorts and other internal restrictions may prevent access within limited areas.

**Exclusion Area.** An exclusion area is a restricted area containing a security interest. Uncontrolled movement permits direct access to the item.

There are other important considerations concerning restricted areas and their lines of division. These considerations include the following:

- A survey and analysis of the facility, its missions, and its security interests. This can determine immediate and anticipated needs that require protection. Anticipated needs are determined from plans for the future.
- The size and nature of the security interest being protected. Safes may provide adequate protection for classified documents and small items; however, large items may have to be placed within guarded enclosures.
- Some security interests are more sensitive to compromise than others. Brief observation or a simple act by an untrained person may constitute a compromise in some cases. In others, detailed study and planned action by an expert may be required.

**American Association of State Highway and Transportation Officials**

*A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*, May 2002 , The American Association of State Highway and Transportation Officials' Security Task Force, Washington, DC

<http://security.transportation.org/community/security/guides.html>

**The American Institute of Architects**

*Building Security Through Design: A Primer for Architects, Design Professionals, and their Clients*, November 2001, The American Institute of Architects (book)

<http://www.aia.org/security>

**American Institute of Chemical Engineers**

Pub No: G-79, *Guidelines for Analyzing and Managing the Security Vulnerabilities at Fixed Chemical Sites*, 2002, Center for Chemical Process Safety, ISBN No: 0-8169-0877-X

<http://www.aiche.org/ccpssecurity>

**American Medical Association**

*Physical injuries and fatalities resulting from the Oklahoma City bombing*, August 7, 1996, S. Mallonee, S. Shariat, G. Stennies, R. Waxweiler, D. Hogan, and F. Jordan., *The Journal of the American Medical Association*, Vol. 276 No. 5., pp 382-387

Abstract at URL:

<http://jama.ama-assn.org/cgi/content/abstract/276/5/382>

**American Society of Civil Engineers**

Architectural Engineering Institute of American Society of Civil Engineers, AEI Newsletter, *The Team, Special Terrorism Issue*, Fall 2001, Volume 4, Issue 3

[http://www.asce.org/pdf/aei\\_11\\_1.pdf](http://www.asce.org/pdf/aei_11_1.pdf)

*Blast Effects on Buildings: Design of Buildings to Optimize Resistance to Blast Loading*, 1995, G.C. Mays and P.D. Smith, London: Thomas Telford, Ltd., American Society of Civil Engineers, ISBN: 0-7277-2030-9  
<http://www.pubs.asce.org/BOOKdisplay.cgi?9990338>

*Blast Resistant Design of Commercial Buildings*, 1996, M. Ettouney, R. Smilowitz, and T. Rittenhouse, Practice Periodical on Structural Design and Construction, Vol. 1, No. 1, February 1996, American Society of Civil Engineers  
<http://ojps.aip.org/dbt/dbt.jsp?KEY=PPSCFX&Volume=1&Issue=1>  
A preprint of the final article is available at  
<http://www.wai.com/AppliedScience/Blast/blast-struct-design.html>

*Design of Blast Resistant Buildings in Petrochemical Facilities*, 1997, American Society of Civil Engineers, ISBN: 0-7844-0265-5  
<http://www.pubs.asce.org/BOOKdisplay.cgi?9704510>

*Glass-Related Injuries in Oklahoma City Bombing*, Journal of Performance of Constructed Facilities, May 1999, 13, No. 2, H Scott Norville, Natalie Harville, Edward J. Conrath, Sheryll Shariat, and Sue Mallonee  
<http://www.pubs.asce.org/WWWdisplay.cgi?9902006>

*Lessons from the Oklahoma City Bombing: Defensive Design Techniques*, January 1997, Eve E. Hinman and David J. Hammond, January 1997, American Society of Civil Engineers (ASCE Press), Reston, VA, ISBN: 0784402175  
<http://www.asce.org/publications/booksdisplay.cfm?type=9702295>

*Minimum Design Loads for Buildings and Other Structures, ASCE 7-02*, 2002, American Society of Civil Engineers, ISBN: 0-7844-0624-3 [Note revision of 7-98, does not include building security or antiterrorism, but covers all natural hazards]  
<http://www.pubs.asce.org/ASCE7.html?9991330>

Structural Engineering Institute of American Society of Civil Engineers, *Structural Design for Physical Security: State of the Practice*, 1999, Edward Conrath, et al., Reston, VA, Structural Engineering Institute of American Society of Civil Engineers  
<http://www.pubs.asce.org/BOOKdisplay.cgi?9990571>

*Vulnerability and Protection of Infrastructure Systems: The State of the Art*,  
An ASCE Journals Special Publication compiling articles from 2002  
and earlier available online

[https://ascestore.aip.org/OA\\_HTML/aipCCtpItmDspRte.jsp?a=b  
& item=39885](https://ascestore.aip.org/OA_HTML/aipCCtpItmDspRte.jsp?a=b&item=39885)

### **American Society of Heating, Refrigerating, and Air-Conditioning Engineers**

*Defensive Filtration*, ASHRAE Journal, December 2002, James D. Miller  
[http://resourcecenter.ashrae.org/store/ashrae/  
newstore.cgi?itemid= 9346&view=item&categoryid=409&page=1&l  
oginid=29483](http://resourcecenter.ashrae.org/store/ashrae/newstore.cgi?itemid=9346&view=item&categoryid=409&page=1&loginid=29483)

*Report of Presidential Ad Hoc Committee for Building Health and Safety  
under Extraordinary Incidents on Risk Management Guidance for Health,  
Safety and Environmental Security under Extraordinary Incidents*,  
Washington, DC, January 26, 2003  
<http://xp20.ashrae.org/about/extraordinary.pdf>

*Risk Management Guidance for Health and Safety under Extraordinary  
Incidents*, ASHRAE 2002 Winter Meeting Report, January 12, 2002  
<http://atfp.nfesc.navy.mil/pdf/ASHRAE%20CBR%20Guidance.pdf>  
or  
[http://engineering.tamu.edu/safety/guidelines/faclab/ASHRAE\\_  
Security\\_Rpt\\_12Jan02.pdf](http://engineering.tamu.edu/safety/guidelines/faclab/ASHRAE_Security_Rpt_12Jan02.pdf)

Standard 62-2001, *Ventilation for Acceptable Indoor Air Quality* (ANSI  
Approved), ISSN 1041-2336, addenda to basic ANSI/ASHRAE  
Standard 62 basic (1989)  
[http://resourcecenter.ashrae.org/store/ashrae/newstore.cgi?  
itemid= 6852&view=item&categoryid=311&page=1&loginid=29483](http://resourcecenter.ashrae.org/store/ashrae/newstore.cgi?itemid=6852&view=item&categoryid=311&page=1&loginid=29483)

### **Building Owners and Managers Association International**

*How to Design and Manage Your Preventive Maintenance Program*, 1996  
<http://www.boma.org/pubs/bomampm.htm>

## **Centers for Disease Control and Prevention/ National Institute for Occupational Safety and Health**

Publication No. 2002-139, *Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks*, May 2002, Cincinnati, OH  
<http://www.cdc.gov/niosh/bldvent/2002-139.html>

Publication No. 2003-136, *Guidance for Filtration and Air Cleaning Systems to Protect Building Environments from Airborne Chemical, Biological, or Radiological Attacks*, April 2003, Cincinnati, OH  
<http://www.cdc.gov/niosh/docs/2003-136/2003-136.html>

## **Central Intelligence Agency**

*Chemical, Biological, Radiological Incident Handbook*, October 1998  
[http://www.cia.gov/cia/publications/cbr\\_handbook/cbrbook.htm](http://www.cia.gov/cia/publications/cbr_handbook/cbrbook.htm)

## **Council on Tall Buildings and Urban Habitat**

*Building Safety Enhancement Guidebook*, 2002  
<http://www.ctbuh.org>

*Task Force on Tall Buildings: "The Future,"* October 15, 2001  
[http://www.lehigh.edu/ctbuh/htmlfiles/hot\\_links/report.pdf](http://www.lehigh.edu/ctbuh/htmlfiles/hot_links/report.pdf)  
or [http://www.ctbuh.org/htmlfiles/hot\\_links/report.pdf](http://www.ctbuh.org/htmlfiles/hot_links/report.pdf)

## **Federal Aviation Administration**

DOT/FAA/AR-00/52, *Recommended Security Guidelines for Airport Planning, Design and Construction*, Revised June 2001, Associate Administrator for Civil Aviation Security Office of Civil Aviation Security, Policy and Planning, Federal Aviation Administration, Washington, DC 20591 (not available on Internet)

FAA Order 1600.69A, *FAA Facility Security Management Program*, updated FAA Order 1600.69B to be published shortly – The Federal Aviation Administration’s criteria for the protection of its facilities. *[For Official Use Only]* (not available on Internet)

## **Federal Emergency Management Agency**

FEMA 152, *Seismic Considerations: Apartment Buildings, Earthquake Hazards Reduction Series 37*, November 1988, Washington, DC (not available on Internet) Contact FEMA Distribution Center, P.O. Box 2012, 8231 Stayton Drive, Jessup, MD 20794-2012, Telephone: 1-800-480-2520, Fax: 301-362-5335

FEMA 153, *Seismic Considerations: Office Buildings, Earthquake Hazards Reduction Series 38*, November 1988, Washington, DC (not available on Internet) Contact FEMA Distribution Center, P.O. Box 2012, 8231 Stayton Drive, Jessup, MD 20794-2012, Telephone: 1-800-480-2520, Fax: 301-362-5335

FEMA 154, *Rapid Visual Screening of Buildings for Seismic Hazards: A Handbook (2<sup>nd</sup> Edition)*, 2002, 1988, Washington, DC (not available on Internet) Contact FEMA Distribution Center, P.O. Box 2012, 8231 Stayton Drive, Jessup, MD 20794-2012, Telephone: 1-800-480-2520, Fax: 301-362-5335

FEMA 277, *The Oklahoma City Bombing: Improving Building Performance through Multi-Hazard Mitigation*, August 1, 1996, Washington, DC  
<http://www.fema.gov/mit/bpat/bpat009.htm>

FEMA 372, *Mitigation Resources for Success (CD-ROM)*, October 2001, Washington, DC  
[http://www.fema.gov/pdf/library/poster\\_fnl2.pdf](http://www.fema.gov/pdf/library/poster_fnl2.pdf)

FEMA 386-2, *Understanding Your Risks, Identifying Hazards and Estimating Losses*, August 2001  
[http://www.fema.gov/fima/planning\\_toc3.shtm](http://www.fema.gov/fima/planning_toc3.shtm)

FEMA 386-7, *Integrating Human-Caused Hazards Into Mitigation Planning*, September 2002  
<http://www.fema.gov/fima/antiterrorism/resources.shtm>

FEMA 403, *World Trade Center Building Performance Study: Data Collection, Preliminary Observations, and Recommendations*, May 2002, Washington, DC  
<http://www.fema.gov/library/wtcstudy.shtm>

State and Local Guide 101, *Guide for All-Hazard Emergency Operations Planning, Chapter 6, Attachment G, Terrorism*, April 2001

<http://www.fema.gov/rrr/allhzpln.shtm>

### **General Services Administration**

*Balancing Security and Openness: A Thematic Summary of a Symposium on Security and the Design of Public Buildings*, November 30, 1999

[http://hydra.gsa.gov/pbs/pc/gd\\_files/SecurityOpenness.pdf](http://hydra.gsa.gov/pbs/pc/gd_files/SecurityOpenness.pdf)

*Cost Impact of ISC Security Criteria*, GSA & Applied Research Associates, Inc., L. Bryant and J. Smith, Vicksburg, MS

**[Restricted Access]**

<http://www.oca.gsa.gov/specialphp/References.php>

*Facility Standards for the Public Building Service (PBS-P100)*; Chapter 8, Security Design, Revised November 2000

<http://hydra.gsa.gov/pbs/pc/facilitiesstandards/>

*Mail Center Manager's Security Guide – Second Edition*, October 22, 2002

[http://www.gsa.gov/attachments/GSA\\_PUBLICATIONS/extpub/MailCenterManagersSecurityGuideV2.pdf](http://www.gsa.gov/attachments/GSA_PUBLICATIONS/extpub/MailCenterManagersSecurityGuideV2.pdf)

Progressive Collapse Analysis and Design Guidelines for New Federal Office Buildings and Major Modernization Projects, November 2000 **[Restricted Access]**

<http://www.oca.gsa.gov/specialphp/References.php>

*Security Reference Manual, Part 3: Blast Design and Assessment*

Guidelines, July 31, 2001 **[For Official Use Only]** **[Restricted Access]**

<http://www.oca.gsa.gov/specialphp/References.php>

### **Healthy Building International, Inc.**

*Vulnerability Assessments and Counter Terrorist Protocols*

<http://www.healthybuildings.com/s2/vacbt.pdf>

### **Interagency Security Committee (executive agent - GSA)**

*ISC Security Design Criteria for New Federal Office Buildings and Major Modernization Projects*, May 28, 2001, **[For Official Use Only]**



*[Restricted Access]*

<http://www.oca.gsa.gov/specialphp/References.php>

### **Institute of Transportation Engineers**

*The Influence of Traffic Calming Devices upon Fire Vehicle Travel Times*,  
Michael A. Coleman, 1997, ITE Annual Meeting Compendium,  
1997 pp. 838-845

<http://webservices.camsys.com/fhwa/cmn/cmn33.htm>

*Split Speed Bump*, 1998, Kathy Mulder, Washington, DC, TE  
International Conference, 1998

<http://www.ite.org/traffic/documents/CCA98A33.pdf>

### **Lawrence Berkeley National Lab**

*Protecting Buildings From a Biological or Chemical Attack: actions to take  
before or during a release*. LBNL/PUB-51959, January 10, 2003

<http://securebuildings.lbl.gov/images/bldgadvice.pdf>

### **National Academy of Sciences**

*Combating Terrorism: Prioritizing Vulnerabilities and Developing  
Mitigation Strategies*, Project Identification Number: NAEP-R-02-01-  
A, National Academy of Engineering on-going project – results to  
be published.

[http://www4.nationalacademies.org/webcr.nsf/ProjectScopeDisplay/  
NAEP-R-02-01-A?OpenDocument](http://www4.nationalacademies.org/webcr.nsf/ProjectScopeDisplay/NAEP-R-02-01-A?OpenDocument)

### **National Capital Planning Commission**

*Designing for Security in the Nation's Capital*, October 2001

[http://www.ncpc.gov/planning\\_init/security/DesigningSec.pdf](http://www.ncpc.gov/planning_init/security/DesigningSec.pdf)

*The National Capital Planning Urban Design and Security Plan*,  
October 2002

<http://www.ncpc.gov/publications/udsp/Final%20UDSP.pdf>

### **National Institute of Building Sciences**

*Whole Building Design Guide: Provide Security for Building Occupants and Assets*

<http://www.wbdg.org/design/index.php?cn=2.7.4&cx=0>

### **National Research Council**

*Protecting Buildings and People from Terrorism: Technology Transfer for Blast-effects Mitigation*, 2001, National Academy Press, Washington, DC, ISBN 0-309-08286-2

<http://books.nap.edu/books/0309082862/html/index.html>

*Protecting Buildings From Bomb Blast, Transfer of Blast-Effects Mitigation Technologies from Military to Civilian Applications*, 1995, National Academy Press, Washington, DC, ISBN 0-309-05375-7

<http://books.nap.edu/books/0309053757/html/index.html>

*Protection of Federal Office Buildings Against Terrorism*, 1988, Committee on the *Protection of Federal Facilities Against Terrorism*, Building Research Board, National Academy Press, Washington, DC, ISBN 0-309-07691-9

<http://books.nap.edu/books/0309076463/html/index.html>

### **Society of American Military Engineers**

National Symposium of Comprehensive Force Protection, October 2001, Charleston, SC, Lindbergh & Associates. For a list of participants, access

<http://www.same.org/forceprot/force.htm>

### **Technical Support Working Group (TSWG)**

*Terrorist Bomb Threat Stand-Off Card with Explanation of Use*

[http://www.tswg.gov/tswg/prods\\_pubs/newBTSCPress.htm](http://www.tswg.gov/tswg/prods_pubs/newBTSCPress.htm)

### **The House National Security Committee**

Statement of Chairman Floyd D. Spence on the Report of the Bombing of Khobar Towers, August 1996, Washington, DC

<http://www.house.gov/hasc/Publications/104thCongress/Reports/saudi.pdf>

## **U.S. Air Force**

ESL-TR-87-57, *Protective Construction Design Manual*, November 1989; Contact Airbase Technologies Division (AFRL/MLQ) at Tyndall Air Force Base, FL, via e-mail to [techinfo@afrl.af.mil](mailto:techinfo@afrl.af.mil). [Superseded by Army Technical Manual TM 5-855-1 (Air Force Pamphlet AFPAM 32-1147(I), Navy Manual NAVFAC P-1080, DSWA Manual DAHSCWEMAN-97), December 1997]

*Expedient Hardening Methods for Structures Subjected to the Effect of Nonnuclear Munitions*, October 1990, Wright Laboratory Report (not available on Internet)

*Installation Entry Control Facilities Design Guide*, October 2002, Air Force Center for Environmental Excellence  
<http://www.afcee.brooks.af.mil/dc/dcd/gate/index.html>

*Installation Force Protection Guide*, 1997, Air Force Center for Environmental Excellence  
<http://www.afcee.brooks.af.mil/dc/dcd/arch/force.pdf>

*Vehicle Bomb Mitigation Guide*, July 1, 1999, Force Protection Battlelab [**For Official Use Only**] Contact the USAF Force Protection Battlelab, Lackland Air Force Base, TX, Telephone: (210)671-0058

## **U.S. Army**

### **Field Manuals (FM)**

FM 3-19.30, *Physical Security*, January 8, 2001, Washington, DC  
<http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/3-19.30/fm3-19.30.pdf>  
or  
[http://www.wood.army.mil/mpdoctrine/PDF\\_Files/FM\\_3-19.30.pdf](http://www.wood.army.mil/mpdoctrine/PDF_Files/FM_3-19.30.pdf)

FM 5-114, *Engineer Operations Short of War*, July 13, 1992  
<http://155.217.58.58/cgi-bin/atdl.dll/fm/5-114/toc.htm>

Technical Instruction 853-01 (Draft), *Protecting Buildings and Their Occupants from Airborne Hazards*, October 2001  
[http://buildingprotection.sbcom.army.mil/basic/airborne\\_hazards](http://buildingprotection.sbcom.army.mil/basic/airborne_hazards)

## **U.S. Army Corps of Engineers**

### **Engineer Technical Letters (ETL)**

ETL 1110-3-494, *Airblast Protection Retrofit for Unreinforced Concrete Masonry Walls*, July 14, 1999 [**Restricted Access**]  
<http://www.usace.army.mil/inet/usace-docs/eng-tech-ltrs>

ETL 1110-3-495, *Estimating Damage to Structures from Terrorist Bombs Field Operations Guide*, July 14, 1999 [**Restricted Access**]  
<http://www.usace.army.mil/inet/usace-docs/eng-tech-ltrs>

ETL 1110-3-498, *Design of Collective Protection Shelters to Resist Chemical, Biological, and Radiological (CBR) Agents*, February 24, 1999  
<http://www.usace.army.mil/inet/usace-docs/eng-tech-ltrs>

ETL 1110-3-501, *Window Retrofit Using Fragment Retention Film with Catcher Bar System*, July 14, 1999 [**Restricted Access**]  
<http://www.usace.army.mil/inet/usace-docs/eng-tech-ltrs>

### **Protective Design – Mandatory Center of Expertise – Technical Reports**

PDC-TR-91-6, *Blast Analysis Manual, Part 1 – Level of Protection Assessment Guide*, July 1991 [**For Official Use Only**]  
Contact U.S. Army Corps of Engineers Protective Design Center, ATTN: CENWO-ED-ST, 215 N. 17th Street, Omaha, NE 68102-4978, Telephone: (402)221-4918

### **Technical Manuals (TM)**

TM 5-853-1, *Security Engineering Project Development*, May 12, 1994, also Air Force Manual 32-1071, Volume 1  
**[For Official Use Only]**  
<http://www.usace.army.mil/inet/usace-docs/armytm>

TM 5-853-2, *Security Engineering Concept Design*, May 12, 1994, also Air Force Manual 32-1071, Volume 2  
**[For Official Use Only]**  
<http://www.usace.army.mil/inet/usace-docs/armytm>

TM 5-853-3, *Security Engineering Final Design*, May 12, 1994, also Air Force Manual 32-1071, Volume 3

*[For Official Use Only]*

<http://www.usace.army.mil/inet/usace-docs/armytm>

TM 5-853-4, *Security Engineering Electronic Security Systems*,  
May 12, 1994

<http://www.usace.army.mil/inet/usace-docs/armytm>

TM 5-855-4, *Heating, Ventilation, and Air Conditioning of  
Hardened Installations*, November 28, 1986

<http://www.usace.army.mil/inet/usace-docs/armytm/tm5-855-4/toc.htm>

TM 5-1300, *Structures to Resist Accidental Explosions*,  
November 19, 1990, (also Navy NAVFAC (Naval Facilities)  
P-397, Air Force Regulation 88-2); Contact David Hyde,  
U.S. Army Engineer Research and Development Center,  
3909 Halls Ferry Road, Vicksburg, MS 39180 or via e-mail  
to [hyded@ex1.wes.army.mil](mailto:hyded@ex1.wes.army.mil)

## **U.S. Department of Commerce**

### **Administrative Orders (DAO)**

DAO 206-5, *Occasional Use of Public Areas in Public Buildings*,  
December 9, 1986

<http://www.osec.doc.gov/bmi/daos/206-5.htm>

DAO 207-1, *Security Programs*, June 24, 1991, Amended  
September 6, 1991

<http://www.osec.doc.gov/bmi/daos/207-1.htm>

### **Critical Infrastructure Assurance Office**

*Vulnerability Assessment Framework 1.1*, October 1998

<http://www.ciao.gov/resource/vulassessframework.pdf>

*Practices For Securing Critical Information Assets*, January 2000

[http://www.ciao.gov/resource/Practices\\_For\\_Securing\\_Critical\\_Information\\_Assets.pdf](http://www.ciao.gov/resource/Practices_For_Securing_Critical_Information_Assets.pdf)

## **U.S. Department of Defense**

*DoD Security Engineering Manual* [Expected to have a major portion for public distribution once published as Unified Facilities Criteria and a smaller portion For Official Use Only similar to the UFC for AT Standards for Buildings listed below. This publication will replace Army Technical Manual 5-853 (Air Force Joint Manual 32-1071), Volumes 1, 2, and 3 and Navy Military Handbook 1013/1A]

DoD O-2000.12-H, *Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence: Mandatory Standards and Implementing Guidance, with Changes 1 and 2*, February 1993, Change 1 — May 21, 1993, Change 2 – October 3, 1997  
**[For Official Use Only]**

<http://www.dtic.mil/whs/directives/corres/pub1.html>

Force Protection Equipment Demonstration IV, 6-8 May 2003  
<http://www.fped4.org>

*Interim Antiterrorism/Force Protection Construction Standards*, December 16, 1999 **[For Official Use Only]** Contact U.S. Army Engineer District, Omaha, NE ATTN: CENWO-ED-ST, 215 North 17<sup>th</sup> Street, Omaha, NE 68102-4978, Telephone: (402)221-4918.

*Interim Antiterrorism/Force Protection Construction Standards—Progressive Collapse Guidance*, April 4, 2000 (not available on Internet) Contact U.S. Army Corps of Engineers Protective Design Center, ATTN: CENWO-ED-ST, 215 N. 17th Street, Omaha, NE 68102-4978, Telephone: (402)221-4918

### **Unified Facilities Criteria (UFC)**

UFC 3-340-01, *Design and Analysis of Hardened Structures to Conventional Weapons Effects*, June 30, 2002  
**[For Official Use Only]** [Formerly Army TM 5-855-1]  
<http://www.hnd.usace.army.mil/techinfo/ufc/UFC3-340-01 WEB.PDF>

UFC 4-010-01, *DoD Minimum Antiterrorism Standards for Buildings*, July 31, 2002  
<http://www.wbdg.org/ccbref/ccbdoc.php?category=ufc&docid=106&ref=1>

## Unified Facilities Guide Specifications (UFGS)

UFGS-02821A, *Fencing*, February 2002

<http://www.ccb.org/ufgs/pdf/02821A.pdf>

UFGS-02840A, *Active Vehicle Barriers*, February 2002

<http://www.ccb.org/ufgs/pdf/02840A.pdf>

UFGS-02841N, *Traffic Barriers*, August 2001

<http://www.ccb.org/ufgs/pdf/02841N.pdf>

UFGS-08390A, *Blast Resistant Doors*, April 2001

<http://www.ccb.org/ufgs/pdf/08390.pdf>

UFGS-08581, *Blast Resistant Tempered Glass Windows*,  
August 2001

<http://www.ccb.org/ufgs/pdf/08581.pdf>

UFGS-08840A, *Plastic Glazing*, July 1995

<https://www.ccb.org/ufgs/pdf/08840A.pdf>

UFGS-08850, *Fragment Retention Film for Glass*, July 1992

<https://www.ccb.org/ufgs/pdf/08850.pdf>

UFGS-11020, *Security Vault Door*, August 2002

<http://www.ccb.org/ufgs/pdf/11020.pdf>

UFGS-11025, *Forced Entry Resistant Components*, August 2001

<http://www.ccb.org/ufgs/pdf/11025.pdf>

UFGS-11035, *Bullet-Resistant Components*, April 2000

<http://www.ccb.org/ufgs/pdf/11035.pdf>

UFGS-13095A, *Electromagnetic (EM) Shielding*, July 2001

<http://www.ccb.org/ufgs/pdf/13095A.pdf>

UFGS-13420A, *Self-Acting Blast Valves*, November 1997

<http://www.ccb.org/ufgs/pdf/13420A.pdf>

## U.S. Department of Energy

DOE/TIC 11268, *A Manual for the Prediction of Blast and Fragment Loadings on Structures*, February 1992, Albuquerque, NM, Southwest Research Institute [not available on Internet]

## **U.S. Department of Homeland Security**

*National Strategy for Homeland Security*, July 2002

[http://www.dhs.gov/interweb/assetlibrary/nat\\_strat\\_hls.pdf](http://www.dhs.gov/interweb/assetlibrary/nat_strat_hls.pdf)

*The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, February 2003

[http://www.dhs.gov/interweb/assetlibrary/Physical\\_Strategy.pdf](http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf)

National Strategy to Secure Cyberspace, February 2003

[http://www.dhs.gov/interweb/assetlibrary/National\\_Cyberspace\\_Strategy.pdf](http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf)

*President's Homeland Security Advisory Council - Statewide Template Initiative*, March 2003

[http://www.dhs.gov/interweb/assetlibrary/Statewide\\_Template\\_Initiative.pdf](http://www.dhs.gov/interweb/assetlibrary/Statewide_Template_Initiative.pdf)

*State and Local Actions for Homeland Security*, July 2002

[http://www.whitehouse.gov/homeland/stateandlocal/State\\_and\\_Local\\_Actions\\_for\\_Homeland\\_Security.pdf](http://www.whitehouse.gov/homeland/stateandlocal/State_and_Local_Actions_for_Homeland_Security.pdf)

## **U.S. Department of Housing and Urban Development**

*The Avoidance of Progressive Collapse, Regulatory approaches to the problem*, PB-248 781, October 1975, Division of Energy, Building Technology and Standards, Office of Policy Development and Research, Washington, DC 20410 (not available on Internet)

*Creating Defensible Space*, April 1996, Oscar Newman, Washington, DC

<http://www.huduser.org>

## **U.S. Department of Justice**

### **Federal Bureau of Investigation (FBI)**

*Terrorism in the United States, 1999*, Washington, DC, Counterterrorism Division

<http://www.fbi.gov/publications.htm>



## Office of Domestic Preparedness (ODP)

*Fiscal Year 1999 State Domestic Preparedness Equipment Program, Assessment and Strategy Development Tool Kit*, NCJ181200, May 15, 2000, [**For Official Use Only**]  
<http://www.ojp.usdoj.gov/odp/docs/assessment.txt>

## National Institute of Justice (NIJ)

*The Appropriate and Effective Use of Security Technologies in U.S. Schools: A Guide for Schools and Law Enforcement Agencies*, September 1999, with U.S. Department of Education, Safe and Drug-Free Schools Program; and U.S. Department of Energy, Sandia National Laboratories  
<http://www.ncjrs.org/school/home.html>

NIJ Guide 100-00, *Guide for the Selection of Chemical Agent and Toxic Industrial Material Detection Equipment for Emergency First Responders*, June 2000  
<http://www.ncjrs.org/pdffiles1/nij/184449.pdf>

NIJ Guide 101-00, *An Introduction to Biological Agent Detection Equipment for Emergency First Responders*, December 2001  
<http://www.ncjrs.org/pdffiles1/nij/190747.pdf>

NIJ Guide 102-00, *Guide for the Selection of Personal Protective Equipment for Emergency First Responders*, Volumes I-IV, November 2002  
<http://www.ncjrs.org/pdffiles1/nij/191518.pdf>

NIJ Guide 602-00, *Guide to the Technologies of Concealed Weapon and Contraband Imaging and Detection*, February 2001  
<http://www.ncjrs.org/pdffiles1/nij/184432.pdf>

NIJ Standard 0108.01, *Blast Resistant Protective Materials*, September 1985 [**Subscription Required**]  
<http://www.ccb.org>

*Crime Prevention Through Environmental Design and Community Policing*, August 1996, Dan Fleissner and Fred Heinzelmann, Washington, DC

<http://www.ncjrs.org/pdffiles/crimepre.pdf>

*Crime Prevention Through Environmental Design in Parking Facilities*, April 1996, Mary S. Smith, Washington, DC

<http://www.ncjrs.org/pdffiles/cptedpkg.pdf>

*“Designing Out” Gang Homicides and Street Assaults*, November 1998, James Lasley, Washington, DC

<http://www.ncjrs.org/pdffiles/173398.pdf>

*The Expanding Role of Crime Prevention Through Environmental Design in Premises Liability*, April 1996, Corey L. Gordon and William Brill Washington, DC

<http://www.ncjrs.org/pdffiles/cptedlia.pdf>

*Physical Environment and Crime*, January 1996, Ralph B. Taylor and Adele V. Harrell, Washington, DC

<http://www.ncjrs.org/pdffiles/physenv.pdf>

*Visibility and Vigilance: Metro’s Situational Approach to Preventing Subway Crime*, November 1997, Nancy G La Vigne, Washington, DC

<http://www.ncjrs.org/pdffiles/166372.pdf>

#### **U.S. Marshals Service**

*Vulnerability Assessment of Federal Facilities*, June 28, 1995

**[Restricted Access]**

<http://www.oca.gsa.gov>

#### **U.S. Department of State, Bureau of Diplomatic Security**

*Architectural Engineering Design Guidelines* (5 Volumes), March 1998  
**[For Official Use Only]** (not available on Internet)

Certification Standard SD-STD-01.01, Revision G (Amended),  
*Forced Entry and Ballistic Resistance of Structural Systems*, Amended

April 30, 1993 [Subscription Required]

<http://www.ccb.org>

*Patterns of Global Terrorism, 2002*, April 2002, Washington, DC

<http://www.state.gov/s/ct/rls/pgtrpt/2002/pdf/>

*Physical Security Standards Handbook*, January 7, 1998 [**For Official Use Only**] (not available on Internet)

*Structural Engineering Guidelines for New Embassy Office Buildings*, August 1995 [**For Official Use Only**] (not available on Internet)

*The Report of the Accountability Review Board on the Embassy Bombings in Nairobi and Dar es Salaam on August 7, 1998*, January 1999, Washington, DC

[http://www.state.gov/www/regions/africa/accountability\\_report.html](http://www.state.gov/www/regions/africa/accountability_report.html)

### **U.S. Department of the Treasury/Bureau of Alcohol, Tobacco, and Firearms**

*Vehicle Bomb Explosion Hazard And Evacuation Distance Tables*, 1999, request in writing, address information available at

[http://www.atf.treas.gov/pub/fire-explo\\_pub/i54001.htm](http://www.atf.treas.gov/pub/fire-explo_pub/i54001.htm)

### **U.S. Department of Veterans Affairs**

*Physical Security Assessment of Veterans Affairs Facilities*,

Recommendations of the National Institute of Building Sciences Task Group to the Department of Veterans Affairs, 6 September 2002

<http://www.va.gov/facmgt/standard/etc/vaphysicalsecurityreport.pdf>

### **U.S. Fire Administration (USFA of FEMA)**

*The Critical Infrastructure Protection Process Job Aid*, May 1, 2002

<http://www.usfa.fema.gov/dhtml/fire-service/cipc-jobaid.cfm>

### **U.S. Navy**

**Design Manuals (DM) NAVFAC (Naval Facilities Command)**

NAVFAC DM 2.08, *Blast Resistant Structures*, December 1986

<http://www.wbdg.org/ccbref/ccbdoc.php?category=nav&docid=46&ref=1>

NAVFAC DM 13.02, *Commercial Intrusion Detection Systems (IDS)*, September 1986  
<http://www.wbdg.org/ccbref/ccbdoc.php?category=nav&docid=47&ref=1>

**Interim Technical Guidance (ITG) 03-03, *Entry Control Facilities***, 20 February 2003  
[http://www.lantdiv.navfac.navy.mil/servlet/page?pageid=8609,8611&\\_dad=lantdiv&\\_schema=LANTDIV&11435\\_ACTIVE\\_1777132.p\\_subid=60007&11435\\_ACTIVE\\_1777132.p\\_sub\\_siteid=51&11435\\_ACTIVE\\_1777132.p\\_edit=0](http://www.lantdiv.navfac.navy.mil/servlet/page?pageid=8609,8611&_dad=lantdiv&_schema=LANTDIV&11435_ACTIVE_1777132.p_subid=60007&11435_ACTIVE_1777132.p_sub_siteid=51&11435_ACTIVE_1777132.p_edit=0)

### **Military Handbooks (MIL-HDBK)**

MIL-HDBK-1002/1, *Structural Engineering General Requirements*, November 30, 1987  
<http://www.wbdg.org/ccbref/ccbdoc.php?category=nav&docid=48&ref=1>

MIL-HDBK-1004/4, *Electrical Utilization Systems*, October 13, 1987  
<http://www.wbdg.org/ccbref/ccbdoc.php?category=nav&docid=49&ref=1>

MIL-HDBK-1012/3, *Telecommunications Premises Distribution Planning, Design, and Estimating*, May 31, 1996  
<http://www.wbdg.org/ccbref/ccbdoc.php?category=nav&docid=50&ref=1>

MIL-HDBK-1013/1A, *Design Guidelines for Physical Security of Fixed Land-Based Facilities*, December 15, 1993. For copies, contact Defense Printing Service, Building 40, 700 Robbins Avenue, Philadelphia, PA 19111-5094, Telephone: (215)697-2179, Fax: (215)697-1462 or available on the National Institute of Building Sciences' Construction Criteria Base

MIL-HDBK-1013/10, *Design Guidelines for Security Fencing, Gates, Barriers, and Guard Facilities*, May 14, 1993. For copies, contact Defense Printing Service, Building 40, 700

Robbins Avenue, Philadelphia, PA 19111-5094, Telephone: (215)697-2179, Fax: (215) 697-1462 or available on the National Institute of Building Sciences' Construction Criteria Base

MIL-HDBK-1013/12, *Evaluation of Security Glazing for Ballistic, Bomb, and Forced Entry Tactics*, March 10, 1997. For copies, contact Defense Printing Service, Building 40, 700 Robbins Avenue, Philadelphia, PA 19111-5094, Telephone: (215)697-2179, Fax: (215) 697-1462 or available on the National Institute of Building Sciences' Construction Criteria Base

MIL-HDBK-1013/14, *Selection and Application of Vehicle Barriers*, February 1, 1999. For copies, contact Defense Printing Service, Building 40, 700 Robbins Avenue, Philadelphia, PA 19111-5094, Telephone: (215)697-2179, Fax: (215)697-1462 or available on the National Institute of Building Sciences' Construction Criteria Base

**TechData Sheets – Naval Facilities Engineering Service Center (NFESC)**

TDS-2062-SHR, *Estimating Damage to Structures from Terrorist Bombs*, September 1998 [**For Official Use Only**] Requests for publication can be made to Naval Facilities Engineering Service Center, Security Engineering Division (ESC66), 1100 23rd Ave, Port Hueneme, CA 93043-4370, Telephone (805)982-1582 (Primary), (805)982-4817 (Alternate); Fax: (805)982-1253

TDS-2063-SHR, *Blast Shielding Walls*, September 1998 [**For Official Use Only**] Requests for publication can be made to Naval Facilities Engineering Service Center, Security Engineering Division (ESC66), 1100 23rd Ave., Port Hueneme, CA 93043-4370, Telephone: (805)982-1582 (Primary), (805)982-4817 (Alternate); Fax: (805)982-1253

TDS-2079-SHR, *Planning and Design Considerations for Incorporating Blast Mitigation in Mailrooms*, May 2000. For copies, contact Defense Printing Service, Building 40, 700

Robbins Avenue, Philadelphia, PA 19111-5094, Telephone:  
(215)697-2179, Fax: (215) 697-1462

TDS-2090-SHR, *Design Parameters for a Controlled Entry Point*.  
For copies, contact Defense Printing Service, Building  
40, 700 Robbins Avenue, Philadelphia, PA 19111-5094,  
Telephone: (215)697-2179, Fax: (215)697-1462

### **User Guides — Naval Facilities Engineering Service Center (NFESC)**

UG-2030-SHR, *Security Glazing Applications*, May 1998,  
distributed June 25, 1998. [**For Official Use Only**] Requests  
for publication can be made to Naval Facilities Engineering  
Service Center, Security Engineering Division (ESC66),  
1100 23rd Ave., Port Hueneme, CA 93043-4370, Telephone:  
(805)982-1582 (Primary), (805) 982-4817 (Alternate); Fax:  
(805)982-1253

UG-2031-SHR, *Protection Against Terrorist Vehicle Bombs*, May  
1998, distributed June 25, 1998. [**For Official Use Only**]  
Requests for publication can be made to Naval Facilities  
Engineering Service Center, Security Engineering Division  
(ESC66), 1100 23rd Ave, Port Hueneme, CA 93043-4370,  
Telephone: (805)982-15.82 (Primary), (805) 982-4817  
(Alternate); Fax: (805)982-1253

### **Other Books, Magazines, Magazine Articles, and Newspaper Articles**

Archibald, Rae W., et al., 2002, *Security and Safety in Los Angeles  
High-Rise Buildings after 9/11*. RAND, Santa Monica, CA,  
ISBN: 0-8330-3184-8  
<http://www.rand.org/publications/DB/DB381>

Atlas, Randall I., June 1998, *Designing for Crime and Terrorism*, *Security  
and Technology Design*, Security Technology and Design Magazine  
Reprint Services, Jim Benesh, Telephone: (800)547-7377 x324, Fax:  
(920)568-2244, e-mail: [jim.benesh@cygnuspub.com](mailto:jim.benesh@cygnuspub.com)

Broder, James F., December 15, 1999, *Risk Analysis and the Security Survey, 2nd Edition*, Butterworth-Heinemann, Stoneham, MA, ISBN: 0750670894

Craighead, Geoff, December 2002, *High-Rise Security and Fire Life Safety, 2nd Edition*, Academic Press, ISBN: 0750674555

Crowe, Timothy D., 2000, *Crime Prevention Through Environmental Design: Applications Of Architectural Design And Space Management Concepts (2nd Edition)*, Stoneham, MA, Butterworth-Heinemann, ISBN: 075067198X

Fehr, Stephen C., July 1996, Parking Under Siege in D.C.: U.S. Anti-Terrorism Plan Threatens 360 Spaces, *The Washington Post*, July 13, 1996  
<http://www.washingtonpost.com/wp-adv/archives/advanced.htm>

Fenelly, Lawrence J., June 1997, *Effective Physical Security, 2nd Edition*, Stoneham, MA, Butterworth-Heinemann, ISBN: 0-75-069873-X

Garcia, Mary Lynn, February 23, 2001, *The Design and Evaluation of Physical Protection Systems*, Stoneham, MA, Butterworth-Heinemann, ISBN: 0750673672

Gonchar, Joann, March 2002, Building for a Secure Future: Government Facilities under way incorporate already tough standards, *Engineering News-Record*, March 25, 2002  
<http://www.construction.com/NewsCenter/Headlines/ENR/20020325e.asp>

Greene, R.W., October 2002, *Confronting Catastrophe: A GIS Handbook*, ESRI Press, ISBN: 1589480406

Hart, Sara, March 2002, In the aftermath of September 11, the urban landscape appears vulnerable and random: Architects and consultants focus on risk assessment and security through design, *Architectural Record*, March 2002  
[http://archrecord.construction.com/CONTEduc/ARTICLES/03\\_02\\_1.asp](http://archrecord.construction.com/CONTEduc/ARTICLES/03_02_1.asp)

Kowalski, Wladyslaw Jan, P.E., Ph.D., September 26, 2002, *Immune Building Systems Technology*, McGraw-Hill Professional, ISBN: 0-07-140246-2

Nadel, Barbara A, March 1998, Designing for Security, *Architectural Record*, March 1998

[http://www.archrecord.com/CONTEDEC/ARTICLES/3\\_98\\_1.asp](http://www.archrecord.com/CONTEDEC/ARTICLES/3_98_1.asp)

Owen, David D. and R.S.Means Engineering Staff, *Building Security: Strategies and Costs*, Construction Publishers & Consultants, ISBN: 0-87629-698-3, 2003

Pearson, Robert, September 1997, *Security through Environmental Design, Security and Technology Design*, Security Technology and Design Magazine Reprint Services, Jim Benesh, Telephone: (800) 547-7377 x324; Fax: (920) 568-2244; e-mail: [jim.benesh@cygnuspub.com](mailto:jim.benesh@cygnuspub.com)

Rochon, Donald M., June 1998, *Architectural Design for Security, Security and Technology Design*, Security Technology and Design Magazine Reprint Services, Jim Benesh, Telephone: (800)547-7377 x324; Fax: (920)568-2244; e-mail: [jim.benesh@cygnuspub.com](mailto:jim.benesh@cygnuspub.com)

Security Magazine [on-line magazine]

<http://www.securitymagazine.com>

Security Solutions Online: Access Control and Security Systems [on-line magazine] <http://securitysolutions.com/>

Security Technology and Design [on-line and print magazine]

<http://www.st-and-d.com>

Sidell, Frederick R., et al, 1998, *Jane's Chem-Bio Handbook*, Jane's Information Group, Alexandria, VA, ISBN 0-7106 2568-5

[http://www.janes.com/company/catalog/chem\\_bio\\_hand.shtml](http://www.janes.com/company/catalog/chem_bio_hand.shtml)

Smith, Keith, November 2000, *Environmental Hazards: Assessing Risk and Reducing Disaster*, Routledge, New York, NY, ISBN 0415224632

<http://www.routledge-ny.com/books.cfm?isbn=0415224632>



- American Lifelines Alliance  
<http://www.americanlifelinesalliance.org>
- Applied Technology Council  
<http://www.atcouncil.org>
- Battelle Memorial Institute, National Security Program  
<http://www.battelle.org/natsecurity/default.stm>
- Center for Strategic and International Studies (CSIS)  
<http://www.csis.org>
- Centers for Disease Control and Prevention (CDC)/National Institute for Occupational Safety and Health (NIOSH)  
<http://www.cdc.gov/niosh>
- Central Intelligence Agency (CIA)  
<http://www.cia.gov>
- Council on Tall Buildings and Urban Habitat (CTBUH)  
<http://www.ctbuh.org>
- Federal Aviation Administration (FAA)  
<http://www.faa.gov>
- Healthy Buildings International, Inc.  
<http://www.healthybuildings.com>
- Institute of Transportation Engineers  
<http://www.ite.org>
- Interagency Security Committee (ISC) led by the U.S. General Services Administration [*Restricted Access*]  
<http://www.oca.gsa.gov>
- International CPTED [Crime Prevention Through Environmental Design] Association (ICA)  
<http://new.cpted.net/home.amt>
- Lawrence Berkeley National Laboratory (LBNL)  
<http://securebuildings.lbl.gov>

- National Academy of Sciences  
<http://www4.nationalacademies.org/nas/nashome.nsf>
  - Federal Facilities Council (FFC) Standing Committee on Physical Security and Hazard Mitigation  
[http://www7.nationalacademies.org/ffc/Physical\\_Security\\_Hazard\\_Mitigation.html](http://www7.nationalacademies.org/ffc/Physical_Security_Hazard_Mitigation.html)
  - National Research Council  
<http://www.nationalacademies.org/nrc>
- National Defense Industrial Association (NDIA)  
<http://www.ndia.org>
- Public Entity Risk Institute  
<http://www.riskinstitute.org>
- Security Design Coalition  
<http://www.designingforsecurity.org>
- Security Industry Association (SIA)  
<http://www.siaonline.org/>
- Technical Support Working Group  
(Departments of Defense and State)  
<http://www.tswg.gov>
- U.S. Air Force Electronic System Center (ESC),  
Hanscom Air Force Base  
<http://eschq.hanscom.af.mil/>
- U.S. Army Soldiers and Biological Chemical Command  
(SBCCOM): Basic Information on Building Protection  
<http://buildingprotection.sbccom.army.mil>
- U.S. Department of Justice  
<http://www.usdoj.gov>
  - Federal Bureau of Investigation: Terrorism in the United States reports  
<http://www.fbi.gov/publications/terror/terroris.htm>
  - National Institute of Justice (NIJ)  
<http://www.ojp.usdoj.gov/nij>

- Office of Domestic Preparedness (ODP)  
<http://www.ojp.usdoj.gov/odp>
- U.S. Marshals Service (USMS)  
<http://www.usdoj.gov/marshals>

## **The Infrastructure Security Partnership (TISP)**

<http://www.tisp.org>

### **Founding Organizations**

- American Council of Engineering Companies (ACEC)  
<http://www.acec.org>
- The American Institute of Architects (AIA), Security Resource Center  
<http://www.aia.org/security>
- American Society of Civil Engineers (ASCE)  
<http://www.asce.org>
  - Architectural Engineering Institute (AEI) of ASCE  
<http://www.asce.org/instfound/aei.cfm>
  - Civil Engineering Research Foundation (CERF) of ASCE  
<http://www.cerf.org>
  - Structural Engineering Institute (SEI) of ASCE  
<http://www.seinstitute.org>
- Associated General Contractors of America  
<http://www.agc.org>
- Construction Industry Institute  
<http://construction-institute.org>
- Federal Emergency Management Agency (FEMA)  
<http://www.fema.gov>
  - Building Performance Assessment Team  
<http://www.fema.gov/mit/bpat>
  - Human Caused Hazards  
<http://www.fema.gov/hazards>

- Mitigation Planning  
<http://www.fema.gov/fima/planning.shtm>
- Federal Facilities Council – See National Academy of Sciences
- National Institute of Standards and Technology (NIST),  
Building and Fire Research Laboratory  
<http://www.bfrl.nist.gov>
- Naval Facilities Engineering Command  
<http://www.navfac.navy.mil>
  - Naval Facilities Engineering Service Center (NFESC),  
Security Engineering Center of Expertise ESC66  
<http://atfp.nfesc.navy.mil>
- Society of American Military Engineers (SAME)  
<http://www.same.org>
- U.S. Army Corps of Engineers  
<http://www.usace.army.mil>
  - Blast Mitigation Action Group, U.S. Army Corps of  
Engineers Center of Expertise for Protective Design  
<http://bmag.nwo.usace.army.mil>
  - U.S. Army Corps of Engineers, Electronic Security Center  
<http://www.hnd.usace.army.mil/esc>
  - U.S. Army Corps of Engineers, Protective Design Center  
<http://pdc.nwo.usace.army.mil>

#### **Selected Member Organizations**

- Air-Conditioning and Refrigeration Institute, Inc.  
<http://www.ari.org>
- Air Conditioning Contractors of America  
<http://www.acca.org>
- Airport Consultants Council  
<http://www.acconline.org>
- Alliance for Fire & Smoke Containment & Control  
<http://www.afsconline.org>

- American Association of State Highway and Transportation Officials (AASHTO)  
<http://www.transportation.org>
- American Institute of Chemical Engineers, Center for Chemical Process Safety  
<http://www.aiche.org/ccps>
- American Planning Association  
<http://www.planning.org>
- American Portland Cement Alliance  
<http://www.portcement.org/apca>
- American Public Works Association  
<http://www.apwa.net>
- American Railway Engineering & Maintenance of Way Association  
<http://www.arena.org>
- American Society for Industrial Security International (ASIS)  
<http://www.asisonline.org>
- American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE)  
<http://www.ashrae.org>
- American Society of Interior Designers  
<http://www.asid.org>
- American Society of Landscape Architects (ASLA)  
<http://www.asla.org>
- American Society of Mechanical Engineers (ASME)  
<http://www.asme.org>
- American Underground Construction Association (AUA)  
<http://www.auca.org> or <http://www.auaonline.org>
- American Water Resources Association (AWRA)  
<http://www.awra.org>
- Associated Locksmiths of America  
<http://www.aloa.org>

- Association of Metropolitan Water Agencies  
<http://www.amwa.net>
- Association of State Dam Safety Officials  
<http://www.damsafety.org>
- Building Futures Council  
<http://www.thebfc.com>
- Building Owners and Managers Association International (BOMA), Emergency Resource Center  
<http://www.boma.org/emergency>
- California Department of Health Services, Division of Drinking Water & Environmental Management  
<http://www.dhs.cahwnet.gov/ps/ddwem>
- Construction Industry Roundtable  
<http://www.cirt.org>
- Construction Innovation Forum  
<http://www.cif.org>
- Construction Specifications Institute  
<http://www.csinet.org>
- Construction Users Roundtable  
<http://www.curt.org>
- Defense Threat Reduction Agency (DTRA)  
<http://www.dtra.mil>
- Design-Build Institute of America  
<http://www.dbia.org>
- Drexel (University) Intelligent Infrastructure & Transportation Safety Institute  
<http://www.di3.drexel.edu>
- Federal Highway Administration  
<http://www.fhwa.dot.gov>
- Florida Department of Transportation, Emergency Management Office  
<http://www11.myflorida.com/safety/Emp/emp.htm>

- or  
Florida Department of Community Affairs, Division of  
Emergency Management  
<http://www.floridadisaster.org/bpr/EMTOOLS/Severe/terrorism.htm>
- or  
[http://www.dca.state.fl.us/bpr/EMTOOLS/CIP/critical\\_infrastructure\\_protecti.htm](http://www.dca.state.fl.us/bpr/EMTOOLS/CIP/critical_infrastructure_protecti.htm)
- George Washington University, Institute for Crisis, Disaster, and Risk Management  
<http://www.cee.seas.gwu.edu>  
or  
<http://www.seas.gwu.edu/~icdm>
  - Homeland Protection Institute, Ltd.  
<http://www.hpi-tech.org>
  - Inland Rivers Ports and Terminals  
<http://www.irpt.net>
  - Institute of Electrical and Electronics Engineers, Inc. - USA  
<http://www.ieeeusa.org> or <http://www.ieee.org/portal/index.jsp>
  - International Association of Foundation Drilling  
<http://www.adsc-iafd.com>
  - International Code Council (ICC)  
<http://www.intlcode.org>  
Consolidates services, products, and operations of BOCA (Building Officials and Code Administrators), ICBO (International Conference of Building Officials) and SBCCI (Southern Building Code Congress International) into one member service organization — the International Code Council (ICC) in January 2003.
  - International Facility Management Association (IFMA)  
<http://www.ifma.org>
  - Market Development Alliance of the FRP Composites Industry  
<http://www.mdacomposites.org>

- Multidisciplinary Center for Earthquake Engineering Research  
<http://mceer.buffalo.edu>
- National Aeronautics and Space Administration  
<http://www.nasa.gov>
- National Capital Planning Commission (NCPC)  
<http://www.ncpc.gov>
  - Security and Urban Design  
[http://www.ncpc.gov/planning\\_init/security.html](http://www.ncpc.gov/planning_init/security.html)
- National Center for Manufacturing Sciences  
<http://www.ncms.org>
- National Concrete Masonry Association  
<http://www.ncma.org>
- National Conference of States on Building Codes and Standards  
<http://www.ncsbc.org>
- National Council of Structural Engineers Associations (NCSEA) <http://www.ncsea.com> or  
<http://dwp.bigplanet.com/engineers/homepage>
- National Crime Prevention Institute  
<http://www.louisville.edu/a-s/ja/ncpi/courses.htm>
- National Fire Protection Association  
<http://www.nfpa.org>
- National Institute of Building Sciences (NIBS)  
<http://www.nibs.org> and <http://www.wbdg.org>
- National Park Service, Denver Service Center  
<http://www.nps.gov/dsc>
- National Precast Concrete Association  
<http://www.precast.org>
- National Wilderness Training Center, Inc.  
<http://www.wildernesstraining.net>



- New York City Office of Emergency Preparedness  
<http://www.nyc.gov/html/oem>
- Ohio State University  
<http://www.osu.edu/homelandsecurity>
- Pentagon Renovation Program  
<http://renovation.pentagon.mil>
- Portland Cement Association (PCA)  
<http://www.portcement.org>
- Primary Glass Manufacturers Council  
<http://www.primaryglass.org>
- Protective Glazing Council  
<http://www.protectiveglazing.org>
- Protective Technology Center at Penn State University  
<http://www.ptc.psu.edu>
- SAVE International  
<http://www.value-eng.org>
- Society of Fire Protection Engineers  
<http://www.sfpe.org>
- Southern Building Code Congress, International  
<http://www.sbcci.org>
- Sustainable Buildings Industry Council  
<http://www.sbicouncil.org>
- Transit Standards Consortium  
<http://www.tsconsortium.org>
- Transportation Research Board/Marine Board  
<http://www.trb.org>
- Transportation Security Administration - Maritime and Land  
<http://www.tsa.dot.gov>
- U.S. Air Force Civil Engineer Support Agency  
<http://www.afcesa.af.mil>

- U.S. Coast Guard  
<http://www.uscg.mil>
- U.S. Department of Energy  
<http://www.energy.gov>
  - Sandia National Laboratories (SNL)  
<http://www.sandia.gov>
    - Architectural Surety Program  
<http://www.sandia.gov/archsur>
    - Critical Infrastructure Protection Initiative  
[http://www.sandia.gov/LabNews/LN02-11-00/steam\\_story.html](http://www.sandia.gov/LabNews/LN02-11-00/steam_story.html)
- U.S. Department of Health and Human Services  
<http://www.hhs.gov>
- U.S. Department of Veterans Affairs (VA)  
<http://www.va.gov/facmgt>
- U.S. Environmental Protection Agency (EPA), Chemical Emergency Preparedness and Prevention Office (CEPPO)–Counter-terrorism  
<http://www.epa.gov/swercepp/cntr-ter.html>
- U.S. General Services Administration (GSA)  
<http://www.gsa.gov>
  - Office of Federal Protective Service (FPS) of GSA  
[http://www.gsa.gov/Portal/content/orgs\\_content.jsp?contentOID=117945&contentType=1005&P=1&S=1](http://www.gsa.gov/Portal/content/orgs_content.jsp?contentOID=117945&contentType=1005&P=1&S=1)
  - Office of Public Building Service (PBS) of GSA  
[http://www.gsa.gov/Portal/content/orgs\\_content.jsp?contentOID=22883&contentType=1005&PPzz=1&S=1](http://www.gsa.gov/Portal/content/orgs_content.jsp?contentOID=22883&contentType=1005&PPzz=1&S=1)
  - Office of the Chief Architect of GSA  
[http://www.gsa.gov/Portal/content/orgs\\_content.jsp?contentOID=22899&contentType=1005](http://www.gsa.gov/Portal/content/orgs_content.jsp?contentOID=22899&contentType=1005)  
and  
<http://www.oca.gsa.gov>

- U.S. Green Building Council  
<http://www.usgbc.org>
- U.S. Marine Corps Headquarters  
<http://www.usmc.mil>
- U.S. Society on Dams  
<http://www.ussdams.org>
- University of Missouri, Department of Civil & Environmental Engineering, National Center for Explosion Resistant Design  
<http://www.engineering.missouri.edu/explosion.htm>
- Virginia Polytechnic Institute and State University  
<http://www.ce.vt.edu>
- Water and Wastewater Equipment Manufacturers Association  
<http://www.wwema.org>

### **The Partnership for Critical Infrastructure (PCIS)**

<http://www.pcis.org>

Note: Involved mainly with information systems and not building real property.

#### **Government**

- Department of Commerce Critical Infrastructure Assurance Office (CIAO)  
<http://www.ciao.gov>
- Department of Energy (DOE)  
<http://www.energy.gov>
- Department of Homeland Security  
<http://www.whitehouse.gov/deptofhomeland>
- National Infrastructure Protection Center (NIPC)  
<http://www.nipc.gov>

#### **Private Sector**

- Anser Institute for Homeland Security (ANSER)  
<http://www.homelandsecurity.org>

- CERT<sup>®</sup> Coordination Center (CERT/CC)  
<http://www.cert.org>
- Electronic Warfare Associates (EWA)  
<http://www.ewa.com>
- Information Technology Association of America (ITAA)  
<http://www.ita.org>
- The Institute for Internal Auditors (IIA)  
<http://www.theiia.org>
- National Cyber Security Alliance (Alliance)  
<http://www.staysafeonline.info>
- North American Electric Reliability Council (NERC)  
<http://www.nerc.com>
- SANS Institute (SANS - SysAdmin, Audit, Network, Security)  
<http://www.sans.org>
- The Financial Services Roundtable Technology Group (BITS)  
<http://www.bitsinfo.org>
- The U.S. Chamber of Commerce, Center for Corporate Citizenship (CCC)  
<http://www.uschamber.com/cc>

**Selected States and Local Organizations**

- Association of Metropolitan Water Agencies  
<http://www.amwa.net>
- The Council of State Governments (CSG)  
<http://www.csg.org>
- International Association of Emergency Managers (IAEM)  
<http://www.iaem.com>
- National Association of State CIOs (NASCIO)  
<http://www.nascio.org>
- National Emergency Managers Association (NEMA)  
<http://www.nemaweb.org>

- National Governor's Association (NGA)  
<http://www.nga.org>
- The National League of Cities (NLC)  
<http://www.nlc.org>

