

# COMMERCIAL FACILITIES PROTECTION AND HOMELAND SECURITY



**FRANK R. SPELLMAN**

Copyright 2019, Berrett-Koehler Publishers. All rights reserved. May not be reproduced without permission from the publisher, except for those permitted under U.S. or applicable copyright law.

EBSCO Publishing : eBook Collection (EBSCOhost) : printed on 2/8/2023 10:03 PM via  
AN: 2212229 ; Frank R. Spellman ; Commercial Facilities Protection and Homeland Security  
Account: ns335141

# **Commercial Facilities Protection and Homeland Security**



# Commercial Facilities Protection and Homeland Security

Frank R. Spellman



Lanham • Boulder • New York • London

Published by Bernan Press

An imprint of The Rowman & Littlefield Publishing Group, Inc.

4501 Forbes Boulevard, Suite 200, Lanham, Maryland 20706

[www.rowman.com](http://www.rowman.com)

800-462-6420


6 Tinworth Street, London SE11 5AL, United Kingdom

Copyright © 2019 by The Rowman & Littlefield Publishing Group, Inc.

*All rights reserved.* No part of this book may be reproduced in any form or by any electronic or mechanical means, including information storage and retrieval systems, without written permission from the publisher, except by a reviewer who may quote passages in a review.

ISBN: 978-1-64143-347-1

E-ISBN: 978-1-64143-346-4

™ The paper used in this publication meets the minimum requirements of American National Standard for Information Sciences—Permanence of Paper for Printed Library Materials, ANSI/NISO Z39.48-1992.

Printed in the United States of America

*For Kathern Welsh*



# Contents

Acronyms and Abbreviations	ix
To the Reader	xiii
Preface	xv
Prologue—Hell’s Garbage Dump	1
<b>1</b> Introduction	9
<b>2</b> Sector Profile	21
<b>3</b> Resilience Measurement Index	35
<b>4</b> Active Shooters	55
<b>5</b> Critical Infrastructure Security and Resilience	63
<b>6</b> Vulnerability Assessment (VA)	79
<b>7</b> Preparation: When is Enough, Enough?	107
<b>8</b> Cybersecurity	115
<b>9</b> Emergency Response	125
<b>10</b> Security Techniques and Hardware	137
<b>11</b> The Paradigm Shift	197
Glossary	209
Index	227





# Acronyms and Abbreviations

ACH	Automated Clearing House
APEC	Asia-Pacific Economic Cooperation
APM	Asset Prioritization Model
ATM	Automated Teller Machine
ATM	Asynchronous Transfer Mode
BCPEI	Business Continuity Plan Exercise
BCPI	Business Continuity Plan Index
BIS	Bureau of Industry and Security
BSS	Broadcast Satellite Service
CATV	Cable Television
CERT	Computer Emergency Readiness Team
CFR	Code of Federal Regulations
CFTC	Commodity Futures Trading Commission
CHIPS	The Clearing House Interbank Payments System
CII	Critical Infrastructure Information
CIKR	Critical Infrastructure and Key Resources
CINS	FS-ISAC's Critical Infrastructure Notification System
CIP	Critical Infrastructure Protection
CLEC	Competitive Local Exchange Carrier
CME	Chicago Mercantile Exchange
CMI	Consequences Measurement Index
CS	Commercial Services
CSBS	Conference of State Bank Supervisors
CS/IA	Cybersecurity/Information Assurance
DCIP	Defense Critical Infrastructure Program
DHS	Department of Homeland Security
DIB	Defense Industrial Base

DOC	Department of Commerce
DOD	Department of Defense
Dodd	Department of Defense Directive
Dodin	Department of Defense Instruction
DOJ	Department of Justice
DOS	Department of State
DPAS	Defense Priorities and Allocations System
ECIP	Enhanced Critical Infrastructure Protection (program)
E.O.	Executive Order
FAA	Federal Aviation Administration
FBIIC	Financial and Banking Information Infrastructure Committee
FCA	Farm Credit Administration
FDIC	Federal Deposit Insurance Corporation
FEMA	Federal Emergency Management Agency
FOIA	Federal of Information Act
GDP	Gross Domestic Product
GPS	Global Positioning System
HSPD	Homeland Security Presidential Directive
IA	Information Assurance
IMCC	Incident Management & Command Center
IP	Office of Infrastructure Protection
IST	Infrastructure Survey Tool
IT	Information Technology
IXC	Interexchange Carrier
LEC	Local Exchange Carrier
MAUT	Multi-attribute Utility Theory
MOA	Memoranda of Agreement
MOU	Memoranda of Understanding
NCIP	National Critical Infrastructure Protection
NCS	National Communications System
NG	National Guard
NIAC	National Infrastructure Council
PMI	Protective Measures Index
PPD	Presidential Policy Directive
PrI	Preparedness Index
PSA	Protective Security Advisor
PSPrep	Private Sector Preparedness Program
PSTN	Public Switched Telephone Network
QA	Quality Assurance
RI	Resilience Index
RMI	Resilience Measurement Index
SAA	Significant Assets/Areas

SME	Subject Matter Expert
SSA	Sector-Specific Agency
SSP	Sector-Specific Plan
TSA	Transportation Security Administration
UAS	Unmanned Aircraft Systems



# To the Reader

As with all sixteen editions making up this series. . .

I am going to make you wake up scared; that is, if you sleep at all.

I am going to make you go through your day looking over your shoulder, to each side of you, in front of you and above you and aware of anyone and everyone you see or come into contact with.

I am going to make you shop at the mall in fear.

I am going to make you sit in your school desk ill at ease.

I am going to make you finish your day wondering when I will come after you and destroy you.

I will make your smart phone inoperative; you will not be able to use your favorite signoff: CUL8R.

When you go to bed, you will take a loaded heater, a fully loaded Dirty Harry Special with you because you will shoot into the darkness if necessary.

I am not crazy. I am not a Muslim. I am not afraid. My goal is to scare the be-Jesus out of you . . . constantly . . . all the time . . . any time . . . now and forever.

Again, I am not a Muslim. I am not crazy. I am not afraid.

What I am is a terrorist . . . plain and simple.

Live in terror, grasshoppers.

—Your Friendly Homegrown Radical Terrorist



# Preface

The thirteenth volume of a new, well-received, and highly acclaimed series on critical infrastructure and homeland security *Commercial Services Protection and Homeland Security* is an eye-opening account and an important reference source of a diverse and complex sector. This book was designed and written to serve and advise U.S. financial planners, project designers, engineers, communications technicians, law enforcement and security specialists, managers, and superintendents and/or supervisors, and responsible managers in charge of protecting the multifaceted nature of critical infrastructure in the United States. Whenever I mention to a colleague of mine that I was in the process of writing another volume of this series and I described the topic to be covered, she was surprised as always that I would embark on such a mind-numbing and difficult task. I remember that bewildered look on her face and her exact words when she asked: “How can you . . . or anyone . . . write about and describe the U.S. Commercial Services Sector Infrastructure when it is so deep, tall, and wider than wide and all encompassing and almost indefinable in terms of total reach, scope, extent etc., etc., etc.?” I had heard this statement many times in the past but my reaction remained the same when I remember scratching my head and trying to answer her again in an impressive way (not easy) and finally coming up with what for me was the ultimate answer. I replied, “If it exists, it can be written about and described.” Then she scratched her head and smiled while nodding her head side to side (meaning no way, Jose) and then she just changed the subject.

Anyway, currently, the CS sector critical infrastructure sector includes a diverse range of sites that draw large crowds of people (a terrorist’s dream situation) for shopping, business, entertainment, or lodging. Facilities within the sector operate on the principle of open public access (a key factor for terrorists), meaning that the general public can move freely without the deterrent



of highly visible or obstructive (bollards) security barriers. The majority of these facilities are privately owned and operated, with minimal interaction with the federal government and other regulatory agencies.

This book is organized to simplify and present in a logical and sequential manner a discussion of not only the elements comprising the CS sector in the United States but also many of the security measures employed to protect the various entities and equipment involved.

Let's face today's reality, those who want quick answers to complicated questions—to help employers and employees handle security threats—must be prepared to meet and deal with the threat of terrorism on a 24/7 basis. It is important to point out that this book does not discuss and focus on security concerns related to natural disasters; on the contrary, the focus here is on the security aspects in the design of systems that need to be able to deal robustly with possible sources of disruption, specifically from malicious acts; moreover, the focus includes the added dimension of preventing misuse and malicious behavior. In the post-9/11 world, the possibility of CS sector infrastructure terrorism—the malicious use of substances, weapons, and cyber intrusion to cause devastating damage to CS sector infrastructure and its associated subsectors along with—literally—its cascading effects—is very real. Thus, the need is clear and real and so is the format and guidelines presented in this text to improve protection and resilience of CS sector infrastructure.

This book describes the sector-subsector-wide process required to identify and prioritize assets, assess risk in the sector, implement protective programs and resilience strategies, and measure their effectiveness. This book and the complete sixteen volumes (upgraded from the original fourteen volumes) of the critical infrastructure sector series were written as a result of 9/11 to address these concerns. It is important to point that our CS sector infrastructure (as is the case with the other fifteen critical infrastructures) cannot be made absolutely immune to all possible intrusions/attacks; thus, it takes a concerted, well-thought-out effort to incorporate security upgrades in the retrofitting of existing systems and careful security planning for all new facility infrastructure components. These upgrades or design features need to address issues of monitoring, response, critical infrastructure redundancy, and recovery to minimize risk to the facility infrastructure. However, based on personal experience none of these approaches is or can be effective unless CS sector staff members at all levels of the chain of command are cognizant of the threats.

*Commercial Services Protection and Homeland Security* presents common-sense methodologies in a straightforward, almost blunt manner. Why so blunt? At this particular time, when dealing with security of workers, family members, citizens, and society in general—actually, with our very way of life—politically correct presentations on security might be the norm, might

be expected, and might be demanded but my view is that there is nothing normal or subtle about killing thousands of innocent people; mass murders certainly should not be expected; the right and need to communicate and the right to live in a free and safe environment is a reasonable demand.

This text is accessible to those who have no experience with or knowledge of the CS sector. If you work through the text systematically, you will gain an understanding of the challenge of domestic preparedness—that is, an immediate need for a heightened state of awareness of the present threat facing the CS sector members as potential terrorist targets. Moreover, you will gain knowledge of security principles and measures that can be implemented—not only adding a critical component to your professional knowledge but also giving you the tools needed to combat terrorism in the homeland—our homeland, both by outsiders and insiders.

One final word to readers: This book is written in the conversational and engaging and reader-friendly style that is the author's trademark. Why? Well, when demonstrating how one or anyone can write about the U.S. CS sector when it is so deep, tall, wide, and all-encompassing and almost indefinable in terms of total reach, scope, extent, etc., etc., etc., I never apologize for attempting to communicate.

Frank R. Spellman  
Norfolk, VA.



## *Prologue*

# Hell's Garbage Dump

*Note:* The following fictitious account is included here in order to set the stage for what follows in the text and to continue the sordid saga of the Williams family. The Williams are homegrown radicalized terrorists (smart and brutal; you might say they are clones of Timothy McVeigh types) who have done whatever they could do to bring about the death and destruction of innocents in the United States, with particular attention being paid to attacking, impacting, and/or destroying sectors of critical infrastructure.

\*\*\*\*\*

Again, repeatedly, uncontrollably, I'm dreaming that I am awake and still in that place, unrelenting.

I dream that I am looking around my location for the first time. I'm in an enclosure, of sorts. And the smell, that stink, that stench, that reek; it is never-ending, never fading, never masked (well, that's not quite the case; it is subtly masked by that penetrating smell of old urine); it's everywhere, all enveloping and encapsulating like air. It's like wet or damp cement (with the absorbed urine), concrete. Ah, and that is no surprise because it is cement, concrete, all concrete: the four windowless walls, the floor, the ceiling interrupted with a recessed metal fan (or, more correctly, under the designed function of this space maybe it is made of plastic, for the occupant's and guards' safety, you understand). Then there is the heavy metal door, with its slot and small shelf for sliding in and out the food tray, framed soundly in and by an even heavier frame. The contents of this 7 by 12-foot enclosure? Sparse, is the understated description and concrete is the reality. With the exception of the overhead recessed fan and one corner light fixture (also recessed into the concrete and its fixture window made of heavy wire mesh and giving off a

dim, checkered board light), all fixtures are concrete: toilet (no toilet seat), sink, supply, and waste pipes, the bed. Bed? Yes, that concrete bed. Mattress? No way, Jose and Maria. It is a stone mattress (now, please, do not confuse this stone mattress with the excellent tale of horror and murder about Verna who killed four of her husbands [don't you just love a ruthless, evil, in-charge woman?] the same title by my favorite female blood and guts author, you know the one who professed: don't let the bastards grind you down. That would be Margaret Attwood, of course). I do have two gray blankets stamped "U.S." I use one for cover and one covering the stone mattress.

How about the contents; that is, besides the concrete toilet without toilet seat, concrete piping, the metal or plastic ceiling fan, and the concrete bed with its stone mattress? Well, there is no chair, no table, no lamp, no reading material, no computer, no phone, no clock, and no hanging pictures, photos, etc. One wall ornament is included: a fly on the wall: a hidden smoke detector camera. Intuitively, I know what it is a CCTV covert camera; surely I am monitored daily and nightly, because the caged, dim light is never extinguished and the monitors are manned around the clock. Besides, with my beauty queen good looks why would you (or anyone else) not want to observe my every move and action, 24/7?

What about personal hygiene products and utensils? Well, there is no toothbrush; it could be sharpened into a pointed weapon. A roll of toilet paper sits on the concrete sink next to the concrete toilet.

How about tenure, time spent daily within the cell; it is a cell, but you've figured that out by now . . . I suppose. Anyway, they let me out one hour per day for exercise in a sunless hole of a courtyard, again with that horrible wet cement odor throughout. But, anyway, when you are twenty-one years old with a body that would stop two freight trains and models and Hollywood deadheads would die for, I needed to exercise for body toning . . . not for weight loss because the food is unfit for consumption . . . it was the daily rice allocation that saved me. It is difficult to mess up rice.

The jolt that begins to bring me out of the dream and to start the awakening process is that final realization: there is no mirror; none, nowhere. You see, not only do I have a freight train stopping body but I also have that knock-down, drag-out beauty that all women desire. But that is not the point, even if I looked like a clone of Freddy Krueger, I would want to be able to check on my appearance and especially my flame red hair to make sure all is well with that, at least.

Ironically and fittingly, it is a mirror, a full length, wall covering mirror, a mirror that can't be missed or ignored, that necessary glass eye stationed at the end of my bed in my pent house that lets me know I am awake. I know I do not look my best when I first awake, do any of us, but I do not care . . .

the ability to look in the mirror, any mirror, is important to me. I think you can understand that.

I seem to have morphed from what I call a Super Duper Max confinement cell to my present location in the pent house. I can read your thoughts and hear your questions about this one . . . and much more.

Okay, guess I ought to begin my story at the beginning. First, I am B. M. Williams VIII. Yes, if you guessed or ascertained that I am part and parcel of the infamous Williams family known for terrorist acts here, there, and anywhere you are one smart cookie. Unfortunately, most of my blood (family members) are incarcerated for life in places similar to the one described in my reoccurring dream. People and mostly the bleeding heart left-wing media have branded me and them terrorists of the worst sort: cold-blooded killers with zero empathy for anyone. This is true, of course. But think about it. If it is okay for those who kneel during the playing of our national anthem, why is it not okay for my family to protest by killing, and maiming, and destroying? The Williams' feel like we have a right to our point of view too, grasshoppers!

Anyway, you want to know how I became incarcerated and ended up spending three years locked up in Super Duper Max . . . the cement hell. I was born to be a terrorist. I am a terrorist and will be a card-carrying terrorist until death do we part. However, I take a different slant on homegrown terrorism than most of my blood. I do not necessarily need to kill people, blow up buildings, burn ISIS flags, or spit on alt-left wingers to accomplish my goal(s). No, sir. I have my own view and modus operandi. You see, if you kill or blow things up or burn the crazies' flag(s), you will either die in the performance of such applaudable actions or end up in Super Duper Max for life. Of course, that is better than the rope, electric chair, firing squad, or being gassed to death in one of the Nazi-like gas chambers. You see, my friends, I know that if you commit capital crimes in the bleeding heart liberal wacko states like Washington, Oregon, California, and a few East Coast states, the death penalty is never exercised . . . the bleeders protect killers and ignore victims—that is a given.

Anyway, I decided to commit terrorist acts that do not necessarily kill people or blow things up. No. There are things (chemical compounds) that explode with bizarre violence (and that is good) even in laughably small amounts, leaving ruined buildings and shattered people in their wake. Nope, I will not work with such. There is a better way to get the message across . . . to hurt all those bleeders . . . to accomplish my goal(s) . . . and, if caught to receive a short sentence . . . enabling future endeavors, events . . . if so desired. Besides, killing people or blowing up things is too dangerous. Additionally, if the targets get a whiff of what my intentions are they have

the choice to flee, hide, or fight. It is the fight I do not want. I am a patriotic terrorist and not a martyr . . . no way, Jose and Maria.

You see, being the genius that I am, a former child prodigy in all things mathematical and science-based, I was an expert in chemistry by age sixteen. The fact is I knew more about chemistry than any of my teachers, professors, or others and could outdo them all anytime in that field. So, being the genius that I am and being filthy rich, like all my blood, I came up with the perfect terrorist scenario, plain and simple, or so I thought at the time.

What was my scenario and if I performed it and was perfect why did I end up in Super Duper Max? Hmmmm, good questions, grasshoppers. Patience, please.

Anyway, I decided to pick on, to attack the commercial sector. Namely, I decided to put that multinational retailing corporation that operates as a chain of hypermarkets, discount department stores, and grocery stores out of business. You know the one. Just about everyone shops there. But, in case your mind is blank on this one, check out figure 0.1.

You might say I wanted to stink up the place . . . and as many other stores as I possibly could contaminate before they caught on. What I did was experiment with several different smelly chemical concoctions. For example, I played around with ethyl mercaptans, putrescine, or tetramethylenediamine, which give off the foul odor of dead organisms. But they proved to be too mild for my intended purposes . . . more like perfume, not Joy perfume of course, instead of the really stinky stuff I wanted. So, I looked at some more



**Figure 0.1 Wel Merc.** *Source:* Illustration by F. R. Spellman.

isocyanides, where the nitrogen and carbon atoms are swapped; their disagreeable odor is legendary. Not good enough. What I needed was a herd of skunks in crisis and emanating their overwhelming stink . . . a persistent stink. Persistence is the key characteristic I was looking for. I wanted an odor that would drive customers to their knees begging for mercy and for their mommas and contaminate the store for a long period of time.

After a few weeks of experimenting with pinched nostrils and covered mouth and after destroying several contaminated lab gowns and other clothing items, I settled on the perfect substance: An offshoot, a derivative of thioacetone. Someone said thioacetone smelled like hell's dumpster . . . but I needed a substance that smelled terrible on a much larger scale, like hell's garbage dump. So, I modified thioacetone to make it to what I thought would be the worst smelling substance known to both man or beast. I will not reveal the chemical formula or composition or the cracked trimer here; there are some things that I will not discuss with anyone.

Anyway, after I had made up my stinky concoction, which I titled Thio-Max, fitting, of course, I thought through the rest of my plan. Thio-Max was (by the way, it no longer exists) in liquid form, brown in color, and slightly viscous, tacky. I wanted it tacky so when applied to the target with a cotton swab it would readily adhere to the target. I wanted it penetrating to the senses, extremely unpleasant; enough so to foul up the air and anything it was applied to for several weeks, months, or forever. After my concoction met all my parameters, I decided there would be multiple product targets; basically, anything on a shelf or in or on an open stand, accessible. After I had made up a dozen test tube size containers, rubber stoppered, I placed them into a test tube stand, to hold temporarily, waiting for application.

I had planned out the Wel Merc stores that I would attack in the northern Seattle area. I made sure I knew how to get from one store to another, quickly. In order to safely apply Thio-Max to items inside the store without totally contaminating myself, I wore glasses (safety glasses that looked like regular glasses) and I included one of those swimmer's nose clips; it was transparent and small not to attract attention. I carried one tube of Thio-Max and a couple of swaps. I wore a nonsignificant, plain-looking white set of coveralls and white tennis shoes; no undergarments. And, I also made sure I had the thinnest, tightest fitting plastic gloves I could find.

I was equipped and ready. I entered my first Wel Merc store at 10:00 a.m. on that warm and sunny Friday. It was a payday for most and I knew that the store would be packed with shoppers to spend money and with tire kickers to look. I did not hesitate; it is not any part of my being. "I am like that guy who said Damn the torpedoes, full speed ahead!" I walked in and straight for the clothes and linen section and performed my dip and dab, dib and dab, dib and dab . . . here, there, and everywhere within reach. All was going as planned



until shoppers and lookers started to cough, cry, breathe hard, scream, go crazy, and start running in all directions. The stench was overwhelming, like a giant's large hand reaching from all directions and grouping them . . . then the mishap. The mishap? Well, when the mass hysteria and convulsive panic set in there were bodies, groceries, clothes, auto parts, soap bottles, candies flying, and bodies sprawling in all directions, some lying in mountains of puke that was building here and there. The mishap accelerated when mass hysteria and bedlam took over and a herd of desperate people ran me over as I headed for more targets. I was trampled to the floor and the tube of Thio-Max fell from my hand and spilled all over the floor. You might say that it was like stink on floor . . . literally. But, I swear it was more like a mushroom cloud of stink ascending to the rafters above. Somewhere close I heard a kid scream: **"MAMA, THERE'S A WHOLE BUNCH OF STINK IN THIS PLACE . . .!"** And then all went black . . . I was out.

I awoke to the sounds of horrendous and non-stopping bitching and moaning by a couple of humungous cops, and also to the severe pinching of my wrists from handcuffs too tightly constraining my wrists, and finally to a terrific headache with body swellings from the top to bottom of my body . . . I guessed it was caused by falling or maybe from being brutalized by the cops. They continued their terrible bitching and cussing as they drove me to the nearest lockup. In their irate descriptions of the filthy stench that I had encapsulated them with . . . simply, they were extremely disturbed and enraged . . . and that was a pleasant thought to me, at least at that time. But I have to admit the overwhelming stench on me, about me, on and in the police car was sickening and I remember puking a few times before we arrived at the lockup.

At the lockup, after three jailers put on hazmat suits and self-contained breathing apparatus, they removed my stinking self from the car (which I overheard them say would be towed and totally destroyed via crushing and melting) and carried me into the jailhouse shower room where two burly looking female wrestler types, also donned in hazmat attire, were waiting to scrub me down, literally. That is, to scrub me down right after my haircut . . . a pig shave is what they called it. All that beautiful flaming red hair was history; it seems like it has taken forever to grow it back to a reasonable length, but still bright red, thankfully. To me, red is important.

You know what? It was not the essential oils, soap, turpentine (felt like it) they used on my body when they scrubbed me down that was so horribly, painfully, excruciatingly, and downright despicable . . . no, sir, it was those two long-handled bristle brushes they used (I thought torture was outlawed in this country?); they almost took off my skin, although I have to admit it is good to shed worn skin, to a degree. And, later on, even to this day, right now, as a matter of fact, I have a constant hint of that stench, no matter what or where or when; it is persistent like lead in drinking water and seems

permanent like one of my tattoos. One of those guards tried to scrub off my upside down American flag tattoo off from my left upper arm. She did not succeed. At the present time seems ironic to me that anyone would want to remove that tattoo. Gee, it is okay for many to kneel during the national anthem and to abuse our flag; thus, why can't I display my feeling about the flag in my way? To me it was outlandish and directed abuse. I guess I am stuck with that kind of treatment; the price paid for being a patriot.

Well, it is time to summarize my failed plot, my court experience, and my situation at this very moment. And, besides, I have a lot of planning to do for my future goals; thus, time is limited. Is this not always the case, grasshoppers? Anyway, first, my plot did fail; I was only capable of contaminating one Wel Merc store, instead of the dozens I had planned on. The good news is that I completely put that particular mega-store at that location out of business. They tried to restore the place; they even sandblasted the cement floor and roof rafters; it was to no avail. They say that location still stinks, even after the store was leveled and hauled away in pieces. I also heard they are planting trees and bushes at the old spot, hoping that will solve the stink problem . . . and make that horrible memory fade. No one died from the event and that is one reason I received such a light sentence. However, several people who became sick and were hospitalized have shunned Wel Merc stores—that was my goal. And, not to be ignored is the fact that the corporation had to spend millions installing odor detection technology . . . makes me feel warm inside . . . you too? My family trust fund did have to pay out several million, only pocket change to us, for the damages to the store and hospital expenses and lawsuits, many of the lawsuits are still ongoing. So be it.

Anyway, speaking of court cases, I had a short trial because I pleaded guilty to all. Why not? I was guilty and proud of it. Even though I tried to shorten the trial with my pleading the U.S. Attorney went on the attack against my family and me and called us a bunch homegrown wackoes and deadly killers. Wow! I have to give that woman credit; she knew how to stir the anti-patriotic pot. She is definitely my kind of woman; that is, except for being a brain-dead liberal. But, I was not worried. I was being tried in a city that does all it can to protect the perps and ignore the victims. Isn't this the American way? Anyway, I got three years . . . and served less than two because I was a good girl . . . and that is almost true, the good girl part . . . I know how to play the game. Don't you?

Also, I learned an important lesson in planning such events (not saying I will try again somewhere else; keep in mind that the Feds are reading this too; they stick like burrs). The lesson? Well, when acting as I did in a place with hundreds of people in fairly close quarters, panic, bedlam, and fear turn the madding crowd into stampeding animals . . . and even the innocent like me can be hurt.

Oh well, as I sit here in my fifteenth-story penthouse at the southern end of Phinney Ridge in Seattle with an open copy of James Thomson's work *The Castle of Indolence* on my lap, and now looking out my huge picture window over the Fremont District and Lake Union at Queen Anne Hill and watching the top of the Space Needle that looks like a flying saucer hovering above the hilltop, I am thinking . . . planning . . . dabbing Joy perfume on my neck to quell that persistent odor . . . smiling. Why? Because, to echo those famous words I am thinking: "I will be back." Though much is accomplished, much remains. Count on accomplishment, grasshoppers . . . but, don't tell the Feds . . . ha.

## Chapter 1

# Introduction

Never underestimate the time, expense, blood, sweat, and effort a terrorist will apply to compromise the security of any industrial facility.

As I compose the contents of this edition of the sixteen-volume series on Homeland Security, I just heard on *Fox News* that there are over 50 dead, 200 injured (and counting) in Las Vegas after the deadliest shooting in modern U.S. history (October 2, 2017).

### WHAT IS TERRORISM?

Since 9/11, we have heard it said by many of our teachers, neighbors, security specialists and students (and many others) that there is controversy about the definition of the politically charged word *terrorism*. Terrorism, like pollution, is a judgment call. For example, with regard to defining pollution, if two neighbors live next door to an air polluting facility, one neighbor who has no personal connection with the polluting plant is likely to label the plant's output as pollution. The other neighbor who is an employee of the plant may see the plant's pollution as dollar bills—dollars that are his or her livelihood. I have heard workers who dive into ponds full of raw sewage to find a leak in an effluent pipe say that the sewage in the pond and its associated odor is money in the bank . . . and long-term employment because toilets are not likely to vanish anytime soon. Why a money-making enterprise? Because there are few people around who would join them in diving into trenches filled with raw sewage and in doing their work. On the terrorism front, when someone deliberately spikes a tree to prevent loggers from cutting it down, the tree-spiker might feel he or she is a patriot, just a knight in shining green armor and definitely

not a terrorist. On the other hand, the logger who has to take the tree down and puts his or her life and limbs at risk in taking down the spiked tree has little doubt in his or her mind on what to call the tree-spiker, and what the tree-spiker is called certainly has nothing to do with patriotism. Thus, what we are saying here in the example presented, pollution versus terrorism, is that along with attempting to define pollution, trying to define terrorism may be a judgment call, especially in the view of the terrorists.

## SETTING THE STAGE

The Commercial Services (CS) Critical Infrastructure sector includes a host of soft targets including the following subsectors:

- Gaming (e.g., casinos)
- Lodging (e.g., hotels, motels, conference centers)
- Entertainment and media
- Outdoor events (e.g., theme and amusement parks, fairs, campgrounds, parades)
- Public assembly (e.g., arenas, stadiums, zoos, aquariums, museums, convention centers)
- Real estate (e.g., office and apartment buildings, condominiums, mixed use facilities, self-storage)
- Retail (e.g., retail centers and districts, shopping malls—the Wel Mercs of the world).

The CS sector faces a complex and evolving risk environment that has the potential to disrupt the sector's ability to deliver services that are critical to the nation's economy. To manage this risk, a diverse set of stakeholders—including CS companies; sector trade associations; federal government agencies; financial regulators, state, local tribal, and territorial governments; and other government and private sector partners in the United States and around the world—collaborate to enhance the sector's security and resilience—resilience being the key goal (USDOT/DHS, 2015).

## SECTOR OVERVIEW

From the above list of CS components, it is clear that the sector is made up of an extremely diverse range of sites and assets where large numbers of people congregate daily to conduct business, purchase retail products, and enjoy

recreational events and accommodations. Given the national and international visibility and potential human and economic consequences associated with CS entities, it is important for the federal government and the CS sector to work together to ensure the protection of our nation’s prominent business centers and gathering places.

Working together and assigning responsibility is the key requirement in providing protection for the CS sector. The primary tandem entities responsible for protecting CS sector infrastructure and assets are U.S. Department of Homeland Security (U.S. DHS) and the private sector. In conjunction with the federal government, the private sector is able to predict, anticipate, and respond to sector outages and understand how they might affect the ability of the national leadership to continue CS during times of crisis, impact the operations of other sectors, and affect response and recovery efforts.

The CS sector is closely linked to other sectors (see figure 1.1). Specifically, without energy, communications, and potable water, the CS sector would not be able to sustain operations. Transportation systems allow employees and customers to travel to and from facilities and enable facilities to receive products and supplies. The CS sector partners regularly with emergency services personnel to mitigate risk, and the Emergency Services Sector responds to disasters that occur at facilities. Healthcare partners provide services to the public after an event, including a large-scale outbreak of an illness. The CS sector relies on financial services to conduct daily business operations, and the financial services sector needs the CS sector for its facilities. Government

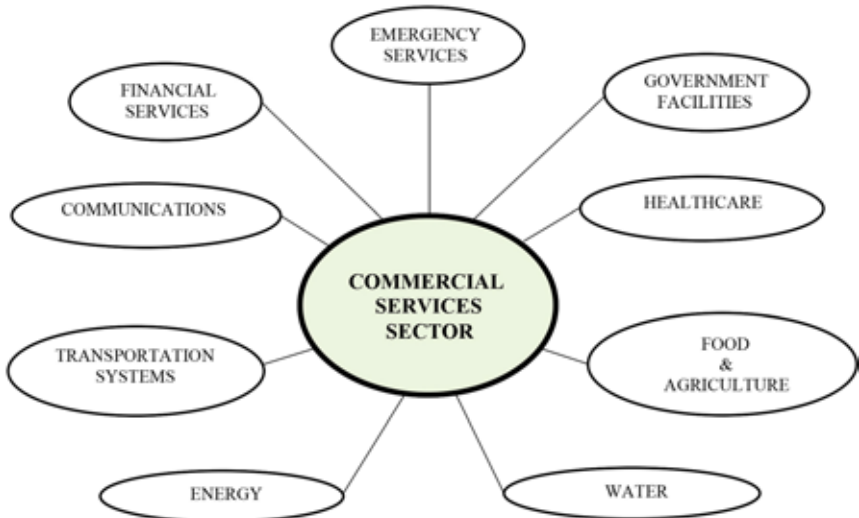


Figure 1.1 Critical Sector Interdependencies.

facilities sometimes reside within CS sector properties as tenants or adjacent to commercial facilities. This affects the risk of the CS and Government Facilities sectors, which collaborate to address security challenges, and could impact continuity of government operations and timely recovery from events. For those of us who enjoy partaking of food and drink that is commonly served in commercial facilities, vendors' menus would be nonexistent and their prepared food bins empty without the Food and Agriculture sector. Indeed, the CS sector is closely linked to other critical sectors (each of which is covered or their coverage is in production in separate, forthcoming editions in this series). For now consider a couple of snapshot examples (DHS, 2017):

- The *Energy Sector*, which provides the flow of energy in different forms to run the engines of industry and just about everything else we have come to count on to maintain the so-called good life. Without the flow of commercial products to maintain the flow of energy, the engines of industry would come to a screeching halt and the so-called good life might revert to a time when caves again become the primary domiciles.
- The *IT Sector*, which provides critical control systems and services, physical architecture, and Internet infrastructure, and also relies on communication to deliver and distribution applications and services, is another sector that cannot exist or survive without commercial resources.
- The *Emergency Services Sector*, which depends on the other sectors for direction resources, coordinating response, operating public alert and warning systems, and receiving emergency 911 calls, cannot function without commercial support of one type or another.
- The *Transportation Systems Sector*, which provides the fuel needed to power backup generators and relies on financing to maintain monitoring and control of the flow of ground, sea, and air traffic, cannot function without being fueled by finances.
- The *Financial Services Sector* provides financing and banking services needed to ensure the viability via cash flow and financial security to the CS sector.
- It is safe to say that none of the other fifteen critical infrastructure sectors could function as they presently do without the products and services provided by the CS sector.

The majority of CS sector facilities are privately owned, operated with minimal regulations, and house the business activities and commercial transactions that dominate the U.S. economy. The eight subsectors included in the CS sector facilitate coordination among facilities with similar functions, operations, and security issues. Note that the Retail Subsector is

further divided into two councils: the Shopping Center Subsector, which includes mall developers, and the Council of Retailers, which includes stores within malls and stand-alone retail establishments. Unlike many of the other critical infrastructure sectors the CS sector stakeholders have the added burden of balancing security priorities with their need for open access, public confidence, and economic vitality. Needless to say, this is no easy task.

Along with terrorist threats, the CS sector faces other persistent risks such as natural disasters, armed attacks, pandemics, theft, supply chain, and geopolitical disruptions. Moreover, risks associated with cyberattacks continue to grow, as CS sector reliance on cyber systems, such as for online financial transactions and building management, rises. In addition, the use of social media has facilitated increasingly coordinated protest activities and also allowed terrorist organizations to solicit support. The CS sector is also working on collaborating with the FAA) to address risks posed by the growing prevalence of UAS or drones.

### DID YOU KNOW?

Whenever we think of a typical deadly terrorist event, what usually comes to mind is some wacko wearing an explosive laden suicide vest that mingles within a large crowd and then detonates at the exact right moment to cause the most death and destruction. In other circumstances you might visualize a cold-blooded wacko with a rocket-propelled grenade . . . or you might visualize a hotel balcony and some radicalized idiot with automatic weapons shooting and killing randomly into a crowd from the 32nd floor. However, a new methodology is occurring that includes motor vehicles of various sizes and makes driven by some heartless insane person into crowds of shoppers or others innocents, maiming and killing and many as possible. But, it should be pointed out that these are old and somewhat archaic terrorist acts. Today, the terrorist paradigm, because of advances in technology, has shifted to the use of drones loaded with explosives to maim and kill. Unfortunately, as the drone technology advances, an increase in their use to kill is likely to increase in an exponential manner.

At this point you have probably surmised that the one way of investigating the interdependence of the CS sector architecture is to look at them from a critical consumer services infrastructure perspective. The *National Infrastructure Protection Plan* (NIPP, 2013) is intended to meet the requirements set forth by the president in Homeland Security Presidential



Directive 7 (HSPD-7). The Treasury Assistant Secretary for Financial Institutions implements the Treasury Department's responsibilities under HSPD-7. To meet objectives set forth by HSPD-7 for collaboration with the private sector, the Homeland Security Department works closely with the private sector. Further, NIPP utilizes Critical Infrastructure Identification, Prioritization, and Protection which is an overarching approach for integrating the nation's Critical Infrastructure and Key Resources (CIKR) protection initiatives.

It is clear that when owners and operators better understand their risks and interdependencies, they can develop business continuity strategies that build agility and redundancy into operations and implement security practices that mitigate facility and asset risks.

Each CS company is responsible for managing individual operational risks. Owners and operators in the CS sector assess individual risks and establish internal plans to mitigate risks and respond to disruptions. After assessing risks and establishing internal plans the next steps taken are to conduct vulnerability assessments (VAs) of high-priority infrastructure; developing webinars, threat briefings, tabletop exercises, and training; and collaborating with state, local, and regional authorities to build disaster response.








## **CS SECTOR GOALS, PRIORITIES, AND ACTIVITIES**

The CS sector has identified goals and priorities to guide the sector's security and resilience efforts to meet the sector's risk profile. As part of a detailed implementation plan, the sector identified twenty-four activities that partners plan to undertake, as resources allow, to improve the security and resilience of U.S. CS operations. Table 1.1 lists CS sector goals and priorities; also see table 1.2.












## **BENCHMARKING**

After an organization implements its security procedures, equipment, programs, training, and organizational attitude (i.e., ensuring all employees' awareness) the so-called security-conscious organization needs some type of methodology for checking (measuring—using metrics) just how effective their security preparation really is. Based on experience, I have found that when an organization thinks they are bullet proof, they are not. So, the question becomes, how does the organization measure its security preparedness and effectiveness? Actually there are a number of ways and a few are discussed in chapter 3 (Resilience Measurement Index), but one technique that can be effective, initially, is benchmarking.

**Table 1.1 Commercial Services Sector Goals and Priorities (DHS, 2015)**

<i>Goals</i>	<i>Priorities</i>
<p>1. Strengthen trusted and protected information sharing and ensure sector access to timely, actionable, and threat-specific information and analysis.</p>	<p> <b>PRIORITY A</b></p> <p>Improved formal public-private information-sharing processes at all levels; expand owner and operator access to relevant intelligence; and centralize two-way, public-private threat sharing to streamline reporting.</p> <p> <b>PRIORITY B</b></p> <p>Promote value of participation in the sector partnership to better engage and reach out to all subsectors, smaller owners and operators, and industry organizations in the sector partnership.</p>
<p>2. Support the sector’s needs for open access, public confidence, and economic vitality while cost effectively reducing physical and cyber risks and enhancing overall security and resilience.</p>	<p> <b>PRIORITY C</b></p> <p>Expand upon sector products, training, and exercises to enable owners and operators to reduce risk and improve readiness.</p> <p> <b>PRIORITY D</b></p> <p>Improve CS cyber-security knowledge, tools, capabilities, risk assessments, and practices to secure critical cyber and physical assets linked to cyber systems.</p>
<p>3. Increase capabilities and maintain advanced planning systems to ensure timely and effective response and recovery of critical services.</p>	<p> <b>PRIORITY E</b></p> <p>Enhance coordination with interdependent sectors and community response partners to improve resilience and enhance decision-making.</p>
<p>4. Assess and analyze threats, vulnerabilities, and consequences to inform facility and sector-wide risk management.</p>	<p> <b>PRIORITY F</b></p> <p>Continue to conduct cyber and physical risk assessments And develop risk reduction strategies for evolving threats in collaboration with cross-sector, federal, regional, and local security stakeholders.</p>
	<p> <b>PRIORITY G</b></p>

**Table 1.2 CS Sector Activities Mapped to Priorities (DHS, 2015)**

Map to Priority	Sector Activities
	<p>Improve DHS coordination with other federal, state, regional, and local agencies—including the Federal Protective Service and General Services Administration—and centralize government sources for CS owners and operators to access information from across all agencies, including fusion centers.</p>
	<p>Formalize the process across DHS to provide sector feedback on intelligence that should be delivered at the <i>For Official Use Only</i> level. Increase the number of clearances in each CS subsector.</p>
	<p>Promote coordination among seventy-seven fusion centers to connect nationwide information, particularly for national and global corporations. Use the Real Estate Information Sharing and analysis Center as a resource.</p>
	<p>Increase awareness of the sector partnership framework, available resources, and strategic value to better engage all subsectors and small-scale owners and operators and to recruit new members. Engage unions, Chambers of Commerce, and the Small Business Administration in security awareness training activities.</p>
	<p>Continue to expand the Real Estate Information Sharing and Analysis Center to include the Entertainment and Media, Outdoor Events, Public Assembly, and Sports Leagues Subsectors, and strengthen information-sharing relationships with owners and operators.</p>
	<p>Reevaluate and restructure the CS Sector to optimize organization and reflect relationships between subsectors.</p>
	<p>Continue to conduct outreach for existing risks assessment tools/resources and leverage them to conduct onsite risk assessments at high-priority facilities.</p>
	<p>Leverage cyber-assessment capabilities from DHS and other federal agencies to conduct onsite assessments and share common vulnerabilities across subsector facilities.</p>
	<p>Evaluate potential cyber risks and encourage CS sector members to use the National Institute for Standards and Technology Cybersecurity Framework. Formulate communities of subsector information technology experts (connected to the Sector Coordinating Council) to address sector-specific cyber threats.</p>
	<p>Expand armed attacker training to help smaller companies prepare and to provide materials for owners and operators to address employee training gaps.</p>
	<p>Develop surveillance curriculum for security directors and leaders with in the Surveillance Awareness Working Group.</p>

(Continued)

**Table 1.2 CS Sector Activities Mapped to Priorities (DHS, 2015)—Continued**

Map to Priority	Sector Activities
	Develop a Sector Coordinating Council play book for government and industry coordination and communication protocols during disaster response and recovery.
	Develop an inventory of all documents and guides in each subsector.
	Track after-action reports from previous events across critical sectors to completion.
	Work with the lifeline sectors, particularly the Energy and Water sectors, to examine strategies to sustain CS Sector identifying ideas to improve resiliency or organizing other activities.
	Work with the Emergency Services Sector and local officials to develop and conduct outreach for low-cost, unified, and nationwide response efforts—such as crisis reentry credentialing to ensure access to restricted areas after a disaster.
	Facilitate collaboration among owners, management companies, and tenants along with federal, state, and local partners—to improve joint risk mitigation and response to armed attacker threats.
	Collaborate with the Financial Services Sector to create a joint resource for logging the accessibility of ATM and banking resources during disasters, leveraging the Financial Services Information Sharing and Analysis Center and the Real Estate Information Sharing and Analysis Center.
	Work with Outdoor Events Subsector partners to increase resilience of outdoor events.
	Identify regions most at risk from climate change, determine which factors place them at risk, and develop mitigation strategies for CS infrastructure.
	Work with government and private sector partners, including the Federal Aviation Administration, to evaluate the emerging risk of unmanned aircraft systems and develop response strategies.
	Improve the sector’s ability to leverage and respond to social media to enhance security during incidents and steady-state operations.
	Encourage more CS partners to seek SAFETY Act designation or certification, where appropriate.
	Build on the Resilience Measurement Index to establish a resilience “score card” that helps owners and operators in the CS sector and lifeline sectors determine how resilience is being measured and managed, and assists government agencies with tracking their effectiveness in information sharing.

Benchmarking, a relatively new buzzword, is a valuable tool for use under any management system. For security and safety management, benchmarking is defined as a process for rigorously measuring your security and/or safety program versus “best in class” programs, and for using the analysis to meet and exceed the best in class. The fact is you can never make security perfect. However, benchmarking versus best practices gives organizations a way to evaluate their security/safety programs—how effective and how cost effective they are. Benchmarking also shows companies both how well their programs stack up and how well those programs are implemented. Simply, (1) benchmarking is a new way of doing business; (2) it is an objective-setting process; (3) it forces an external view to ensure correctness of objective setting; (4) it forces internal alignment to achieve company security/safety goals; and (5) it promotes teamwork by directing attention to those practices necessary to remain competitive. The benchmarking process is shown in figure 1.2.

**Start → Plan → Research → Observe → Analyze → Adapt**

**Figure 1.2 Benchmarking Process.**

Benchmarking can reveal

- how effective the organization or process is;
- how cost effective the organization or process is;
- Benchmarking shows security/safety engineers both how well their operations stack up and how well those operations are implemented.

Potential results of benchmarking:

- Benchmarking is an objective-setting process;
- Benchmarking is a new way of doing business;
- Benchmarking forces an external view to ensure correctness of objective setting;
- Benchmarking forces internal alignment to achieve plant goals;
- Benchmarking promotes teamwork by directing attention to those practices necessary to remain competitive;
- Benchmarking may indicate direction of required change rather than specific metrics which are as follows:
  - costs must be reduced
  - customer satisfaction must be increased
  - return on assets must be increased
  - improved maintenance
  - improved operational practices
  - best practices translated into operational units of measure.

## Targets

- Consideration of available resources converts benchmark findings to targets;
- A target represents what can realistically be accomplished in given time frame;
- A target can show progress toward benchmark practices and metrics;
- Quantification of precise targets should be based on achieving benchmark.

NOTE: Benchmarking can be performance based, process based, or strategic based and can compare financial or operational performance measures, methods or practices, or strategic choices.

## Benchmarking: The Process

When forming a benchmarking team, the goal should be to provide a benchmark that allows the security/safety engineer to evaluate and compare. The key to the learning process is looking outside one's own organization to other organizations that have discovered better ways of achieving improved performance, and determining how to apply these more effective methods to your own operation (see table 1.3).

**Table 1.3 Benchmarking Steps**

Step 1	Planning	Managers must select a process (or processes) to be benchmarked. A benchmarking team should be formed. The process of benchmarking must be thoroughly understood and documented. The performance measure for the process should be established (i.e., cost, time, and quality).
Step 2	Research	Information on the "best-in-class" performer must be determined through research. The information can be derived from the industry's network, industry experts, industry and trade associations, publications, public information, and other award-winning operations.
Step 3	Observation	The observation step is a study of the benchmarking subject's performance level, processes, and practices that have achieved those levels and other enabling factors.
Step 4	Analysis	In this phase, comparisons in performance levels among facilities are determined. The root causes for the performance gaps are studied. To make accurate and appropriate comparisons, the comparison data must be sorted, controlled for quality, and normalized.
Step 5	Adaptation	This phase is putting what is learned throughout the benchmarking process into action. The findings of the benchmarking study must be communicated to gain acceptance, functional goals must be established, and a plan must be developed. Progress should be monitored and, as required, corrections in the process made.

Note: Benchmarking should be interactive. It should also recalibrate performance measures and improve the process itself.

## THE BOTTOM LINE

In addition to the critical dependencies for the CS sector mentioned to this point it is important to note that physical security of sector facilities (covered in detail later) is important but, actually, the focus of security of this sector is a different kind and relatively new to most. Much of the CS infrastructure is vulnerable to cyberattack from either inside or outside of the network. Cyber security is addressed later. Also, CS infrastructure is extremely dependent on the IT sector (covered in detail in one of the volumes in this series).

The bottom line is that from this discussion, it is clear that any number of interdependencies could threaten one of the key components of our critical national infrastructure, the CS sector. These factors are the “realities” of the CS sector and go beyond just the core precepts of good system development and design. Clearly, there is a great deal of interdependence on other outside factors that could threaten CS and other key resources. Without the active participation of each of these sectors, the key and essential facilities of the CS industry could be very vulnerable a fact that is not acceptable for the protection of our national interests.

## REFERENCES AND RECOMMENDED READING

- Department of Homeland Security (DHS). 2015. *Commercial Facilities Sector-Specific Plan—An Annex to the National Infrastructure Protection Plan*. Washington, DC: DHS.
- Haines, Y.Y. 2004. *Risk Modeling, Assessment, and Management*. 2nd Edition. New York: John Wiley & Sons, p. 699.
- Henry, K. 2002. “New Face of Security.” *Gov. Security*, April, pp. 30–37.
- National Strategy for Homeland Security, Homeland Security Council, October 2007. [https://www.dhs.gov/xlibrary/assets/nat\\_strat\\_homelandsecurity\\_2007.pdf](https://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf).
- Sauter, M.A., & Carafano, J.J. 2005. *Homeland Security: A Complete Guide to Understanding, Preventing, and Surviving Terrorism*. New York, NY: McGraw-Hill.
- Spellman, F.R. 1997. *A Guide to Compliance for Process Safety Management/ Risk Management Planning (PSM/RMP)*. Lancaster, PA: Technomic Publishing Company.

## *Chapter 2*

# **Sector Profile**

The primary goal of terrorism is twofold: to invoke shock and to instill fear.

While it is difficult to pinpoint an exact definition of terrorism (but not difficult to rename it and call it something else), we certainly have little difficulty in identifying it when we see it, when we feel it, when we suffer from it. By any other name terrorism is best summed up as an absolute feeling of Terror—nothing judgmental about that—just Terror with a capital *T*. Terror!

### **INTRODUCTION**

The CS sector is made up of an extremely diverse range of sites and assets where large numbers of people congregate daily to conduct business, purchase retail products, and enjoy recreation events and accommodations. The majority of facilities has open public access and houses the business activities and commercial transactions that dominate the U.S. economy. CS stakeholders must balance security priorities with their need for open access, public confidence, and economic vitality. In general, commercial facilities are privately owned and operated with minimal oversight from federal, state, and regional government regulatory entities: however, government facilities may reside within commercial properties. Assets can range from as small as one-room museum to stadiums that can host events large and high-profile enough to be designated as National Special Security Events (NSSEs) by the Secretary of Homeland Security (DHS, 2015).



## KEY SECTOR OPERATING CHARACTERISTICS

The following overview provides a snapshot of CS sector assets operations (DHS, 2015).

- **Open public access**—Facilities and events operate on the principle of open public access, meaning people may move freely through the facilities without the deterrent of highly visible security barriers. This layout can go against design security principles. Additionally, high-profile tenants, neighbors, and special events may add risks to individual assets.
- **Soft targets with limited security barriers**—Many facilities are considered soft targets—sites that are relatively vulnerable to a terrorist attack due to their open access and limited security barriers. This makes intelligence and information sharing especially critical in recognizing and monitoring trends and thwarting attacks.
- **Nationally and internationally recognize icons with large population densities**—Many facilities, such as stadiums, malls, and museums, are nationally and internally recognized icons and have large population densities when occupied, which increases their likelihood of being targeted by adversaries. Facility attendance can act as a barometer of public confidence in national security.
- **Large national security interest**—High economic significance and public safety implications result in a large national security interest in facilities that are privately owned and secured. This dynamic necessitates a strong information-sharing relationship between owners and operators and their federal, state, and regional government intelligence partners.
- **Widely dispersed**—Although commercial facilities are widely dispersed, certain subsectors (e.g., gaming and entertainment and media) are concentrated in specific regions, necessitating regional security coordination between private and government partners.
- **Impact on the economy**—Given CS sector's significant impact on the economy, reestablishing the sector's assets after a disaster is required to ensure local and state financial security.

## COMMERCIAL SERVICES SECTOR SNAPSHOT<sup>1</sup>

### Assets, Impacts, and Owners/Operators

- **Entertainment and media**—The U.S. media and entertainment industry is the largest in the world. At \$735 billion, it represents a third of the global media and entertainment industry.

---

<sup>1</sup> The following material is from U.S. Department of Homeland Security *Commercial Facilities Sector—Specific Plan* (2015). Washington, D.C.

- **Gaming**—There were over 19,000 gaming locations in the United States in 2017. Commercial casinos contributed \$9.23 billion dollars in direct gaming taxes to state and local governments across the country (American Gaming Association, 2018).
- **Lodging**—There are more than 54,200 hotel properties with over 5 million guestrooms. Each year, there are over 1.1 billion guest nights in hotels in the United States (American Lodging and Hotel Association, 2019).
- **Outdoor events**—Fairs, exhibitions, outdoor venues, parades, and hundreds of amusement and theme parks are all included as outdoor events.
- **Public assembly**—There are 124,773 establishments: stadiums, arenas, movies theaters, and cultural properties such as museums, zoos, libraries, and performance venues (U.S. Census Bureau, 2015b).
- **Real estate**—The Commercial Buildings Energy Consumption Survey (CBECS) estimates that there were 5.6 million commercial buildings in the United States in 2012, comprising 87 billion square feet of floorspace. This level represents a 14 percent increase in the number of buildings and a 21 percent increase in floorspace since 2003 (Energy Information Administration, 2015).
- **Retail**—Total sales from the nearly 3.8 million retail establishments in the United States reached about \$2.6 trillion in 2016. Retailers employ almost 29 million, and support more than 42 million jobs in the United States. According to the National Retail Federation, retail industry sales are expected to increase 3.4 percent, with e-commerce retail sales expected to grow 7–10 percent (SelectUSA).
- **Sports leagues**—In 2018, nearly 131 million people attended game in the four major sports leagues—the National Football League (NFL), the National Basketball Association (NBA), the National Hockey League (NHL), and Major League Baseball (MLB) (ESPN).
- **Owners and operators**—The majority of the CS Sector is privately owned and operated, but includes publicly traded companies and some publicly owned buildings (e.g., libraries, museums). Owners and operators assess vulnerabilities of their specific facilities and practice prudent risk management and mitigation measures. Individual owners and operators most commonly provide funding of security and residence programs, making cost a significant challenge to implementing modern security programs (DHS, 2015).

## SECTOR COMPONENTS AND ASSETS

The CS sector profile is best described by defining the services offered by its subsectors. The sector is divided into eight subsectors—entertainment and media, gaming, lodging, outdoor events, public assembly, real estate, retail, and sports leagues—to facilitate coordination among facilities with similar

functions, operations, and security issues. The Retail Subsector is further divided into two councils, the Shopping Center Subsector Council, which includes mall developers, and the Council of Retailers, which includes stores within malls and stand-alone retail establishments. The following sections provide brief overviews of the assets and key security and resilience considerations unique to each subsector.

Keep in mind that despite their differences, nearly all commercial facilities are privately owned and operated with minimal regulations. Structures and establishments in every subsector are almost entirely regulated at the state and local levels through building codes and requirements geared toward improving the safety of employees and visitors. Federal oversight is mostly limited to safety- or access-related requirements of the Occupational Safety and Health Administration (OSHA) and American with Disabilities Act (ADA), or standards from the National Fire Protection Associate (NFPA).

These codes and regulations are not focused on resilience. (*Note:* Chapter 3 of this book focuses exclusively on resilience, the measurement of, because when you get right down to it, survival is all about resilience.) Anyway, as a result of the codes and regulations non-focus on resilience, individual owners and operators take responsibility for assessing facility risks and implemented risk management and mitigation actions. Owners and operators within each subsector have formed associations, working groups, the Real Estate Information Sharing and Analysis Center (RE-ISAC), and other mechanism to facilitate intelligence and risk information sharing and to exchange best practices and tools for security and resilience (DHS, 2015).

## Entertainment and Media Subsector

This subsector encompasses films, movie theaters, TV subscriptions, and electronic home video production, and distribution and consumption. Box office receipts reached just over \$11 billion in 2017 (this figure includes cinema advertising earnings of \$881 million), and home video reached \$107.9 billion in 2017. The TV market and television subscriptions will remain static at \$100.8 billion through 2018. Competition is heating up from the new digital economy, and streaming video on demand (SVOD) is growing rapidly. This sector enjoyed a trade surplus of \$13.3 billion in 2015 (latest available data), which was 5 percent of the total U.S. private sector services trade surplus that year.

### *Key Asset Considerations*

- **Relatively limited access**—Unlike the majority of the CS sector, entertainment and media subsector facilities are generally closed to the public and employ visible security barriers and access control measures.

- **High-profile celebrities and media outlets**—High-profile celebrities are regularly present on studio sites, requiring security producers to deal with the public, paparazzi, and stalkers. Stars often have private security details as well. Recently, the paparazzi have started to use drones to capture pictures in studio areas. News and broadcasting facilities may also attract the attention of attackers due to their high public profile. This may particularly affect facilities in large metro areas where the public can park and congregate near broadcast buildings.
- **Geographical concentration**—Major movie studios are located in relatively close proximity in the Los Angeles area and often have corporate affiliations with television studios in the New York City area.
- **Self-contained services**—Primarily on the West Coast, larger movie studios operate like small cities and maintain their own emergency services equipment and personnel. The studios also coordinate closely with each other, county and city police and fire departments. In some cases, studio employees receive search and rescue, earthquake response, and emergency medical service training.
- **Hacking and piracy**—Hacking and piracy are major concerns for studios. The distribution of a film prior to its release or the release of business documents and correspondence could cost a studio millions of dollars. Employees use electronic access cards to enter studio sites and are subject to many of the same security measures as visitors (e.g., searches).

## Gaming Subsector

Consumer spending on casino gaming surpassed \$40 billion for the first time in 2017. This represented an increase of 3.4 percent from 2016. The 460 casinos in the United States generated \$9.23 billion in direct gaming tax revenue in 2017.

According to the National Indian Gaming Commission, there were 238 gaming tribes with 474 gaming operations. In 2015 gross gaming revenues equaled nearly \$30 billion which was a 5 percent increase from 2014. This was the largest increase in ten years.

### *Key Asset Considerations*

- **Small cities**—A large gaming facility complex is like a small city, with numerous types of large facilities (e.g., casinos, convention centers, performance venues, hotels, restaurants, and shopping centers) under one roof. In major casino markets, gaming facilities are grouped close together in a “strip” area, creating several small cities in a relatively small geographical area. These gaming facilities employ large staff and welcome large numbers of visitors.

- **24/7 operations**—The casino portion of a gaming facility complex operates under an open public access model, 24 hours a day, 7 days a week. Although there may be access control measures in other parts of the complex (e.g., tickets are required in a theater), casino customers enter and exit the facility continuously and freely.
- **Sophisticated surveillance**—Casino gaming complexes are typically a mix of open/unrestricted access (gaming and restaurant areas) and also highly restricted access areas (closed-circuit television, security command, information technology, and currency storage area that contain large amounts of cash). Although access controls are not employed to gain entrance onto a casino floor, a sophisticated array of surveillance measures continuously monitors activities in that area. State gaming commissions regulate the gaming part of casino operations and can establish specific standards for security and surveillance (e.g., the number and type of cameras, pixels of resolution, the number of security guards in the gaming areas).

## Lodging Subsector

This subsector includes nongaming resorts, hotels and motels, hot-based conference centers, and bed-and-breakfast establishments. Travel and tourism generated over \$1.5 trillion in economic output in 2016, supporting 7.6 million jobs. One out of every eighteen Americans is employed, either directly or indirectly, in a travel or tourism-related industry. In 2016, U.S. travel and tourism output represented 2.7 percent of gross domestic product.

The accommodations subsector under travel and tourism accounts for 19 percent of total travel and tourism spending. People spent nearly \$300 billion on traveler accommodations in 2016. This sector supports more than 3.4 million U.S. jobs.

### *Key Asset Considerations*

- **Continuous occupancy**—Unlike many other commercial facilities, hotel and motels are occupied around the clock. People can eat, sleep, conduct business, and take part in entertainment activities within the same facility over multiple days.
- **Emergency shelters**—Hotels and motels have been used as shelters during natural disasters. Owners and operators have performed services such as collaborating to find rooms for disaster victims and making properties available in times of need.
- **Self-contained**—Some hotels operate similar to small cities. They are capable of generating their own electrical power, and they operate their own water filtration and wastewater treatment facilities. Many full-service hotels have restaurants, shops, and meeting rooms. Convention centers, shopping

malls, sports facilities, office buildings, and public transportation facilities may be adjacent to or integrated into the hotel facility.

- **Just-in-time buyers**—Many hotels are “just-in-time” buyers. They often rely on the Internet to place orders and on the transportation and commercial distribution systems to deliver goods and services when needed. This results in fresh food and supplies being available without the need to store, prepare, or process them on-site. However, this reliance on just-in-time supply chains creates the potential for a lack of sufficient supplies if the hotel is used for shelter during a disaster.
- **High-profile guests and events**—High-profile hotel guests—such as dignitaries and celebrities—and events—such as a military ball or religiously affiliated conference—increase a hotel’s security risks. This requires security procedures to ensure a facility’s resilience. Clients and events may also provide private security details.

## Outdoor Events Subsector

This subsector includes amusement parks, fairs, exhibitions, parks, parades, marathons, and other outdoor venues and events. Thousands of fairs are held in North America each year, including large state fairs with an attendance of more than a million people in a two- or three-week period. Parades in large cities can draw millions of spectators, such as the Macy’s Thanksgiving Day Parade, which attracts millions of people to the streets of New York City each year, and is watched on television by another 50 million people. Although this subsector represents those activities and gatherings of people that take place outdoors there are usually buildings (e.g., restaurants, snack bars, hotels, shops, barns, and exhibition halls) associated with the activity. The outdoor nature of the event may sometime result in attendees being spread out over a larger area than they would have been if the event had taken place in an enclosed structure.

### *Key Asset Considerations*

- **Diversity**—The Outdoor Events Subsector represents an exceptionally diverse range of facilities and activities, from large, established theme parks with annual attendance in the millions, to festivals and parades with attendance in the thousands over a period to hours.
- **Perimeter**—Some events (e.g., parades, festivals, and carnivals) take place not only outside, but in an open environment with no established perimeter or access controls.
- **Seasonality**—Many outdoor events are seasonal or last only a few weeks, days, or hours. Vendors and suppliers, as well as security personnel who service the event, are not permanent employees, but are hired for the length

of the event. Some employees are foreign nationals, working through visas that allow for temporary, nonagricultural jobs. In addition, large numbers of volunteers may be involved in staffing the event.

- **Small cities**—Some of the larger theme parks may function like small cities, with restaurants, hotels, and other diverse facilities on the premises.
- **Ownership**—The assets are generally owned and operated by private sector companies or cooperatives, although local government may own or sponsor some venues, such as public parks or fair grounds.

### Public Assembly Subsector

This subsector includes assets where a large number of people congregate: movie theaters, convention centers, auditoriums, stadiums, arenas, and cultural properties (e.g., museums, zoos, planetariums, aquariums, libraries, and performance venues). Many of these facilities experience high levels of attendance. This subsector also has a significant effect on the economy. Box office receipts were over \$11 billion in 2017 including cinema advertising earnings of \$881 million. Box office numbers are projected to increase as theaters adopt digital screens, increase prices, and diversify consumer options. Museums also have a substantial impact on the economy contributing \$50 billion per year while supporting over 726,000 jobs in the United States (American Alliance of Museums)

#### *Key Asset Considerations*

- **Diversity**—The size, utilization, and owner-management formats of public assembly facilities vary greatly, for example, museums, and libraries may be found in one room of a building or incorporate multiple buildings located throughout a city or state.
- **Emergency shelters**—Public assembly facilities provide extended shelter and comfort for displaced individuals during an incident. These facilities may also serve as emergency services command centers for local and federal first responders.
- **Ownership**—Public assembly facilities that are privately owned and operated are more likely to utilize a private security company.
- **Command center**—Many Public assembly facilities with high attendance numbers use a command center to monitor activities. This can serve as an operations center in the event of a man-made or natural incident.

### Real Estate Subsector

This subsector includes office buildings and office parks, apartment buildings, multifamily towers and condominiums, self-storage facilities, and

property management companies. According to the latest survey by Energy Information Administration, there were approximately 5,557 commercial buildings in the United States in 2012. More than 88 million workers were employed in these buildings. Nearly 76 percent of these building only had one establishment while 0.5 percent had more than twenty.

Traditionally, terrorists have selected buildings (primarily commercial buildings) as the preferred target of attacks. The collapse or failure of these buildings can have a severe effect on all sectors of the economy—including federal, state, and local government resources, and can result in significant loss of life.

### *Key Asset Considerations*

- ***Continuous occupancy***—The real estate subsector experiences continuous occupation because the public both lives and works within this subsector’s facilities.
- ***Division of responsibility between owners and operators***—Tenants renting space in commercial real estate facilities, such as commercial office buildings and residential buildings, are typically responsible for their own safety in any scenario short of emergency evacuation, and each has their own corporate security and polices. The property manager of a facility is responsible for perimeter access controls and continuity of critical functions (e.g., water pumps, heating and air conditioning system evacuation planning) as well as lifeline services supplied by local utilities.
- ***Tenant/resident identification***—Residential property owners and operators screen all rental applicants using credit reports, criminal background databases, and federal terrors watch lists prior to granting residency. This information is used to ensure the suitability of the renter, financial security for the owner, and the safety of existing and future building occupants. Some buildings house high-risk tenants (e.g., high-profile government tenants) and special-use tenants (e.g., banking facilities) or a mixture of both high- and low-risk tenants.
- ***Subcontracting***—A vulnerability of the commercial real estate industry is the lack of security controls with regard to cleaning and groundskeeping services, including the issue of illegal subcontracting. Many janitors, for example, have nearly unlimited access to a building’s sensitive areas during and after working hours. If this position were illegally subcontracted, it could allow terrorists, criminals, and former or disgruntled employees to infiltrate and exploit a building.
- ***Faith-based facilities***—Although religious facilities sometimes reside within commercial real estate facilities, the CS sector is not the sector-specific agency for these organizations. The Homeland Security Advisor



Council established the Faith-based Communications and Security Advisory Committee to provide recommendations and exposure current and potential security information-sharing opportunities and methods between the Department of Homeland Security and faith-based organizations (DHS, 2015).

## Retail Subsector

This subsector includes tenant space in enclosed malls, shopping centers, and strip malls, as well as freestanding retail establishments. As previously mentioned, sales from 3.8 million retail establishments reached \$2.6 trillion in 2016. By the end of 2017, foreign direct investment in the retail industry in the United States reached \$100 billion. According to the National Retail Federation, privately held retail businesses account for 95 percent of the retail industry. While brick and mortar stores are still the face of the industry, online sales are expected to increase.

### *Key Asset Considerations*

- **Multiple access points**—Retail establishments have open access for the public, and do not require fees, tickets, or reservations. Establishments have more than one access point for customers, personal vehicles, and delivery trucks.
- **Frequency and volume of people**—Retail establishments are surrounded daily by a steady flow of traffic because they provide basic necessities to the population. In the case of enclosed malls that house independently owned retail tenants, controlling who enters and exits is especially difficult. Patrons also generally carry bags and packages within shopping facilities, which could easily conceal various types of weapons.
- **Highly competitive**—Competition and economic conditions force owners and operators to minimize highly visible or obtrusive protective measures, because these can make prospective patrons uneasy. Retailers strive to maintain the highest reputation possible because customers can easily go elsewhere.
- **Dependence on global supply chains**—Retailers rely on a continuous flow of goods and products, many of which are manufactured overseas and are shipped to the United States, making them vulnerable to supply chain interruption due to port closures, terrorist attacks, or natural disasters.
- **Retail stores as distribution centers during disasters**—Retail distribution centers, such as home improvement stores, supply key resources during disasters, and many response plans use shopping centers as distribution points, with the assumption these facilities will still be operational. During

disasters, the Retail Subsector has played a role in information sharing and donating supplies, services, and money.

- **Reliance on point-of-sale cyber systems**—Retailers rely on point-of-sale cyber systems for financial transactions. These systems have been successfully attacked by hackers, and will likely continue to be targeted in the future.

## Sports Leagues Subsector

This subsector includes major sports leagues and federations. Over 4,000 establishments (U.S. Census Bureau, 2017) related to spectator sports are spread across the United States, and the industry supports more than 133,000 jobs (USDOL, 2015). The Sports Leagues Subsector is closely related to the Public Assembly Subsector. These facilities share many of the same characteristic, demographics, and, in many cases, owner-management relationships.

### *Key Asset Considerations*

- **Ownership/owner-lessee agreements**—In most situations, another entity (e.g., a local government or authority) owns the facility where sports teams hold their events. In many cases, these facilities are also considered multipurpose because other sporting events and different activities (e.g., trade shows, conventions, conferences, and concerts) are held in the same facility. Many of the large venues used in the four major sports leagues are also privately owned.
- **Emergency shelters**—Sports Leagues Subsector facilities may be designated as mega-shooters and used to house evacuees from a major disaster area, such as during wildfires or hurricanes. During an incident, facilities may also act as temporary shelter for displaced individuals or as an emergency services command center for local and federal first responders.
- **Command centers**—Many sports league facilities with large attendance use a command center to monitor activities and to serve as operations center in the event of a man-made or natural incident.
- **Security**—For these facilities, security may be handled by local law enforcement or by a private company, or a mixture of the two.
- **Support Anti-terrorism by Fostering Effective Technologies Act (SAFETY Act)**—Established in 2002, the SAFETY Act created liability limitations for claims resulting from an act of terrorism where qualified anti-terrorism technologies have been deployed, encouraging anti-terrorism programs and technology in stadium applications. Since 2008, the NFL's Best Practices for Stadium Security, Major League Baseball's All Star Game, and several sporting venues have received SAFETY Act protections. Facilities in other

subsectors have also received SAFETY Act protections, and the CS sector is working to raise awareness among the whole sector (DHS, 2015).

## REFERENCES AND RECOMMENDED READING

- American Alliance of Museums (AAM). 2016. "Museum Facts." <http://www.aam-us.org/about-museums/museum-facts>.
- American Gaming Association (AGA). "2018 State of the States." [https://www.americangaming.org/wp-content/uploads/2018/08/AGA-2018-State-of-the-States-Report\\_FINAL.pdf](https://www.americangaming.org/wp-content/uploads/2018/08/AGA-2018-State-of-the-States-Report_FINAL.pdf).
- American Gaming Association. 2015. "Groundbreaking New Research Reveals Impressive Magnitude of U.S. Casino Gaming Industry." <https://www.gettoknowgaming.org/news/groundbreaking-new-research-reveals-impressive-magnitude-us-casino-gaming-industry>.
- Association of Zoos and Aquariums. 2018. "Zoo and Aquarium Statistics." <https://www.aza.org/zoo-and-aquarium-statistics>.
- DHS. 2015. *Commercial Facilities Sector—Specific Plan*. Washington, DC: U.S. Department of Homeland Security.
- ESPN. "2018 NFL Attendance." <http://www.espn.com/nfl/attendance>.
- ESPN. "2018 MLB Attendance." [http://www.espn.com/mlb/attendance/\\_/year/2018](http://www.espn.com/mlb/attendance/_/year/2018).
- ESPN. "2017–2018 NHL Attendance." [http://www.espn.com/nhl/attendance/\\_/year/2018](http://www.espn.com/nhl/attendance/_/year/2018).
- ESPN. "2018 NBA Attendance." [http://www.espn.com/nba/attendance/\\_/year/2018](http://www.espn.com/nba/attendance/_/year/2018).
- Federal Communications Commission. 2014. "Broadcast Station Totals." <https://www.fcc.gov/media/broadcast-station-totals>.
- Haimes, Y.Y. 2004. *Risk Modeling, Assessment, and Management*. 2nd Edition. New York: John Wiley & Sons, p. 699.
- Henry, K. 2002. "New Face of Security." *Gov. Security*, April, pp. 30–37.
- Motion Picture Association of American. 2002. "The Economic Contribution of the Motion Picture Industry of the United States." <https://www.mpa.org/what-we-do/driving-economic-growth/>.
- National Association of Broadcasters. 2018. "Frequently Asked Questions about Broadcasting." <http://www.nab.org/documents/resources/broadcastFAQ.asp>.
- National Retail Federation (NRF). 2016. "National Retail Federation Annual Report." <https://nrf.com/annual-reports>.
- Sauter, M.A. & Carafano, J.J. 2005. *Homeland Security: A Complete Guide to Understanding, Preventing, and Surviving Terrorism*. New York, NY: McGraw-Hill.
- SelectUSA. <https://www.selectusa.gov/welcome>.
- Spellman, F.R. 1997. *A Guide to Compliance for Process Safety Management/ Risk Management Planning (PSM/RMP)*. Lancaster, PA: Technomic Publishing Company.
- United States Department of Labor. Bureau of Labor Statistics (BLS). "May 2018 National Industry Specific Occupational Employment and Wage Estimates." <https://www.bls.gov/oes/current/oessrci.htm>.

- U.S. Census Bureau. "Statistics of U.S. Businesses." <https://www.census.gov/programs-surveys/susb/about.html>.
- U.S. Energy Information Administration. 2015. "Commercial Buildings Energy Consumption Survey." <https://www.eia.gov/consumption/commercial/reports/2012/preliminary/index.php>.
- U.S. Travel Association. 2014. "Travel Exports: Driving Economic Growth and Creating American Jobs." [https://www.ustravel.org/sites/default/files/media\\_root/2014\\_Export\\_Report-PDF-FINAL.pdf](https://www.ustravel.org/sites/default/files/media_root/2014_Export_Report-PDF-FINAL.pdf).



## *Chapter 3*

# **Resilience Measurement Index**

**ANTICIPATE**

**RESIST**

**ABSORB**

**RESIST TO**

**ADAPT TO**

**RECOVER FROM DISTURBANCE**

**RESILIENCE = ANTICIPATION + ABSORPTION +  
ADAPTATION + RECOVERY**

If an entity is any part of critical infrastructure, responsible persons in charge of the entity must assume they are targets of terrorists or of any other radicalized nutcase. Thus, the question is not when you will be attacked or when your property will be utilized for an attack (remember, Mandalay Inn in Las Vegas), but instead you have to ask can you, your employees, and your property survive an attack—are you resilient?

—Frank R. Spellman

“America is no longer protected by vast oceans. We are protected from attack only by vigorous action abroad, and increased vigilance at home.”

—President George W. Bush (2002)

### KEEP IN MIND!

As noted by that great philosopher (Bob Dylan, of course) in the song: “The Times They Are A Changing” . . . recent terrorist events have made this well worn statement certainly the case. For example, with the manifestation of the Islamic State of Iraq and Syria (ISIS), also known as the Islamic State of Iraq and the Levant (ISIL) and by its Arabic language acronym Daesh and other terrorist groups including inside and outside fanatics there are many out there who would kill us all. It is important to point out with the advent of insider threats the message of this book is the same as the other books in this series where the focus has been shifted to the Lone Wolf (or as Williams VII and others of her blood stated in other prologues, lone Utah Raptor) terrorist. The fact is there are homegrown terrorists who live among us, plotting, quivering in the glory of mass murder, blood and guts and beheadings, destruction and the attended glory of making the headlines as martyrs in the sickest sense possible (remember the Mandalay in Las Vegas). Again, remember, these are people who live among us, who shop in our stores, who use the benefits of our free society to grow their hate and to enhance their total disgust for all those things that we value in life.

### INTRODUCTION<sup>1</sup>

It was not that far in America’s distant past that we dealt mostly with the ramifications of natural disasters: Hurricane Katrina in 2005 and Superstorm Sandy in 2012. We also experienced the human-made Northeast Blackout event in 2003. All of these events were horrific or at least shocking. Okay, then to this terrible mixture let’s add 9/11, the World Trade Center in 2001. This event had even more far-reaching impacts that have (and continue to) directly affected our society’s well-being. Even though current efforts that have focused on preventing or mitigating the impact of incidents have achieved admirable results, a more comprehensive approach is needed to the nation’s overall resilience. Beyond resilience, which is an absolute must, we must also accomplish, practice, and maintain preparedness, mitigation, response, and recovery programs and capabilities, all of which make resilience a reality.

---

<sup>1</sup> Much of this chapter is based on U.S. Department of Energy’s 2013 Argonne National Laboratory: *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience*. Washington, DC.

Presidential policy Directive 21 defines sixteen critical infrastructure sectors that are essential to the nation's security, public health and safety, economic viability, and general quality of life (White House, 2013). Because the operations of these critical infrastructure sectors are essential, their protection and resilience is paramount. As the DHS (2010a) points out, "our goal is to ensure a more resilient Nation—one in which individuals, communities, and our economy can adapt to changing conditions as well as withstand and rapidly recover from disruption due to emergencies."

Developing and enhancing resilience of critical infrastructure requires its owners/operators to determine the ability of the system to withstand specific threats, minimize or mitigate potential impacts, and to return to normal operations if degradation occurs. Accordingly, a resilience methodology requires the comprehensive assessment of critical infrastructure systems/assets—from threat to consequence. The methodology needs to support decision-making for risk management, disaster response, and business continuity. Considering these issues, Argonne Nation Laboratory, in partnership with U.S. DHS, has developed an index, the Resilience Measurement Index (RMI), to characterize the resilience of critical infrastructure.

The RMI was formulated to capture the fundamental aspects of resilience for critical infrastructure with respect to all hazards. The RMI methodology supports decision-making related to risk management, disaster response, and maintenance of business continuity. It complements other indices that have been developed—the Protective Measure Index and the Consequences Measurement Index (CMI)—and thus, in combination with other tools allows critical infrastructure to be compared in terms of resilience, vulnerability, consequences, and ultimately risk. The main objective of the RMI is to measure the ability of a critical infrastructure to reduce the magnitude and/or duration of impacts from disruptive events.

The RMI is based on multi-attribute theory and decision analysis principles. Resilience, in the context of critical infrastructure, is defined as the ability of a facility or asset to anticipate, resist, absorb, respond to, adapt to, and recover from a disturbance (Carlson et al., 2012). These six elements are aggregated into four major (Level 1) components: preparedness, mitigation measures, response capabilities, and recovery mechanisms.

The DHS Enhanced Critical Infrastructure Protection Program's Infrastructure Tool provides the Level 1 indices and overall RMI for an asset facility. The indices are based on the aggregation of pertinent components in the Infrastructure Survey Tool (IST). Each of these components has been weighted by SMEs to indicate its relative importance to a facility's resilience. The value of the RMI ranges between 0 (low resilience) and 100 (high resilience). Note that a high RMI does not mean that a specific event will not affect the facility or have severe consequences. Conversely, a low RMI does



not mean that a disruptive event will automatically lead to a failure of the critical infrastructure and to serious consequences. The RMI instead is used to allow critical infrastructure facilities to compare their level of resilience against the resilience level of other similar facilities (aka benchmarking) nationwide and guide prioritization from improving resilience.

### **ISM RMI Dashboard**

All the data and levels of information used for the RMI, as well as the value of its four Level 1 components, are present on an interactive, web-based tool called the IST RMI Dashboard. The Dashboard provides a snapshot of the resilience of a critical infrastructure at a specific point in time. The Dashboard provides valuable information to owners/operators about their facility's status relative to those of similar assets. The Dashboard can be used to create scenarios and assess the implementation of specific resilience measures or procedures that the facility owner/operator might consider. Using a Dashboard's interactive "Facility Scenario" function makes it possible for the facility owner or operator to select possible resilience enhancements and immediately see the resulting modified RMI. Policies, procedures, or operational methods are enhancements with which the facility may increase resilience.

Experience has shown that combining the RMI information with other indices, such as the Protective Measure Index and the CMI, allows for a comprehensive assessment or risk that can support decision-making about protection, business continuity, and emergency management of critical infrastructure.

### **THE 411 ON THE RMI**

The goal of the RMI is to find a facility's weakest link. In light of this goal, in 2009, the U.S. DHS and its protective security advisors (PSAs) began surveying critical infrastructure using the IST and ultimately produced individual protective measure and vulnerability values through the Protective Measures Index (PMI). This index identifies the protective measures posture of individual facilities at their weakest link, allowing for a survey of the most vulnerable aspects of the facilities.

As critical infrastructure continued to be surveyed using the IST and displayed using the PMI, Argonne National Laboratory, in partnership with the DHS, developed an index for surveying the resilience of critical infrastructure—the RI.

In the practical usage of the RI it became obvious to the users that the index could be improved by better considering elements contributing to business continuity, continuity of service, cyber risk, and resource dependencies. The first requirement for the enhanced RI was a modification of the IST question set. Modification of the IST provided more information on the elements contributing to dependencies on external providers, business continuity, and emergency management.

The development of this new indicator of resilience, named the RMI, was guided by the standards used for the voluntary Private Sector Preparedness Program (PSPrep) and National Security Directive PPD-8. The PSPrep program is based on three main standards (British Standards Institute 25999, NFPA 1600, and ANSI/ASIS SPC.1-2009), which provide a comprehensive management systems approach to organization resilience, preparedness, and business continuity (Federal Emergency Management Agency, 2013). PPD-8 focuses on national preparedness for strengthening the security and resilience of the nation. It promotes an all-hazards approach based on the identification of core capabilities necessary for communities to be better prepared for significant destructive incidents (Department of Homeland Security, 2011).

Resilience measurement must be organized in a way that is consistent with emergency and risk management processes. To accomplish this, the RMI is based on the same methodologies (multi-attribute utility theory [MAUT] and decision analysis) as the RI but organizes the components in terms of preparedness, mitigation measures, response capabilities, and recovery mechanisms.

Combining a pre-incident focus with an enhanced understanding of resilience allows owners/operators to identify improved ways to decrease risk by (1) increasing preparedness for an incident, (2) implementing redundancy to mitigate the effects of an incident, and (3) enhancing emergency action and business continuity planning and implementation to increase the effectiveness of response and recovery procedures. Information provided by the RMI methodology is used by facility owners/operators to better understand how their facilities stack up against similar sector/subsector sites and to help them make risk-informed decisions. This information can also be used for decreasing risk and improving resilience at the regional level. Resilience for the nation includes both critical infrastructure and other components. As stated by Carlson et al. (2012), “The resilience of a community/region is a function of the resilience of its subsystems, including its critical infrastructures, economy, civil society, governance (including emergency services), and supply chains/dependencies.” It is important to point out, however, that additional data and methods must be used to capture the resilience of a community/region or the nation.



**Figure 3.1 Risk Elements.**

## RISK, VULNERABILITY, AND RESILIENCE

DHS defines risk as “the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences” (Department of Homeland Security, 2010b). Risk is thus traditionally defined as a function of three elements: the *threats* to which an asset is susceptible, the *vulnerabilities* of the asset to the threat, and the *consequences* potentially generated by the degradation of the asset (see figure 3.1).

### CS Sector Risks<sup>2</sup>

Note that the CS sector is one of the few U.S. critical infrastructures in which terrorists have executed multiple high-profile attacks directly affecting the public, both in the physical and cyber domain. The following section covers emerging risks to the CS sector and outlines the sector’s risk profile.

#### *Notable Trends and Emerging Issues*

- **Changing domestic and international terrorist threats**—The Boston Marathon bombing in 2013 highlighted the danger posed by homegrown violent extremists (HVEs)—lone actors or insular groups that are not directly tied to terrorist organizations. Federal counterterrorism experts consider HVEs to be “the most likely immediate threat to the homeland” (NCTC, 2014). The United States also faces growing threats from the terrorist group ISIL, those it inspires, and other international terrorist groups.

<sup>2</sup> Based on material in U.S. DHS *Commercial Facilities Sector—Specific Plan*. Washington, DC.

Insider threats—radicalized individuals who may work at a commercial facility and use their inside knowledge to exploit vulnerabilities—are also a growing concern.

- **Increasing interdependencies between sectors**—Cities and regions increasingly rely on complex networks or interconnected infrastructure that comprise and are operated and integrated by physical and cyber systems. After a disaster, a failure in one system—such as in the water or energy sectors, on which the CS sector relies strongly—could cascade and greatly affect the regions they serve.
- **Increased cyber risks**—Adversaries have successfully executed point-of-sale attacks on large retailers and hotels to gain access to confidential data, which has cost companies and financial institutions hundreds of millions of dollars. Governments have launched targeted cyber espionage of sabotage attacks, and there has been an increase in “Hacktivism,” or politically motivated cyberattacks. The Federal Bureau of Investigation (FBI) identified North Korea as the source behind recent cyberattacks that published thousands of confidential company documents online, including personal e-mail correspondences and employee data (Rasmussen, 2015). Building management systems—from heating, ventilations and air conditioning (HVAC) systems, to access control—are increasingly computerized, making a growing portion of operations vulnerable to a cyberattacks or IT outage. Due to the CS sector’s dependency on the Internet and IT, the failure or infiltration of cyber systems would create a significant negative economic impact on the sector.
- **Increasing use of social media**—Social media sites allow people to immediately document and disseminate information, making it crucial for the CS sector to respond to incidents quickly and efficiently. Social media brings both risks and benefits; for example, malicious actors could use social media to disrupt events, facilitate attacks, or organize flash mobs, but the sites may also contain valuable information that could aid security efforts during an event or recovery.
- **Emerging threats from the use of UAS**—The increased use of UAS, also called drones, and the absence of regulation is a growing threat for the CS sector. These devices are of serious concern and can be used to cause damage to persons and property, as well as cause alarm at CS events or locations. Drones also allow individuals to gain access to previously unreachable area, such as the air space above a stadium or movie studio, and could cause harm if armed with explosives.
- **Growing size and frequency of mass protests**—Social media is also facilitating “increasing rapid, broad, and coordinated protest activities” at CS facilities. Protests can pose sanitation, public safety, economic, and other risk to CS occupations and guests.

### *Significant CS Sector Risks*

The CS sector operates through a principle of open public access and experiences high-population densities, which can increase the vulnerability to intentional attacks that aim to harm public health and safety, cause property damage, and inflict economic and psychological consequences. In addition, many venues are highly recognizable, increasing the potential attractiveness to an adversary. The key risks affecting the security and resilience of CS sector assets, operations, and workforce include the following:

- **Natural disasters and extreme weather**—Increasingly severe weather events, including storms, earthquakes, floods, and droughts, can cause significant property and economic damage, threaten safety of employees and guests, and restrict access to critical resources such as power, water, transportation, and food supplies.
- **Armed attacker**—Armed-attacker events at shopping centers, office buildings, and open arenas are difficult to predict, particularly given the sector's open access design. Combating this threat requires advanced planning, resources, such as training material, and information sharing between CS subsectors and federal, state, and local security partners.
- **Pandemic**—A pandemic could severely threaten the large workforce of CS sector establishments, compromising facility operations or limiting services. Pandemics can also spread easily through CS facilities, as large groups of people congregate in them daily. This could have an economic effect on businesses if customers choose to stay home rather than risk infection. Many private businesses lack system-wide business continuity plans for catastrophic health emergencies. Plans must account for extreme health impact assumptions as well as containment.
- **Cyberattacks**—The sector widely uses the Internet for marketing, merchandising, ticketing, and reservations. A mass communications failure leading to a disruption of the Internet could affect the CS sector as a whole and have cascading economic effects. Cyberattacks could also cause a loss of operations for automated building systems, giving hackers access to automated building systems and internal surveillance footage, and result in the release of private information (e.g., customer credit card accounts, financial information, and internal correspondence).
- **Explosive devices**—Attackers have used homemade explosives, improvised explosive devices (IEDs), to attack commercial facilities with the aim of causing mass casualties and property damage. Open public access, particularly at outdoor events or facilities with limited screening, makes many facilities particularly vulnerable to explosives.
- **Chemical, biological, radiological attacks**—Terrorist organizations have expressed interest in acquiring chemical, biological, or radiological (CBR)

weapons, which can be widely dispersed through ventilation systems, food products, or liquids in an arena to inflict severe harm.

- **Mass protests**—Although the majority of mass protests have been peaceful, some have resulted in property damage and can pose sanitation, safety, and other risks to building occupants and guests.
- **Theft**—CS sector businesses are impacted by a range of theft-related crimes. For instance, organized theft of products and goods costs the Retail Subsector billions of dollars each year, and ATM-related thefts impact facilities in the real estate subsector. Intellectual property theft threatens a company's ideas and inventions, including trade secrets, proprietary products, media, and software.
- **Unmanned aircraft systems**—Malicious actors could use UAS or drones to gain security knowledge or private information about a facility or event, which could provide information that could be used for attacks. Drones could also be used for intellectual property theft, such as recording over stadiums or movie studios, or could be armed with a deadly weapon to execute terrorist attacks from the air. This could cause serious damage to persons and property. The CS sector is collaborating with the FAA to address drone safety and security.
- **Supply chain disruptions**—Incredibly efficient supply chains have resulted in a “just-in-time” delivery model—that leaves companies with very limited inventories, making some firms highly sensitive to supply disruptions. If raw materials are unable to reach company facilities, it can disrupt operations or hinder disaster response. Likewise, if finished products are unable to be delivered, it can have a significant economic effect on companies. Supply chain disruptions could result from a range of causes, including geopolitical unrest, natural disasters, or tainted or counterfeit products being introduced into the manufacturing stream. Shipment tracking and management, in particular, may rely on the GPS and its precise position, navigation, and timing data. A data disruption could create cascading supply chain disruptions.
- **Global political and social implications**—The CS sector includes companies with international operations, such as global hotel chains, resorts, retail companies, and theme parks. These organizations need to keep informed of international threats, since maintaining the integrity of their brand and safety and their employees and patrons necessitates remaining aware of global risks.

## Threats

*Threat* is a “natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property” (Department of Homeland Security, 2010b). Do

not confuse the term “hazard” or use it instead of threat because, as defined by the DHS lexicon, a *hazard differs from a threat in that a threat is directed at an entity, asset, system, network, or geographic area, while a hazard is not directed* (Department of Homeland Security, 2010b).

## Vulnerability

*Vulnerability* is a “physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard” (Department of Homeland Security, 2010b). Consequences are the “effects of an event, incident, or occurrence” (Department of Homeland Security, 2010b).

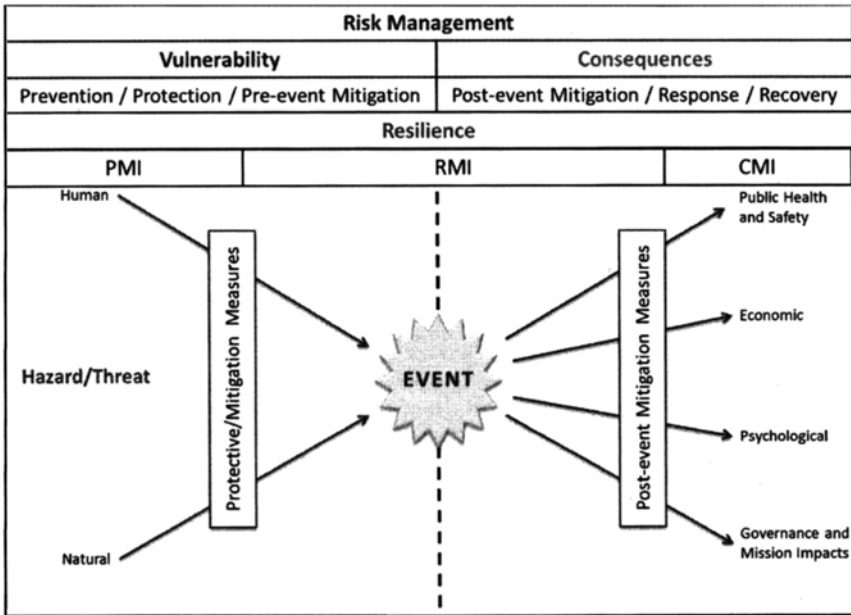
## Resilience

If risk is a function of threats and hazards, vulnerabilities, and consequences, the challenge is to define where and how resilience fits into the determination of risk. *Resilience*, as defined by DHS, is the “ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions” (Department of Homeland Security, 2010b). The DHS lexicon also states that “resilience can be factored into vulnerability and consequence estimates when measuring risk” (Department of Homeland Security, 2010b). On the basis of this statement, the facility resilience would have an effect on both vulnerability and consequences.

## Risk Management

Risk management can be defined as the “process of identifying, analyzing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level at an acceptable cost” (Department of Homeland Security, 2010b). Risk management involves knowing the threats and hazards that could potentially impact a given facility, the impacts on the facility due to its vulnerabilities, and the consequences that might result. On the basis of these characteristics, it is possible to develop specific indicators and metrics to assess the risk to an organization. The main objective is thus to analyze the performance of a facility in terms of protection/vulnerability, resilience, consequence, and, ultimately, risk; and to propose options to improve this performance, see figure 3.2.

How threats, vulnerability, consequences, and resilience fit together in a risk management process is illustrated in the risk management bowtie diagram presented in figure 3.2. Considering a threat or hazard (natural or human-made), the vulnerability and resilience of an organization will impact the potential consequences of an event. The interaction between the elements



**Figure 3.2 Risk Management Bowtie Diagram.** *Source:* U.S. Department of Energy. "Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience."

of risk is complex, and made more so when one considers that transfer of risk between assets in the case of a threat by an intelligent adversary. For example, when protection at a site is increased, vulnerability decreases and the risk at that site declines, but the risk at another site or sites may increase (Phillips et al., 2012).

The PMI developed in 2008 was the first index as part of the DHS Enhanced Critical Infrastructure Protection (ECIP) program. This index captures the protective measures in place in a given facility (Fisher et al., 2009; Petit et al., 2011). The fourth edition of this index, launched in January 2013, addresses elements characterizing physical security, security management, security force, information sharing, and security activity background. Therefore, the PMI focuses on the left side of the risk management bowtie (figure 3.2).

The second index, the RMI, characterizes the resilience of critical infrastructure at the center part of the bowtie, and mitigates the otherwise maximum consequences depicted on the right side of the bowtie (figure 3.2). The objectives of this index are to develop a key performance indicator that characterizes the resilience of the facility and supports the decisions of critical infrastructure owners/operators through the comparison (benchmarking) of like facilities. This index must be applicable to all types



of critical infrastructure sector/subsectors, and must consider all types of hazards (human-made, natural, and cyber), facility dependencies, and facility capabilities with respect to emergency management.

The CMI is the third index (see figure 3.2); it characterizes the maximum consequence potentially generated by an adverse event at a facility. This index includes information on public health and safety, economic, psychological, and governance and mission impacts from the loss of the facility. This index focuses on the right side of the risks management bowtie shown in figure 3.2.

## RMI METHODOLOGY

Of the three indices described above, it is the RMI that is the focus of our discussion. In this regard, it is interesting to note that the current RMI is a descendent of an earlier index called the RI. Both indices support decision-making in risk management, disaster response, and business continuity. The RI was developed in 2010 using a comprehensive methodology of consistent and uniform data collection and analysis. This index was built using the NAIC definition of critical infrastructure resilience: Resilience is the “ability to reduce the magnitude and/or duration of disruptive events” (NIAC, 2009). The effectiveness of a resilient infrastructure or enterprise depends on its “ability to anticipate, absorb, adapt to, and rapidly recover from a potentially disruptive event, whether naturally occurring or human caused” (NIAC, 2009).

The RI characterized the resilience of critical infrastructure in terms of robustness, resourcefulness, and recovery (Fisher et al., 2010; Petit et al., 2012). The main benefit of the RI was to give the critical infrastructure owners/operators a performance indicator of the resilience of their facilities that could support their decisions in risk and resilience management. In early 2012, a review of the index methodology resulted in enhancements to the structure of the RI and the information collected in order to develop a more comprehensive and informative index—the RMI.

The first step in revising the RI was a literature search to determine how to incorporate additional information and provide a better indicator of infrastructure resilience. This work was finished in 2012 and led to the publication of a report titled “Resilience: Theory and Applications” (Carlson et al., 2012). This document outlined the definition of resilience used for developing the RMI:

Resilience is “the ability of an entity—e.g., asset, organization, community, region—to anticipate, resist, absorb, respond to, adapt to, and recover from a disturbance.” (Carlson et al., 2012)

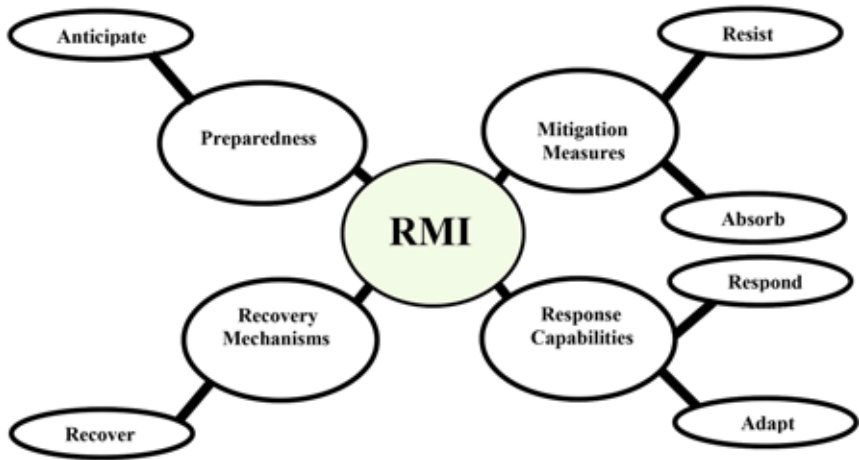


Figure 3.3 Relationship between the RMI Components and the Definition of Resilience.

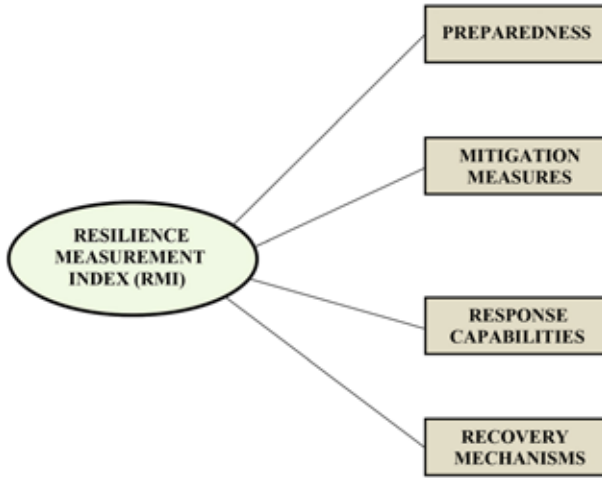
This definition of resilience is broader than the one proposed by NIAC in 2009 by considering not only the capabilities to anticipate, absorb, adapt to, and recover from a disruptive event, but also the notions of resistance and response to the event. The RMI structures the information collected in four categories (Preparedness, Mitigation Measures, Response Capabilities, and Recovery Mechanisms) that characterize the resilience capability of a facility. Figure 3.3 illustrates how the four components constituting the RMI are connected to the six actions that define resilience.

### Organization Of The RMI

Based on the definition of resilience presented in the previous section, the RMI organizes the information collected into four groups, also called RMI Level 1 components (figure 3.4; USDOE, 2013).

The United States Department of Energy's Argonne National Laboratory (2013) points out that the RMI organizes the information collected with the Infrastructure Inventory Tool (IST) into six levels in order of increasing specificity; raw data are gathered at Levels 6 and 5. They are then combined further through Levels 4, 3, 2, and finally to Level 1. Each of the Level 1 components is defined by the aggregation of Level 2 components that allow analysts to characterize a facility. The RMI is constituted from four Level 1 components, ten Level 2 components, and twenty-nine Level 3 components, as defined by SMEs. The Levels 1 and 2 components are shown in table 3.1.

The following sections present the definition and overview of each Level 1 component and associated Level 2 components that contribute to the RMI calculation.



**Figure 3.4** Level 1 Components of the RMI.

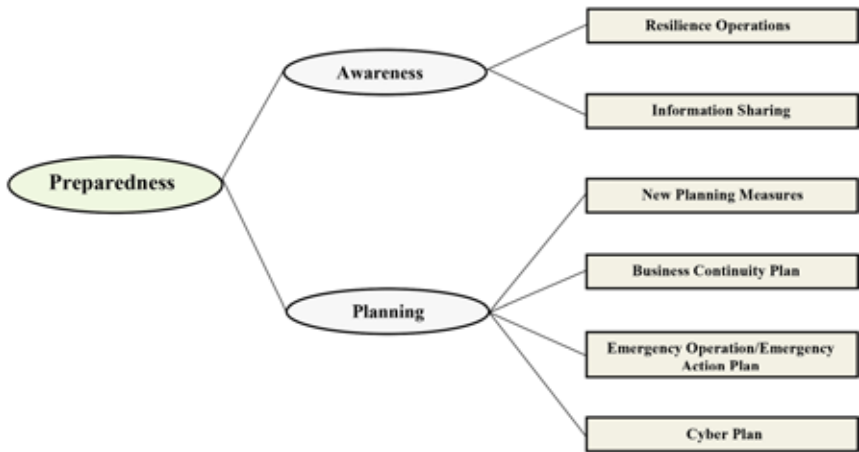
*Preparedness*

Specific activities undertaken by an entity in anticipation of the threats/hazards, and the possible consequences, to which it is subject is known in the RMI as preparedness. The RMI subdivides into two Level 2 and six Level 3 components as shown in figure 3.5 (USDOE, 2013).

It is important to note that specific actions that can be undertaken to enhance awareness related to an asset include the development of hazard-related information, including hazard assessments and information sharing, and the implementation of various measures designed to anticipate potential natural and human-made hazards. This element combines information drawn

**Table 3.1** Major Levels 1 and 2 Components Constituting the RMI

<i>Preparedness—Level 1</i>	<i>Mitigation Measures—Level 1</i>
a. Awareness—Level 2 (2 subcomponents)	a. Mitigating construction—Level 2 (4 subcomponents)
b. Planning—Level 2 (4 subcomponents)	b. Alternate site—Level 2
	c. Resources mitigation measures—Level 2 (8 subcomponents)
<i>Response Capabilities—Level 1</i>	<i>Recovery Mechanisms—Level 1</i>
a. Onsite capabilities—Level 2 (2 subcomponents)	a. Restoration agreements—Level 2 (2 subcomponents)
b. Offsite capabilities—Level 2 (3 subcomponents)	b. Recovery time—Level 2 (2 subcomponents)
c. Incident management and combined center characteristics—Level 2 (2 subcomponents)	



**Figure 3.5** Levels 2 and 3 Components of the RMI Contributing to Preparedness.

from responses to questions characterizing resilience operations and information-sharing processes in place at the facility assessed. It also addresses the type of management in place for business continuity, emergency operations, and IT.

Mitigation planning, response/emergency action planning, and actions undertaken to enhance continuity of operators are planned-related activities. This element combines information drawn from response to questions characterizing the types of plans (business continuity, emergency operations/emergency actions, and cyber) implemented at the facility. For each type of plan, this section of the RMI addresses its characteristics (e.g., level of development and approval), the type of exercises and training defined in the plan, and its content.

### *Mitigation Measures*

Mitigation Measures characterize the facility's capabilities to resist a threat/hazard or to absorb the consequences from the threat/hazard. Mitigation Measures consist of proactive activities; they consist of activities undertaken prior to an event to reduce the severity or consequences of a hazard. Mitigation is meant to capture information on whether the facility's owner or operator recognizes that the facility might be susceptible to certain hazards (e.g., hurricanes for facilities in Florida or earthquakes for facilities in California), has determined the possible consequences/impacts, and has undertaken efforts to mitigate the negative impacts those hazards might impose on the facility. In the RMI, Mitigation Measures are subdivided into three Level 2 and twelve Level 3 components (figure 3.6; USDOE, 2013).

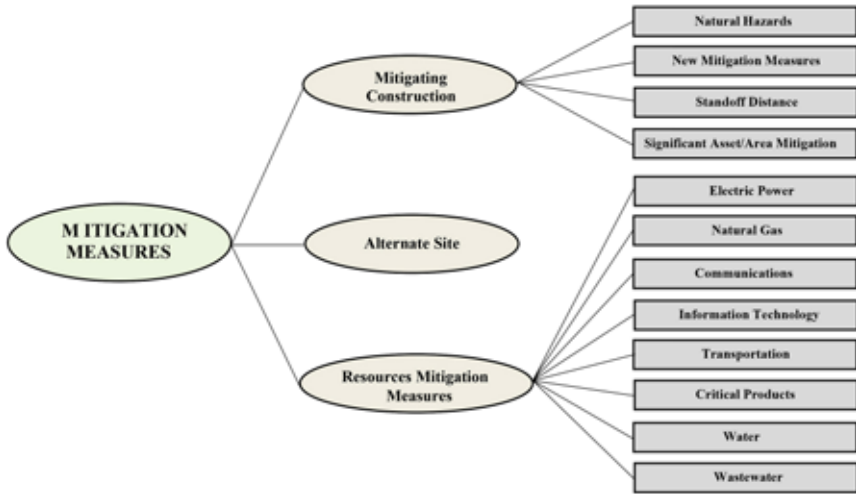


Figure 3.6 Levels 2 and 3 Components of the RMI Contributing to Mitigation Measures.

Specific mitigating construction activities include measures to offset naturally occurring adverse events. This component combines information drawn from responses to questions characterizing Natural Hazards (construction to mitigate impacts, specific plans/procedures for long-term and immediate mitigation measures, deployable mitigation measures), New Mitigation Measures (infrastructure upgrade/redundancy), Standoff Distance (e.g., limiting parking to more than 400 feet from the facility reduces impacts), and the resilience of Significant Assets/Areas (SAA) (time before impact and level of degradation) (DHS, 2015; USDOE, 2013).

Mitigation Measures also address the use of an alternative site (i.e., alternate site—Level 2—is an aggregation of questions within the IST. There is not intermediate level or subcomponent between the alternate site level and the questions used for characterizing the alternate site’s capabilities). Key features of an alternative site include its characterization and the percentage of the normal level of the main facility’s production that the alternative site can maintain. This component combines information drawn from responses to questions characterizing the type of alternative site (full capability, capability to perform essential functions, etc.), its location, equipment, and dependencies.

The Resource Mitigation Measures component, which characterizes an entity’s dependencies on key resources to support its core operations, is assessed by focusing on the facility’s reliance on selected external resources (e.g., electric power, natural gas, communications, IT, transportation, critical products, water, and wastewater), its susceptibility to disruption of these

resources, and any actions that have been undertaken to mitigate the loss of such resources. This component combines information drawn from responses to questions that characterize the resources, alternative resources and backups, and the level of impact to the loss of different resources supporting the facility’s core operations.

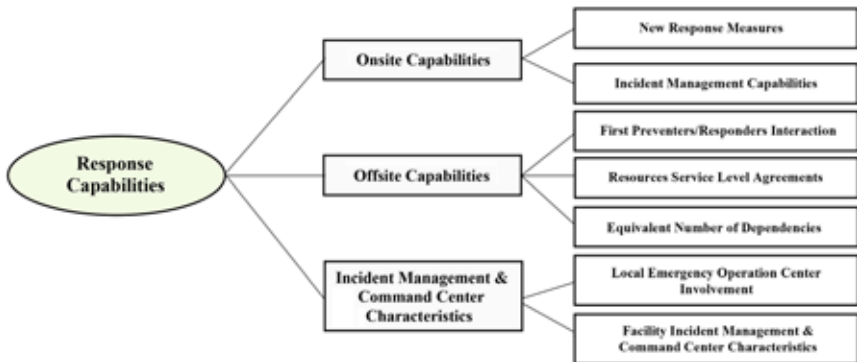
*Response Capabilities*

In the RMI, response capabilities are defined as a function of immediate and ongoing activities, tasks, programs, and systems that have been undertaken or developed to respond and adapt to the adverse effects of an event. The Response Capabilities category is subdivided into three Level 2 and seven Level 3 components (figure 3.7).

The On-site Capabilities component of the RMI captures a facility’s capabilities to respond to an accident without needing an immediate response from external first responders.

This component is made up of security/safety/emergency management aspects. It combines information drawn from response to questions characterizing the implementation within the last year of new communications and incidence response measures and the immediate on-site response capability for six specific types of event (toxic industrial chemical/Hazmat release, firefighting, explosive threat, armed response, law enforcement, and medical emergency).

The Off-site Capabilities component groups elements characterizing the interactions with the energy services sector to respond to an event (e.g., fire, medical problem, or law enforcement issue) and support the facility within its boundaries. This component combines information drawn from responses to questions characterizing the interaction with First Preventers/Responders



**Figure 3.7 Levels 2 and 3 Components of the RMI Contributing to Response Capabilities.**

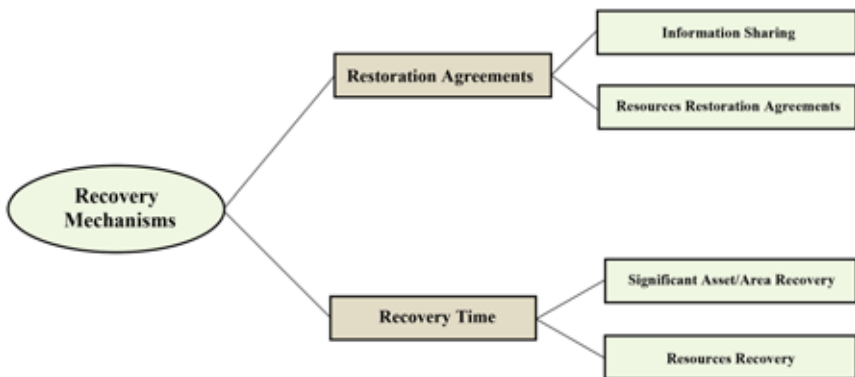
(law enforcement, emergency medical response, and fire response), and the Resource Service-Level Agreements. The First Preventers/Responders Interaction section captures the presence of interoperable communication, existing memoranda of understanding and memoranda of agreement (MOU/MOA), and orientation visits to the facility. Service-Level Agreements with resource providers and the number of dependencies reflect the facility’s lack of self-reliance and especially the implementation of contingency/business continuity plans with providers for restoration and the percentage of degradation of normal business functions once a specific resource is lost.

The Incident Management and Command Center Characteristics section groups information that captures the facility’s capabilities for managing response, continuity, and recovery operations if an incident occurs. This component combines information drawn from response to questions characterizing the facility’s involvement with the local Emergency Operation Center and the Facility Incident Management & Command Center (IMCC) characteristic (primary and alternative centers) (USDOE, 2013).

*Recovery Mechanisms*

The Recovery Mechanisms section includes activities and programs designed to be effective and efficient in returning operating conditions to a level that is acceptable to the entity. In the RMI, the Recovery Mechanisms category is subdivided into two Level 2 and four Level 3 components (see figure 3.8).

Restoration agreements concern information relative to existing MOU/MOA with entities other than emergency responders, as well as procedures/equipment that will support facility restoration. This component combines information drawn from responses characterizing the facility’s participation



**Figure 3.8** Levels 2 and 3 Components of the RMI Contributing to Recovery Mechanisms.

in information-sharing processes with external organizations and restoration resource agreements (e.g., a priority plan for restoration in case of loss of resource supply).

The Recovery Time section groups information characterizing the time necessary for the facility to recover full operations after the loss of one of its significant components.

## REFERENCES AND RECOMMENDED READING

- Carlson, L., G. Bassett, W. Buehring, M. Collins, S. Folga, B. Haffenden, F. Petit, J. Phillips, D. Verner, and R. Whitfield. 2012. *Resilience Theory and Applications*. Argonne, IL, USA: Argonne National Laboratory, Decision and Information Sciences Division, ANL/DIS-12-1.
- Department of Homeland Security (DHS). 2010a. "Quadrennial Homeland Security Review Report: A Strategic Framework for a Security Homeland." Available at [https://www.dhs.gov/xlibrary/assets/qhsr\\_report.pdf](https://www.dhs.gov/xlibrary/assets/qhsr_report.pdf).
- Department of Homeland Security (DHS). 2010b. "DHS Risk Lexicon—2010 Edition." Washington, DC. Available at <https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>.
- Department of Homeland Security (DHS). 2011. "Presidential Policy Directive/PPD-8: National Preparedness." Washington, DC. Available at <https://www.dhs.gov/presidential-policy-directive-8-national-preparedness>.
- Department of Homeland Security (DHS). 2015. *Commercial Facilities Sector—Specific Plan*. Washington, DC: U.S. Department of Homeland Security.
- FEMA. 2013. "The Voluntary Private Sector Preparedness Program—PS-Prep™ & Small Business Preparedness." Washington, DC. Available at <https://www.fema.gov/voluntary-private-sector-preparedness-program-ps-preptm-small-business-preparedness>.
- FEMA. 2015. "Protecting Critical Infrastructure Against Insider Threats." Available at <https://training.fema.gov/is/courseoverview.aspx?code=is-915>.
- Fisher, R.E., W.A. Buehring, R.G. Whitfield, G.W. Bassett, D.C. Dickinson, R.A. Haffenden, M.S. Klett, and M.A. Lawlor. 2009. *Constructing Vulnerability and Protective Measures Indices for the Enhanced Critical Infrastructure Protection Program*. Argonne, IL, USA: Argonne National Laboratory, Decision and Information Sciences Division, ANL/DIS-09-4.
- Haimes, Y.Y. 2004. *Risk Modeling, Assessment, and Management*. 2nd Edition. New York: John Wiley & Sons, p. 699.
- Henry, K. 2002. "New Face of Security." *Gov. Security*, April, pp. 30–37.
- National Infrastructure Advisory Council (NIAC). 2009. *Critical Infrastructure Resilience, Final Report and Recommendations*. Washington, DC: U.S. Department of Homeland Security. Available at <https://www.dhs.gov/publication/niac-critical-infrastructure-resilience-final-report>.
- Perl, R. 2004. *Terrorism and National Security: Issues and Trends*. CRS Issue Brief IB10119. Washington, DC.



- Petit, F., L. Eaton, R. Fisher, S. McAraw, and M. Collins. 2012. "Developing an Index to Assess the Resilience of Critical Infrastructure." *International Journal of Risk Assessment and Management (IJRAM)*, Inderscience Publishers, Geneva, Switzerland, Vol. 16, Nos. 1/2/3, pp. 28–47.
- Petit, R., R. Fisher, W. Buehring, R., Whitfield, and M. Collins. 2011. "Protective Measures and Vulnerability Indices for the Enhanced Critical Infrastructure Protection Program." *International Journal of Critical Infrastructures (IJCIS)*, Inderscience Publishers, Geneva, Switzerland, Vol. 7, No. 3, pp. 200–219.
- Rasmussen, N.J. 2015. "Current Terrorist Threat to the United States, Hearing before the Senate Select Committee on Intelligence, February 12, 2015." Available at <https://www.dni.gov/files/documents/Newsroom/Testimonies/12%20Feb%20SSCI%20Open%20Terrorist%20Threat%20Hearing%20SFR.pdf>.
- Sauter, M.A. and J.J. Carafano. 2005. *Homeland Security: A Complete Guide to Understanding, Preventing, and Surviving Terrorism*. NY: McGraw-Hill.
- Spellman, F.R. 1997. *A Guide to Compliance for Process Safety Management/ Risk Management Planning (PSM/RMP)*. Lancaster, PA: Technomic Publishing Company.
- United States Congress. 2005. "Annual Country Reports on Terrorism. 22 USC, Chapter 38, Section 2656f." Washington, DC.
- United States Department of Energy. 2013. *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience*. Washington, DC: Argonne National Laboratory.
- White House. 2013. "Presidential Policy Directive—Critical Infrastructure Security and Resilience, PPD-21." Washington, DC. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

## *Chapter 4*

# **Active Shooters**

In providing a secure environment, the key function is to connect the dots. In designing and building infrastructure to withstand terrorism, the mantra is Resilience, Resilience, Resilience.

—Frank R. Spellman

While it is not so easy to definitively define terrorism and/or the terrorist, we have less difficulty identifying the likely targets of terrorists. In America, we call these likely targets our critical infrastructure; that is, they are the essential services that underpin American society and serve as the backbone of our Nation's economy, security, and health.

—U.S. Department of Homeland Security (DHS)

Yes, DHS is correct that it is not so easy to definitively define terrorism and/or the terrorist. For example, a terrorist can be defined as an extremist, fanatic, revolutionary, radical, insurgent, guerilla, anarchist, freedom fighter, bomber, gunman, assassin, hijacker, arsonist, and/or an incendiary. However, if you are shopping in a mall, watching a movie in a theatre, attending a sporting event, or visiting any like commercial facility and you have the misfortune of encountering an active shooter or experiencing a bombing, would it matter to you what the perpetrator or incident is called? If you survive, titles probably do not matter.

—Frank R. Spellman

### **IS AN ACTIVE SHOOTER A TERRORIST?**

If we accept that anyone who terrorizes or frightens others by their horrific actions is labeled a terrorist, so be it. Does it matter if an active shooter is called a terrorist

or not? If you are outside of or in a shopping mall or some other commercial establishment and someone drives a vehicle into you and others or is firing bullets or rocket-propelled grenades or igniting a bomb at or near you, again, does it really matter what the hell the perpetrator is labeled or called? Does anything but your survival matter? Probably not. And, moreover, most of us in America do not worry about such events. Mass killings of this type or fashion occur somewhere else; they are rare. Right? Not in America! No way, Jose and Maria! Well, after the mass killings on the night of October 1, 2017, when a gunman opened fire on a crowd of concertgoers at the Route 91 Harvest Music Festival on the Las Vegas Strip in Nevada, that left 58 people dead and 546 injured, we might have second, third, or multiple thoughts about our safety at such events, or anywhere else, for that matter. Again, whether we call a cold-hearted killer a terrorist or an active shooter of innocent people, does it really matter?

### Active Shooter Incidents, 2000–2018

Active shooter incidents in the United States are more common than we might think. They have increased at a rapid rate since 2000. In 2000, seven people were killed in active shooter incidents. In 2017 and 2018, 223 people were killed. Table 4.1 shows the increased number of reported active shooter incidents in the United States since the year 2000.

**Table 4.1 160 Persons Killed and Wounded during Active Shooter Incidents in the United States (2000–2018)**

<i>Year</i>	<i>Killed</i>	<i>Wounded</i>	<i>Total</i>
2000	7	0	7
2001	12	31	43
2002	11	18	29
2003	29	22	51
2004	14	6	20
2005	24	27	51
2006	23	23	46
2007	69	57	126
2008	29	34	63
2009	65	78	143
2010	37	49	86
2011	32	54	84
2012	90	118	208
2013	44	42	86
2014	36	61	97
2015	56	78	134
2016	83	129	212
2017	138	591	729
2018	85	128	213

*Source:* FBI “Quick Look: 250 Active Shooter Incidents in the United States from 2000 to 2017” and “Active Shooter Incidents in the United States in 2018.”

## Active Shootings in The United States, 2000–2017

According to the FBI, 250 active shooter incidents took place in the United States between 2000 and 2017. During these active shootings, 799 people were killed and 1,418 people were wounded. By location, 42 percent or 105 incidents took place in a commercial area. Breaking the 105 incidents down even further, 26 percent or 65 incidents took place in businesses that were open to pedestrian traffic while 12 percent or 30 incidents took place in businesses that were closed to pedestrian traffic. The remaining 4 percent took place in malls.

While 42.0 percent of shootings took place in a commercial area from 2000 to 2017, 20.8 percent took place in schools, 14.0 percent took place in an open space, 10.0 percent took place in a government facility, 4.8 percent took place in a residence while 4.0 percent took place in a house of worship, while another 4.0 percent took place in healthcare facilities. The remaining 0.4 percent took place in other locations.

## Active Shootings in The United States, 2018

In 2018, the FBI designated twenty-seven incidents in sixteen states. There were 213 casualties—85 were killed and 123 were wounded. Ten of the twenty-seven incidents met the definition for mass killing which is defined as three or more killings in a single incident. According to the National Criminal Justice Reference Service, the number of mass shootings in the past ten years is 2.4 times greater than the decade prior (1998 to 2007). Furthermore, more than half of all mass shootings (57%) occurred within the past ten years.

Almost 60 percent (sixteen of twenty-seven incidents) occurred in areas of commerce, resulting in forty-one being killed and sixty-one wounded. Of the sixteen incidents, nine incidents occurred in business environment generally open to the public while seven incidents happened in areas closed to pedestrian traffic. Four of the sixteen shooters were active employees and two nonemployee shooters had grievances against the businesses.

### SELECT ACTIVE SHOOTER INCIDENTS IN THE COMMERCE SECTOR FROM 2000 TO 2017

- **Edgewater Technology, Inc.**—On December 26, 2000, at 11:15 a.m., Michael M. McDermott, forty-two, armed with a rifle, a shotgun, and a handgun, began shooting coworkers in the Edgewater Technology Inc. building in Wakefield, Massachusetts. Seven people were killed; no one was wounded. The shooter was apprehended when police arrived and found him sitting in a conference room.

- **Amko Trading Store**—On January 9, 2001, at 12:00 p.m., Ki Yung Park, fifty-four, fatally shot his estranged wife at a convenience store they owned in Houston, Texas. Armed with two handguns, he then drove to a nearby Amok Trading Store and continued shooting. Four people were killed no one was wounded. The shooter committed suicide when police arrived after being flagged down by a citizen.
- **Bertrand Products, Inc.**—On March 22, 2002, at 8:15 a.m., William Lockey, fifty-four, armed with a rifle and a shotgun, began shooting coworkers in the Bertrand Products, Inc. facility in South Bend, Indiana. As he attempted to flee the scene in a stolen company van, he exchanged gunfire with police, eventually committing suicide. Four people were killed; five were wounded, including three police officers.
- **Labor Ready, Inc.**—On February 25, 2003, at 6:25 a.m., Emanuel Burl Patterson, twenty-three, armed with a handgun, began shooting in the lobby of Labor Ready Inc., in Huntsville, Alabama, after arguing with others about a CD player. He then fled the scene. Four people were killed, one was wounded. The shooter surrendered after police surrounded his apartment eight hours later.
- **ConAgra Plant**—On July 2, 2004, at 5:00 p.m., Elijah J. Brown, twenty-one, armed with a handgun, began shooting employees in the ConAgra plant in Kansas City, Kansas. He had been laid off due to a production slowdown but was rehired six weeks prior to the incident. Six people were killed; two were wounded. The shooter committed suicide before police arrived.
- **Daimler Chrysler's Toledo North Assembly Plant**—On January 26, 2005, at 8.34 p.m., Myles Wesley Meyers, fifty-four, armed with a shotgun, returned from his lunch break and began shooting in DaimlerChrysler's Toledo North Assembly plant in Toledo, Ohio. He took a woman hostage before beginning to shoot at his coworkers. One person was killed; two were wounded. The shooter committed suicide before the police arrived.
- **Safeway Warehouse**—On June 25, 2006, at 3:03 p.m., Michael Julius Ford, twenty-two, armed with a handgun, began shooting in a safeway warehouse in Denver, Colorado, after having recently been passed over for a job promotion. After shooting at his coworkers, he began setting fires in the warehouse. One person was killed; five were wounded, including one police officer. The shooter was killed by police during an exchange of gunfire.
- **Trolley Square Mall**—On February 12, 2007, at 6:42 p.m., Sulejman Talovie, eighteen, armed with a shotgun and a handgun, began shooting as he entered the Trolley Square Mall in Salt Lake City, Utah. Five people were killed; four were wounded. The shooter was killed during an exchange of gunfire by responding officers, including an off-duty police officer who was in the mall at the time of the shooting.

- **Wendy's Fast Food Restaurant**—On March 3, 2008, at 12:15 p.m., Alburn Edward Blake, sixty, armed with a handgun, began shooting in a Wendy's restaurant in West Palm Beach, Florida. One person was killed; four were wounded. The shooter committed suicide before police arrived.
- **The Zone**—On January 24, 2009, at 10:37 p.m. Erik Salvador Ayala, twenty-four, armed with a handgun, began shooting at a crowd outside of the Zone, an under-21 nightclub in Portland, Oregon, and then shot himself before police arrived. He died in the hospital two days later. Two people were killed; seven were wounded.
- **ABB Plant**—On January 7, 2010, at 6:30 a.m., Timothy Hendron, fifty-one, armed with two handguns, a shotgun, and a rifle, began shooting at his coworkers in the parking lot at the ABB Plant in St. Louis, Missouri, before moving into the building. He was a party in a pending lawsuit against his employer regarding the company's retirement plan. Three people were killed; five were wounded. The shooter committed suicide before the police arrived.
- **Minaret Temple**—On April 8, 2011, at 11:27 p.m., Lanai Daniel Avery, sixteen, armed with a handgun, allegedly began shooting during a party at the Minaret Temple 174 in Chester, Pennsylvania. Two people were killed; eight were wounded. The shooter was apprehended by police.
- **McBride Lumber Company**—On January 13, 2012, at 6:10 a.m., Ronald Dean Davis, fifty, armed with a shotgun, began shooting at his coworkers in McBride Lumber Company in Star, North Carolina. Three people were killed; one was wounded. The shooter shot himself at another location and later died in the hospital.
- **Osborn Maledon Law Firm**—On January 30, 2013, at 10:45 a.m., Arthur Douglas Harmon, III, seventy, armed with a handgun, began shooting during a medication session in the Osborn Maledon law firm in Phoenix, Arizona. Two people were killed; one was wounded. The shooter later committed suicide at another location.
- **The Mall in Columbia**—On January 25, 2014, at 11:15 a.m., Darion Marcus Aguilar, nineteen, armed with a shotgun and explosive devices, began shooting in the mall in Columbia in Columbia, Maryland, first in a retail store, then in the open mall. Two store employees were killed; five mall patrons were wounded. One person was shot in the ankle and four others suffered other medical emergencies. The shooter committed suicide before law enforcement arrived.
- **Melbourne Square Mall**—On January 17, 2015, at 9:31 a.m., Jose Garcia-Rodriguez, fifty-seven, armed with three handguns, began shooting at his wife's workplace, Scotto Pizza in Melbourne Square Mall in Melbourne, Florida. One person was killed; the shooter's wife was wounded. The shooter committed suicide before law enforcement arrived.

- **Excel Industries and Newton and Hesston, Kansas**—On February 25, 2016, at 4:57 p.m., Cedric Larry Ford, thirty-eight, armed with a handgun and a rifle, began shooting from his vehicle in Newton, Kansas. He shot and wounded one person, then traveled about two miles north to Hesston and shot and wounded another person. He then traveled to his place of employment, Excel Industries, where he killed three people and wounded twelve. Three people were killed; fourteen were wounded. The shooter was killed in an exchange of gunfire with law enforcement officers.
- **Marathon Savings Bank and Tlusty, Kennedy & Dirks, S.C.**—On March 22, 2017, at 12:27 p.m., Nengmy Vang, forty-five, armed with a rifle and a handgun, began shooting inside the Marathon Savings Bank in Rothschild, Wisconsin, where his estranged wife was employed. Two bank employees were killed. The shooter then went to the law firm Tlusty, Kennedy & Dirks, S.C. in Schofield where he shot and killed his estranged wife’s lawyer. The suspect fled to his apartment complex and barricaded himself in the building for several hours before law enforcement officers engaged him in a shootout. Four people were killed (including one law enforcement officer); no one was wounded. The shooter was wounded by law enforcement during an exchange of gunfire and died a few days later.

## REFERENCES AND RECOMMENDED READING

- Carlson, L., G. Bassett, W. Buehring, M. Collins, S. Folga, B. Haffenden, F. Petit, J. Phillips, D. Verner, and R. Whitfield. 2012. *Resilience Theory and Applications*. Argonne, IL, USA: Argonne National Laboratory, Decision and Information Sciences Division, ANL/DIS-12-1.
- Department of Homeland Security (DHS). 2006. “National Strategy for Homeland Security.” <https://www.dhs.gov/national-strategy-homeland-security-october-2007>.
- Department of Homeland Security (DHS). 2010a. “Quadrennial Homeland Security Review Report: A Strategic Framework for a Security Homeland (February).” Washington, DC. <https://www.dhs.gov/quadrennial-homeland-security-review>.
- Department of Homeland Security (DHS). 2010b. “DHS Risk Lexicon—2010 Edition.” Washington, DC. <https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>.
- Department of Homeland Security (DHS). 2011. “Presidential Policy Directive/PPD-8: National Preparedness.” Washington, DC. <https://www.dhs.gov/presidential-policy-directive-8-national-preparedness>.
- Department of Homeland Security (DHS). 2015. *Commercial Facilities Sector—Specific Plan*. Washington, DC: U.S. Department of Homeland Security.
- Federal Bureau of Investigation (FBI). 2017. “Active Shooter Incidents in the United States from 2000–2017.” Washington, DC. <https://www.fbi.gov/file-repository/active-shooter-incidents-2000-2017.pdf/view>.

- Federal Bureau of Investigation (FBI). "Active Shooter Incidents in the United States from 2018." Washington, DC. <https://www.fbi.gov/file-repository/active-shooter-incidents-in-the-us-2018-041019.pdf/view>.
- Federal Bureau of Investigation (FBI). "Quick Look: 250 Active Shooter Incidents in the United States from 2000 to 2017." Washington, DC. <https://www.fbi.gov/about/partnerships/office-of-partner-engagement/active-shooter-incidents-graphics>.
- Federal Emergency Management Agency (FEMA). 2013. "The Voluntary Private Sector Preparedness Program—PS-Prep™ & Small Business Preparedness." Washington, DC. <https://www.fema.gov/voluntary-private-sector-preparedness-program-ps-preptm-small-business-preparedness>.
- Federal Emergency Management Agency (FEMA). 2015. "Protecting Critical Infrastructure Against Insider Threats." <https://training.fema.gov/is/courseoverview.aspx?code=is-915>.
- National Criminal Justice Reference Service. "Mass Casualty Shootings." [https://ovc.ncjrs.gov/ncvrw2018/info\\_flyers/fact\\_sheets/2018NCVRW\\_MassCasualty\\_508\\_QC.pdf](https://ovc.ncjrs.gov/ncvrw2018/info_flyers/fact_sheets/2018NCVRW_MassCasualty_508_QC.pdf).
- National Infrastructure Advisory Council (NIAC). 2009. *Critical Infrastructure Resilience, Final Report and Recommendations*. Washington, DC: U.S. Department of Homeland Security. <https://www.dhs.gov/publication/niac-critical-infrastructure-resilience-final-report>.
- Perl, R. 2004. "Terrorism and National Security: Issues and Trends." CRS Issue Brief IB10119. Washington, DC.
- Rasmussen, N.J. 2015. "Current Terrorist Threat to the United States, Hearing before the Senate Select Committee on Intelligence, February 12, 2015." <https://www.dni.gov/files/documents/Newsroom/Testimonies/12%20Feb%20SSCI%20Open%20Terrorist%20Threat%20Hearing%20SFR.pdf>.
- Sauter, M.A. and J.J. Carafano. 2005. *Homeland Security: A Complete Guide to Understanding, Preventing, and Surviving Terrorism*. NY: McGraw-Hill.
- United States Congress. 2005. "Annual Country Reports on Terrorism." 22 USC, Chapter 38, Section 2656f.
- United States Department of Energy. 2013. *Resilience Measurement Indeed: An Indicator of Critical Infrastructure Resilience*. Washington, DC: Argonne National Laboratory.
- White House. 2013. "Presidential Policy Directive—Critical Infrastructure Security and Resilience, PPD-21." Washington, DC. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.





## *Chapter 5*

# **Critical Infrastructure Security and Resilience**

The flow of providing security protection, from data to understanding:

**DATA→INFORMATION→KNOWLEDGE→UNDERSTANDING**

In the prevention of and preparation for terrorism, ending well is the best revenge.

—F.R. Spellman

A terrorist act is a Black Swan.

Why?

The event is a surprise (9/11 attack).

The event has a major effect (changed the world).

After the first recorded instance of the event, it is rationalized by hindsight, as if it could have been expected (recall statements by radical know-it-all pundits and snowflakes); that is, the relevant data were available but unaccounted for in risk mitigations programs (really, are you serious?) (Seriously adapted and severely modified from Taleb, 2007).

The only truly secure system is one that is powered off, cast in a block of concrete, and sealed in a lead-lined room with armed guards.

—Gene Spafford

## MR. GRASSHOPPER AND MR. RABBIT

In a recent grasshopper-rabbit conversation, a passerby wolf overheard the following:

“Mr. Rabbit,” said grasshopper, “Do you think them terrorists are trying to do away with all them human friends of ours by shutting down their shopping centers and commercial businesses?”

After a moment of deep thought, reflection and a steady but subtle thumping of one of his back feet, then his other back foot, Mr. Rabbit replied: “That, my long-skinny-legged friend is a good question . . . and I am not sure what the terrorists are up to these days . . . but one thing I know for certain; When one does not have any need for commerce in the first place . . . and they learn to live in Nature and off the Mother of it all, like us, one has nothing to worry about . . . at least, in that regard.”

Grasshopper: “Well, my fury friend that makes good sense.”

Rabbit replied: “Right on, grasshopper!”

Grasshopper nodded in approval of Mr. Rabbit’s statement. In the background, the wolf stalked silently back into the forest . . . hidden from view, for the moment. It was obvious to him that Grasshopper and Mr. Rabbit were too wise for him to mess with . . . so he didn’t . . . she just wandered off looking for easier, dumber prey.

## INTRODUCTION

From the several active shooter incidents listed and described in the previous chapter and other terrorism incidents on CS critical infrastructure in the United States, South America, the Middle East, and Africa, it is apparent that CS infrastructure is a preferred target of the terrorists. Moreover, Al Qaeda, ISIS, homegrown terrorists, and others have made it clear via documented actions or threats that it has an interest in attacking the American CS sector.

Commercial properties do not have military defenses and are generally, in many cases, open to the public; thus, they are soft targets. Beyond this obvious explanation the question might be: What makes the CS sector such an attractive terrorism target? The CS sector is an attractive target because of the following:

- The CS sector is a particularly attractive target because it is easy to infiltrate (ultimate soft target) and like other lifeline functions—which include energy, transportation, and water, and other resources essential to the operations of most critical infrastructure partners and communities financial assets—it is a target of choice.

- CS sector components or assets are spread throughout the nation with little definition of boundaries.
- Initially, several CS sector assets were designed and constructed without concern for terrorist intrusion or destructive activities.
- Many CS systems are monitored and operated using underprotected computer systems.
- As with many of industries attempting to economize, many CS segments and subsegments assign responsibility for safety and security as a collateral duty to a line employee instead of employing a fulltime certified cyber, IT, and safety and security professional.

## CS SECTOR SECURITY GOALS AND ATTRIBUTES

The DHS has identified eight general elements and characteristics of critical infrastructure (including CS sector) security goals and attributes.

- **Critical Asset Reduction Goal.** Sector resiliency will be most assured if no particular asset can be assessed as more critical than any other. While the ultimate ideal goal would be zero-critical CS assets, the sector will strive to reduce the number of critical assets whenever and wherever possible within fiscal and legal constraints. Sound risk management practices, including asset resiliency, mitigation of risks, and redundancy will be shared and advanced throughout the sector.
- **Cyber Goals and Attributes.** Like physical attributes, these assist the CS sector to evaluate consequences and vulnerabilities, and develop protective strategies. Cyber systems that link and help monitor and control the financial services systems are increasingly recognized as a potential vulnerability. All information that identifies or otherwise describes characteristics of a critical CS asset that is created, held, and maintained by the government or the private sector will be protected from unauthorized disclosure according to established procedures, appropriate to the particular level of information.
- **Volumetric or Throughput Attributes.** These define the extent of any damage, depending on the utilized capacity of the systems, or point where the system may be capacity constrained.
- **Personnel Security Goals and Human Attributes.** Ensure all personnel directly associated with a critical CS asset are vetted for employment suitability, reliability, and trustworthiness using established processes commensurate with requirements of the respective positions held in conformance with pertinent security policy. Highly trained and skilled personnel are key factors in a comprehensive CS sector security plan. The availability of skilled and experienced technical talent is a concern in the CS sector.

Sustaining essential technical knowledge is critical to maintaining the sector's safety, reliability, and security.

- **Physical Security Goal.** Determine the impact or consequence of critical CS asset loss its mission(s) supported, the known or perceived threat, and the susceptibility to exploitation of vulnerabilities the threat is capable of perpetuating; identify specific CS assets the destruction or disruption of which could result in human casualties or economic disruption similar to the effects of weapons of mass destruction; compile a composite of facility physical security risk assessments.
- **Insider Threat Goal and Attributes.** Responsible parties in charge provide security education and training aids to CS asset owners/operators not having security program so that they may implement provisions for the vetting of system and network administrators commensurate with the consequences of the loss of sensitive or classified information, production or provisioning capability, and supply chain integrity.
- **Monitoring and Reporting Goals and Attributes.** Ongoing determination of the effectiveness of government threat reporting to officials, owners, and operators responsible for critical CS assets, and to local law enforcement officials and other first responders including, as appropriate, the medical and mass transportation communities.
- **Training and Education Goal and Attributes.** Develop and provide continuous specific security education and training materials for critical CS asset owner/operators.

## HOMELAND SECURITY DIRECTIVES

As a result of 9/11, the Homeland Security Department was formed. On matters pertaining to Homeland Security, HSPDs issued by the president. Each directive has specific meaning and purpose and is carried out by the U.S. DHS. Table 5.1 lists Homeland Security Presidential Directives (HSPDs).

**Note:** HSPD-7 was revoked by the Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience on February 12, 2013. PPD-21 states that “plans developed pursuant to HSPD-7 shall remain in effect until specifically revoked or superseded” (DHS, 2013). Multiple changes came out of PPD-21, including six actions with specific deadlines. One of those actions was to update the NIPP within 240 days.

**Note:** The significance of Presidential Policy Directive 21 (PPD-21) is that it deals specifically with critical infrastructure security and resilience; it defines security as reducing the risk to critical infrastructure by physical

**Table 5.1 Homeland Security Presidential Directives**


---

HSPD—1:	Organization and operation of the Homeland Security Council (White House). Ensures coordination of all homeland security-related activities among executive departments and agencies and promote the effective development and implementation of all homeland security policies.
HSPD—2:	Combating terrorism through immigration policies (White House). Provides for the creation of task force which will work aggressively to prevent aliens who engage in or support terrorist activity from entering the United States and to detain, prosecute, or deport any such aliens who are within the United States.
HSPD—3:	Homeland Security Advisory System (White House). Establishes a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to federal, state, and local authorities and to the American people.
HSPD—4:	National strategy to combat weapons of mass destruction. Applies new technologies, increased emphasis on intelligence collection and analysis, strengthens alliance relationships, and establishes new partnerships with former adversaries to counter this threat in all of its dimensions.
HSPD—5:	Management of domestic incidents (White House). Enhances the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system.
HSPD—6:	Integration and use of screening information (White House). Provides for the establishment of the Terrorist Threat Integration Center.
HSPD—7:	Critical infrastructure identification, prioritization, and protection (White House). Establishes a national policy for federal departments and agencies to identify and prioritize critical infrastructure and key resources of the United States and to protect them from terrorist attacks.
HSPD—8:	National preparedness (White House). Identifies steps for improved coordination in response to incidents. This directive describes the way federal departments and agencies will prepare for such a response, including prevention activities during the early stages of a terrorism incident. This directive is a companion to HSPD-5.
HSPD—8 Annex 1:	National planning. Further enhances the preparedness of the United States by formally establishing a standard and comprehensive approach to national planning.
HSPD—9:	Defense of United States Agriculture and Food (White House). Establishes a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies.
HSPD—10:	Biodefense for the Twenty-first century (White House). Provides a comprehensive framework for our nation's Biodefense.
HSPD—11:	Comprehensive terrorist-related screening procedures (White House). Implements a coordinated and comprehensive approach to terrorist-related screening that supports homeland security, at home and abroad. This directive builds upon HSPD-6.
HSPD—12:	Policy for a common identification standard for federal employees and contractors (White House). Establishes a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors (including contractor employees).
HSPD—13:	Maritime security policy. Establishes policy guidelines to enhance national and homeland security by protecting U.S. maritime interests.

---

*(Continued)*

**Table 5.1 Homeland Security Presidential Directives—Continued**


---

HSPD—14:	Domestic Nuclear Detection established a Domestic Nuclear Detection Office (DNSO) to coordinate efforts to protect the domestic United States against dangers from nuclear or radiological materials. EPA supports the detection, response, law enforcement, and information sharing aspects of the DNDO's mission.
HSPD—16:	Aviation strategy. Details a strategic vision or aviation security while recognizing ongoing efforts, and directs the production of a National Strategy for Aviation Security and supporting plans.
HSPD—18:	Medical countermeasures against weapons of mass destruction (White House). Establishes policy guidelines to draw upon the considerable potential of the scientific community in the public and private sectors to address medical countermeasure requirements relating to CBRN threats.
HSPD—19:	Combating terrorist use of explosives in the United States (White House). Establishes a national policy and calls for the development of a national strategy and implementation plan, on the prevention and detection of, protection against, and response to terrorist use of explosives in the United States.
HSPD—20:	National Continuity Policy (White House). Establishes a comprehensive national policy on the continuity of federal government structures and operations and a single National Continuity Coordinator responsible for coordinating the development and implementation of federal continuity policies.
HSPD—21:	Public Health and Medical Preparedness (White House). Establishes a national strategy that will enable a level of public health and medical preparedness sufficient to address a range of possible disasters.
HSPD—23:	Cyber security requires federal agencies to monitor cyber activity toward federal agencies' computer systems and where necessary, provide action to eliminate sources of hostile action. EPA has a robust security program for both personnel and cyber security as mandate by the directive.

---

*Source:* USEPA (2016).

means or defense cyber measures to intrusions, attacks, or the effects of natural or man-made disasters. Examples of security measures (DHS, 2016):

- Badge entry at doors
- Using antivirus software
- Fencing around buildings
- Locking computer screens

PRD-21 defines resilience as the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. Examples of resilience measures:

- Developing a business continuity plan
- Having a generator for backup power
- Using building materials that are made more durable

## ASSESSING CHALLENGES

The DHS determined that there were many challenges facing the CS sector; in particular it has listed and detailed seven challenges, each of which is covered in this section.

### **Challenge 1: Advancing the State of the Art in Designing and Testing Secure Applications**

Software flaws and inadequate patching and configuration practice are two of the sources of IT vulnerabilities; therefore, they require two different threads of thinking about research. Current research has shown that across the entire financial services industry, the information protection and risk management community is generally not well equipped to accurately or completely define, specify, estimate, calculate, and measure how to design and test secure application software. Experience has shown that continued mitigation against network vulnerabilities is ongoing and remains important; however, an increasing number of attacks are against software applications, which are not the focus of many financial institutions. The fact is business requirements and risk assessments should drive resource allocations. Risks are driven by complex applications developed in-house and by partners, extension of powerful business applications to vulnerable customers, and increasingly organized criminal attacks (e.g., SQL injections to steal copies of data bases, cross-site scripting). To be effective, application security strategies must incorporate development standards and training, automated and manual code reviews, and penetration testing with and without design specifications or source code of the applications being tested. Some financial regulators have issued supervisory guidance on risks associated with web-based applications, urging banks to focus adequate attention on these risks and appropriate risk management practices (US Treasury, 2008).

The testing of financial institution applications for security vulnerabilities stemming from software flaws is often inadequate, incomplete, or nonexistent. Important to CS sector institutions is the gaining of confidence; that is, commercial institutions need to gain the confidence that is need to deploy business-critical software with some proof of evaluation for obvious application security flaws (e.g., un-validated user input, buffer-overflow conditions). Without this confidence, financial institutions are forced to develop countermeasures and compensating controls to counter these unknown potential threats and undocumented features of the software. Without explicit security assurance testing and correspond evidence of testing results, functional testing by development teams and outside software developers is insufficient. Commercial institutions need a robust, effective, affordable, and timely security testing methodology and practice to gain the confidence required



to deploy application software into sometimes hostile environments for purposes of practical and appropriate risk management.

Commercial institutions, to minimize vulnerability, have urged major software providers to improve the quality of their software development and testing processes for utility software, such as operating systems, but are only beginning to urge application software developers to do the same. Major software companies and outsourcing providers are responding by developing more secure code. However, while there are important and worthwhile efforts, the CS industry (and other users of software) remains at risk from fundamental software development practices that produce vulnerable software in the very beginning stages of development. This vulnerable software has, in turn, resulted in substantial increase in application-level attacks. Risk managers in commercial institutions continue to look for solutions.

The bottom line: The CS sector needs research on how to specify, design, and implement secure software and measure its associated life-cycle costs and the benefits of the various information security technologies and processes. The sector would benefit from better understanding of how to develop, test, and measure secure application software.

## **Challenge 2: More Secure and Resilient Financial Transaction Systems**

The CS sector relies on an IT infrastructure, including computing hardware, software, and telecommunications networks. Some of this infrastructure is owned and operated by financial institutions and some is provided by third-party service providers in the United States and around the globe. This infrastructure is probed and attacked by a variety of adversaries, including criminal elements and nation-states. These adversaries exploit vulnerabilities in people, processes, and technologies and perpetuate attacks for financial gain to steal proprietary information, or to undermine consumer confidence in the financial services industry and U.S. economy. Threats from adversaries are increasing, raising concerns over the integrity of devices, networks, and applications. The infrastructure is also vulnerable to natural disasters, pandemics, and other outages. The financial services, IT, and telecommunications industries have responded to these challenges with initiatives to address security, integrity, and resilience; however, significant risks remain in terms of security breaches, fraud (including identity theft), service disruptions, and data integrity.

More secure and resilient financial transaction systems are the key to maintaining the integrity of the CS industry. Because the trustworthiness of networks and devices is uncertain they must resist interception and tampering over an increasingly vulnerable environment. One facet is ensuring that networks and devices are “clean” when restoring services after an interruption. Reconstitution of data after an attack requires an additional step:

decontamination, which is the process of distinguishing a clean system state (unaffected by the intruder) from the portions of infected system state, and eliminating the causes of those differences. Because system users would prefer as little good data as possible be discarded, this problem is quite difficult. Also of primary importance is the retention and reconstruction of transaction history while simultaneously being fully engaged in business continuity operations and executing a recovery plan. Other sectors have expressed concerns about extending their continuity plans to include vital information found on remote workstations. The possibility of this dislocation of normal corporate boundaries could be strained when relying on a distributed computing model.

As a tool for business continuity planning purposes, remote access is necessary for enhancing productivity. For example, commercial institutions have developed business continuity plans to ensure employees can access networks if core facilities are not available.

The bottom line: The challenge is in finding the right mix of hardware and software that gives employees the ability to conduct their work off-site while still adhering to excessive incremental risk. It should also provide employees the ability to seamlessly move from one location to another while retaining their “session state” and desktop customization (US Treasury, 2008; DHS, 2010).

### **Challenge 3: Enrollment and Identity Credential Management**

A secure CS sector infrastructure requires reliable and unambiguous identification of all parties involved in a transaction and non-repudiation of authorized transactions. Current technologies offer “spot” solutions that secure an aspect of identity management; however, much vulnerability remains. Although strong authentication credentialing technology exists, the initial identification of and linkage to an individual’s identity to an authentication credential and the need to replace lost or stolen credentials remain weak links. Commercial institutions rely on the individual’s possession of knowledge that can be stolen, or by biometrics that can be spoofed, and may not scale up to millions of individuals without sacrificing performance. Moreover, the lack of mutual authentication allows for, among other things, the ability for the launching of successful man-in-the-middle attacks (i.e., active eavesdropping attacks). Commercial institutions typically rely on “spot” authentication in which the financial institution authenticates customers before a transaction. Research is needed to develop more continuous authentication and credentialing.

### **Challenge 4: Understanding the Human Insider Threat**

CS institutions grant access to confidential information to authorized parties. To establish and maintain trust in this access granting process, commercial institutions use a variety of tools and controls to identify, verify, authenticate,

and authorize trustworthy individuals and contractors. Measures include background checks, credit history checks, and other historical data checks. The insider threat problem (discussed in detail later) is particularly difficult because of the interplay between technical, legal, managerial, and ethical issues. Commercial institutions recognize that current measures provide only a “coarse-grained” screening for obvious human threats to begin the access granting process; individuals are granted access to networks, systems, databases, applications, and ultimately customer and business information based on their job or role in the institution. The process is enforced via a highly complex set of overlapping operational and technical controls, which requires that a large percentage of each financial institution’s total information protection budget is dedicated to access management, control, and reporting.

CS institutions continue to experience damage from the unprofessional, malicious, or criminal activities committed by individuals with authorized access, sometimes in coordination with external individuals, criminal organizations, or terrorists; this trend continues even through preemployment/engagement checking processes, and the layering of costly operational and technical controls is actively employed. Current approaches suggest adding additional layers—technological or procedural—of surveillance processes to detect, identify, and help stop the unwanted activities of authorized individuals. However, such approaches, while they may reduce undesirable activities, add substantial operating costs to an already costly access management approach.

Commercial institutions currently have tools that could be useful in determining improper behavior of insiders. Many of these tools are based on physical and logical access but are typically not integrated. Improvements in security information management are needed to detect and prevent improper insider behavior. A critical component of improving security information management is ensuring that appropriate controls are in place to address privacy and other human resource protections.

### **Challenge 5: Data Centric Protection Strategies**

With regard to the CS industry protective measures put in place to build a more secure and resilient infrastructure to protect financial transactions, vulnerability still exists because sensitive information can be stolen by criminal elements and other adversaries who attack less secure systems connected to merchants and third-party vendors. Preserving the integrity of each transaction involves identification, authentication, and authorization of each transaction to ensure that counterparties are not criminals or money launderers, and that sensitive information is protected and the loss, copying, or tampering is detected. While commercial institutions have tools that protect data while it

resides in a certain environment, these tools are not effective when the data is taken out of that controlled environment (e.g., when a user cuts and pastes in another form). A key challenge is focusing on metadata to understand when data is accessed, updated, or copied.

### **Challenge 6: Better Measures of the Value of Security Investments**

The CS sector seeks research on the life-cycle costs of security technologies that support critical infrastructure protection, and the creation of cost-benefit models that can be adopted within institutions and across the industry. One of the key issues in the adoption of improved protective technologies and processes is the ability of the purchasing organizations to fully understand the costs and benefits of security technologies. Inflation protection organizations, as part of their regular business, can effectively evaluate specific cost elements for various protective programs in terms of operating cost, contracting costs, and the cost of purchasing the needed technology for an organization. However, information protection organizations typically do not have good estimates of the total life-cycle costs of the protective programs on the businesses lines that are asked to implement, own, and manage these protective programs over the long-term. Across the entire Commerce sector, the information protection and risk management community is generally not well equipped to accurately or completely define, estimate, calculate, measure, or communicate the benefits that result from protective programs. Further exacerbating this issue is that the “benefits” of security are often intangible and often related more to loss avoidance, making traditional return-on-investment (ROI) calculations difficult. There needs to be a stronger correlation between security investment and the reduction of risk and subsequent loss. Some methods used today to justify security investments may not align or be equivalent with methodologies under Generally Accepted Accounting Principles (GAAP). Research is needed to establish a baseline risk and to understand changes from the baseline that result from investment. This research also could benefit the broader risk management community.

### **Challenge 7: Development of Practical Standards**

Practical standards and suggested practices is one of the prevailing techniques for closing the gap between state of the art and state of the practice. In an attempt to further the protection of the CS critical infrastructures, numerous documents outlining suggested practices have been developed, most addressing a closely circumscribed segment of CS systems and practices. Unfortunately, the problem is that, to date, the industry has been unable to

quantitatively correlate best practices with reduced risk. If such a relationship could be determined and quantified, financial institutions would have the tools needed to justify risk management and risk reduction measures. This analysis could, in turn, assist the industry in agreeing on a common and consistent set of practices. A related question is how practitioners and regulators should adopt or consider these in developing robust and resilient infrastructures vis-à-vis the confusion caused by so many different best practices guides and standards.

## ASSESSING CONSEQUENCES

The potential physical and cyber consequences of any incident, including terror attacks and natural or human-made disasters, are the primary consideration in risk assessment. In the context of this text, consequence is measured as the range of loss or damage that can be expected. The consequences that are considered for the national-level comparative risk assessment are based on the criteria as set forth in HSPD-7. These criteria can be divided into four main categories:

- **Human Impact:** Effect on human life and physical well-being (e.g., fatalities, injuries).
- **Economic Impact:** Direct and indirect effects on the economy (e.g., costs resulting from disruption of products or services, costs to respond to and recover from the disruption, costs to rebuild the asset, and long-term costs due to environmental damage).
- **Impact on Public Confidence:** Effect on public morale and confidence in national economic and political institutions.
- **Impact on Government Capability:** Effect on the government's ability to maintain order, deliver minimum essential public services, ensure public health and safety, and carry out national security-related missions.

Moreover, HSPD-7 is important to the CS sector in that it required the Department of Homeland Security to “. . . serve as the focal point for the security of cyberspace . . .” with a mission that included “. . . analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems.” This directive established a national policy for federal departments and agencies to identify and prioritize U.S. CIKR and to protect them from terrorist attacks. In addition, it required heads of all federal agencies to “. . . develop . . . plans for protecting the physical and cyber critical infrastructure and key resources

that they own or operate.” Hence, the federal government began to directly address issues of cyber security within the federal government systems (FCC, 2017).

### **DID YOU KNOW?**

The DHS has the mission to provide a common baseline of security across the federal civilian executive branch and to help agencies manage their cyber risk. The common baseline is provided in part through the EINSTEIN system. EINSTEIN services two key roles in federal government cybersecurity. First, EINSTEIN detects and blocks cyberattacks from compromising federal agencies. Secondly, EINSTEIN provides DHS with the situational awareness to use threat information detected in one agency to protect the rest of the government and to help the private sector protect itself (DHS, 2017b).

As a result of HSPD-7, the DHS established the National Cybersecurity Division (NCSD). The objectives of this division are “. . . to build and maintain an effective national cyberspace response system, and to implement a cyber-risk management program for protection of critical infrastructure.” The primary operational arms of the division are first the Cybersecurity Preparedness and National Cyber Alert System, and secondly the U.S. Computer Emergency Response Team (U.S.-CERT). The National Cyber Alert System was created by U.S.-CERT and the DHS to help protect computers. One of U.S.-CERT’s overarching goals is to ensure that individuals and agencies have access to timely information through tips and alerts about security topics and events. The U.S.-CERT has become the national first line of defense for the war of cyber security. The CERT’s Cyber Risk Management Program assesses risk, prioritizes resources, and executes protective measures in order to secure the cyber infrastructure. It includes such things as current risk assessments and vulnerabilities that are maintained in their vulnerability database, the National Cyber Alert System, for information dissemination, and a number of other references for cyber security measures.

In addition to the importance of HSPD-7 providing guidance and direction in cyber security and CS sector protection objectives, as a further shot in the security arm, so to speak, HSPD-23 was signed in January 2008 by President Bush; this directive was necessary due to increased cyber activity on an international scale and attacks targeted at U.S. computers and networks—including computer-controlled systems. HSPD-7 established a Comprehensive National Cybersecurity initiative (CNCI). Although the document

is classified, public sources have indicated that in addition to establishing the National Cyber Security Center within the DHS, the initiative had twelve other objectives (FCC, 2017):

- Move toward managing a single federal enterprise network;
- Deploy intrinsic detection systems;
- Develop and deploy intrusion prevention tools;
- Review and potentially redirect research and funding;
- Connect current government cyber operations centers;
- Develop a government-wide cyber intelligence plan;
- Increase the security of classified networks;
- Expand cyber education;
- Define enduring leap-ahead technologies;
- Define enduring deterrent technologies and programs;
- Develop multipronged approaches to supply chain risk management;
- Define the role of cyber security in private sector domains.

### DID YOU KNOW?

The federal enterprise network depends on IT systems and computer networks for essential operations. These systems face large and diverse cyber threats that range from unsophisticated hackers to technically competent intruders using state-of-the-art intrusion techniques. Many malicious attacks are designed to steal information and disrupt, deny access to, degrade, or destroy critical information systems (DHS, 2017a).

## REFERENCES AND RECOMMENDED READING

- Crayton, J.W. 1983. "Terrorism and the Psychology of the Self." In Lawrence Zelic Freedman and Yonah Alexander, eds., *Perspectives on Terrorism*. Wilmington, Delaware: Scholarly Resources, 33–41.
- Department of Homeland Security (DHS). 2003. "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets." [https://www.dhs.gov/xlibrary/assets/Physical\\_Strategy.pdf](https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf).
- Department of Homeland Security (DHS). 2013. "Homeland Security Directive 7: Critical Infrastructure Identification, Prioritization, and Protection." <https://www.dhs.gov/homeland-security-presidential-directive-7>.
- Department of Homeland Security (DHS). 2015. *Commercial Facilities Sector—Specific Plan*. Washington, DC: U.S. Department of Homeland Security.
- Department of Homeland Security (DHS). 2017a. "Securing Federal Networks." <https://www.dhs.gov/cisa/securing-federal-networks>.

- Department of Homeland Security (DHS). 2017b. "EINSTEIN." <https://www.dhs.gov/cisa/einstein>.
- Federal Emergency Management Agency (FEMA). 2015. "Protecting Critical Infrastructure Against Insider Threats." <https://training.fema.gov/is/courseoverview.aspx?code=is-915>.
- Federal Registrar* (FR). 2007. 17688–17745.
- Ferracuti, F. 1982. "A Sociopsychiatric Interpretation of Terrorism." *The Annals of the American Academy of Political and Social Science*, 463, September, 129–141.
- Hudson, R.A. 1999. *The Sociology and Psychology of Terrorism: Who Becomes a Terrorist and Why?* Washington, DC: Library of Congress. <https://fas.org/irp/threat/frd.html>.
- Lees, Frank. 1996. *Loss Prevention in the Process Industries*. 3rd Edition. New York: Butterworth-Heinemann, A5.1–A5.11.
- Long, D.E. 1990. *The Anatomy of Terrorism*. New York: Free Press.
- Margolin, J. 1977. "Psychological Perspectives on Terrorism." In Y. Alexander and S.M. Finger, eds., *Terrorism: Interdisciplinary Perspectives*. New York, NY: John Jay Press, 169–175.
- Olson, M. 1971. *The Logic of Collective Action*. Boston: Harvard University Press.
- Office of Management and Budget (OMB). 1998. *Federal Conformity Assessment Activities, Circular A-119*. Washington, DC: White House.
- Pearlstein, R. 1991. *The Mind of the Political Terrorist*. Wilmington, Delaware: Scholarly Resources, Inc.
- Sullivan, J. 2007. *Strategies for Protecting National Critical Infrastructure Assets: A Focus on Problem-Solving*. New York: Wiley & Sons.
- United States Environmental Protection Agency (USEPA). "Homeland Security Presidential Directives." <https://www.dhs.gov/presidential-directives>.
- Wilkinson, P. 1974. *Political Terrorism*. London: Macmillan.





## *Chapter 6*

# **Vulnerability Assessment (VA)**

In God we trust, all others we monitor.

—Intercept Operator’s motto

### **INTRODUCTION**

One consequence of the events of 9/11 was DHS’s directive to establish a Critical Infrastructure Protection Task Force to ensure that activities to protect and secure vital infrastructure are comprehensive and carried out expeditiously. Another consequence is a heightened concern among citizens in the United States over the security of their energy infrastructure (i.e., the uninterrupted supply of electrical power and fuel to power vehicles, homes, and vital communications systems). As mentioned, along with other critical infrastructure, the CS sector is classified as “vulnerable” in the sense that inherent weaknesses in its operating environment could be exploited to cause harm to the system. There is also the possibility of a cascading effect—a chain of events—due to a terrorist act affecting CS sector providers, which could cause corresponding damage (collateral damage) to other nearby users. In addition to significant damage to the nation’s CS sector, entities using and needing CS to function can result in loss of life due to a lack of proper emergency response; shutdown of other industries; loss of electronic communication operational control networks could cause catastrophic environmental damage to rivers, lakes, and wetlands; and other long-term public health impacts.

Public and private members of the CS sector conduct risk assessments. These assessments look at issues and potential vulnerabilities both within

individual organizations and sector wide. Since risk management is part of the commercial operations culture, both regulators and private organization have a long history of conducting regular risk assessments. In the private sector some of these risk assessments are mandated through regulation and validated by the examination process. Furthermore, the private sector institutions conduct voluntary risk assessments to meet their business needs as part of their continuity planning and/or in conjunction with trade associations' recommendations and self-regulatory requirements (DHS, 2007).

## ASSESSING VULNERABILITIES

The CS sector conducts ongoing VAs. What is a VA? For the purpose of this text and according to FEMA 2008, vulnerability is defined as any weakness that can be exploited by an aggressor to make an asset susceptible to hazard damage. In addition, according to the DHS (DHS, 2009), vulnerabilities are physical features or operational attributes that render an entity open to exploitation or susceptible to a given hazard. Vulnerabilities may be associated with physical (e.g., a broken fence), cyber (e.g., lack of a firewall), or a human (e.g., insider threats; untrained guards) factors.

VAs estimate the odds that a characteristic, of, or flaw in, an infrastructure could make it susceptible to destruction, disruption, or exploitation based on its design, location, security posture, processes, or operations. Vulnerabilities typically are identified through internal assessments and information sharing with customers, vendors, and suppliers.

A VA methodology was developed as part of the complete CS sector-specific plan risk assessment methodology. The methodology examined physical, cyber, and human vulnerabilities and considered relevant national preparedness threat scenarios. The process varied depending on the architecture elements being studied and included subject matter expert interviews, site visits, and modeling and analysis.

The vulnerabilities of CS architecture elements may vary depending on whether they are operational or implementation specific. Operational vulnerabilities may include those that result from the inherent principles of network design, unanticipated network congestion caused by external factors, or collateral consequences from major disasters or events. Implementation-specific vulnerabilities may be very particular in nature—from bugs in application software and protocol deficiencies to backdoors in vendor equipment firmware or software. The magnitude of the implementation vulnerabilities also varies depending on the exposure of the vulnerable equipment. While embedded firmware, for example, may have only limited exposures to configuration

and maintenance functions, systems such as the Domain Name Service require a high degree of exposure in order to provide service to customers (DHS, 2010).

Conducting VAs is conducted on many levels. These VAs include examinations into the potential risks resulting from cross-sector dependency, sector-specific vulnerabilities, and dependencies on key assets, systems, technologies, and processes. Moreover, DHS has instituted a process to provide Awareness Training to financial services asset owner/operators. The purpose of the Awareness Training is to provide CS sector personnel with information about the place of their asset within the overall CS mission requirements and acquisition process so they will understand their rules and importance to the entities at the corporate and site levels (DHS, 2010). The training focuses on:

- protection of CS interests
- protection of federal interests
- importance of facilities fostering relationships with local responders and federal, state, and local law enforcement/civil authorities for business recovery planning.

The Awareness Training also informs the asset owner/operators of the protection measures applied to their proprietary and business-sensitive information provided by and to the CS sector. Once critical CS assets are identified and prioritized, the next step is to conduct standardized assessments. DHS, working through and with various agencies, has established a standardized mission assurance assessment for application to critical CS assets. These assessments consider impact, vulnerability, and threat/hazard (whether from natural disaster, technological failure, human error, criminal activity, or terrorist attack). This approach to risk assessment ensures consideration of relevant factors for each CS asset and a relative prioritization of risks to support military operations.

## **INSIDER THREAT VULNERABILITY**

The insider threat to a CS organization and hostile and criminal cyber activities is not about rocket science; instead it is about malicious software (malware) and the variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and others. One does need not be a super genius to understand what insider threat really is. The truth is the insider threat is . . . a human, a person, a mammal, *Homo sapiens*, a breathing organism, a heartbeat. The

point is to protect an organization from insider threats, the organization must “use tools to monitor the traffic in or out of the networks and be able to focus that monitoring on specific people who do something concerning or suspicious; moreover, nontechnical employee behavior must be monitored” (INSA, 2017).

“Behavior must be monitored,” yes, for sure. What monitoring really comes down to, however, is awareness. An important part of any successful VA process is awareness. Security and risk managers (and all employees in general) working in or with the critical infrastructure sectors must be aware of the potential for insider threat vulnerability. Again, the key word is AWARENESS. Awareness means that personnel within the critical infrastructure sectors must know how to identify and take action against insider threats. To achieve this critical goal, safety and security personnel must be provided with an overview of and be cognizant of common characteristics and indicators associated with malicious insiders and effective measures to counter insider threats.

### **Protecting Against Insider Threats (FEMA, 2015)**

As mentioned earlier, when analyzing threats to our nation’s critical infrastructure, we tend to focus on malicious actions from boat or plane loads of outside actors. Of equal concern (and even more so in the author’s view) are threats from an insider—someone we have given legitimate access to information, systems, and resources. The measures we take to detect and protect against external threats may not be sufficient to address threats from insiders.

A malicious insider has access and inside knowledge of the organization and uses that knowledge with the intent to cause harm. The insider may be a current employee, a former employee, a service provider, or, especially in the current era, a planted person inside who has been brainwashed and turned into a terrorist waiting for the moment of maximum impact to people and property.

Given the importance of our nation’s critical infrastructure, the actions taken by a malicious employee or service provider could have devastating consequences.

Let’s look at some actual examples.

- A service provider employee at a nuclear facility stole two 5-gallon containers of low-enriched uranium dioxide and then attempted to extort \$100,000 by threatening to disperse the material in an unnamed U.S. city.
- A power company field engineer, angry with his supervisor, disabled protection systems at a substation and forced the shutdown of the entire network. More than 800,000 customers lost power as a result.

- Two municipal employees used their access credentials to sabotage the system controlling the traffic lights of a major city, causing widespread traffic delays. The damage took four days to repair.
- A disgruntled supermarket meat packaging employee intentionally contaminated hamburger meat with a pesticide, causing various levels of illness in ninety-two consumers.

Insider threats endanger the integrity and security of our workplaces and our communities. This section helps you become aware of threat indicators and actions you can take. As stated earlier, and it can't be overstated, awareness is the first step to keeping our nation and workplaces safe.

### *Insider Threat Defined*

The president's National Infrastructure Advisory Council (2008) defines the insider threat as follows:

The insider threat to critical infrastructure is one or more individuals with the access or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of the entity's security, systems, services, products, or facilities with the intent to cause harm.

A person who takes advantage of access or inside knowledge in such a manner commonly is referred to as a "malicious insider."

### *The Scope of Insider Threats*

Insider threats can be accomplished through either physical or cyber means and may involve any of the following:

- **Physical or IT sabotage**—Involves modification or damage to an organization's facilities, property, assets, inventory, or systems with the purpose of harming or threatening harm to an individual, the organization, or the organization's operations.
- **Theft of intellectual property**—Involves removal or transfer of an organization's intellectual property outside the organization through physical or electronic means (also known as economic espionage).
- **Theft of economic fraud**—Involves acquisition of an organization's financial or other assets through theft or fraud.
- **National security espionage**—Involves obtaining information or assets with a potential impact on national security through clandestine activities.

## DID YOU KNOW?

The FBI testified in June 2012 that in the preceding year, economic espionage losses to the American economy totaled more than \$13 billion. In the previous four years, the number of arrests the FBI made had doubled; indictments increased by a factor of five; and convictions increased by a factor of eight (FBI, 2012). In another survey, security professionals found that 43.2 percent of respondents attributed some loss at their organization to insiders. Forty-six percent of respondents said the damage caused by insider attacks was more damaging than outside attacks (CSI, 2011).

### Common Characteristics and Traits of Malicious Insiders

Based on research conducted by the Software Engineering Institute at Carnegie Mellon University and the U.S. Secret Service National Threat Assessment Center, malicious insiders often are perceived or known to be difficult or high-maintenance employees who are:

- obviously unhappy or extremely resentful;
- having financial, performance, or behavioral problems;
- at risk (or perceived to be) for layoff or termination.

Keep in mind that not all malicious insiders fit this characterization. Insiders involved in national security espionage, for example, may exhibit few outward signs. In the majority of cases, however, management and/or human resources personnel were well aware of the employees and their issues prior to an incident.

### *Personal Factors Associated With Insiders*

The following motives and personal situations frequently are linked with malicious insiders:

- **Personal or Behavioral Problems**
  - Vulnerable to blackmail
  - Experiencing family or financial problems
  - Prone to compulsive or destructive behavior
  - Subject to ego or self-image issues
- **Personal Desires**
  - Seeking adventure or thrill

- Seeking approval and returned favors
- Professing allegiance
- **Workplace Issues**
  - Experiencing problems at work
  - Feeling anger or need for revenge

### *Organizational Factors That Embolden Malicious Insiders*

The following organizational factors have been known to encourage or present opportunities to potential malicious insiders.

- **Access and Availability**
  - Ease of access to materials and information
  - Ability to exit the facility or network with materials or information
- **Policies and Procedures**
  - Undefined or inadequate policies and procedures
  - Inadequate training
  - Lack of training
- **Time Pressure and Consequences**
  - Rushed employees
  - Perception of lack of consequences

### **Insider Activities and Behavior You May See**

Insider threats may be detected through particular activities and behavior on the part of the insider. This section of the presentation identifies those indicators. These activities and behaviors often will appear unusual or suspicious. Keep in mind there may be several explanations for a particular activity or behavior identified here, but when combined with other factors, certain activity or behavior point toward a possible insider threat. A combination or confluence of indicators should not be ignored.

### *Types of Insider Activities and Behavior*

Unusual or suspicious insider activities and behavior can be described using the following categories:

- Inappropriate interest or acquisition
- Unauthorized or unusual computer use
- Unusual hours, contacts, or travel
- Secretive or peculiar behavior
- Personal or financial issues



### *Employer Actions*

- Clearly communicating and consistently enforcing security policies and controls.
- Ensuring that proprietary information and materials are adequately, if not robustly, protected.
- Routinely monitoring computer networks for suspicious activity.
- Ensuring security (to include computer network security) personnel have the tools they need.
- Consulting with legal and law enforcement experts as needed to ensure compliance with the law.

### *Employee Actions*

Critical infrastructure organizations today employ a number of security measures to reduce the risk of insider threats. The measures involving employees include, but are not limited to:

- using appropriate screening processes to select new employees;
- educating employees about security or other protocols;
- encouraging and providing nonthreatening, convenient ways for employees to report suspicious in a confidential manner;
- becoming familiar with behavior and activities associated with malicious insiders;
- documenting and evaluating incidents of suspicious or disruptive behavior;
- consulting with legal and law enforcement experts as needed to ensure compliance with the law.

## THE VULNERABILITY ASSESSMENT<sup>1</sup>

A VA involves an in-depth analysis of the facility's functions, systems, and site characteristics to identify facility weaknesses and lack of redundancy, and determine mitigations or corrective actions that can be designed and implemented to reduce the vulnerabilities. A VA can be a stand-alone process or part of a full-risk assessment. During this assessment, the analysis of site assets is based on: (a) the identified threat; (b) the criticality of the assets; and

---

<sup>1</sup> Much of the information in this section is from U.S. Department of Energy (DOE 2002) *Vulnerability Assessment Methodology: Electric Power Infrastructure*. Washington, DC; US Army Research Laboratory (2000) *Vulnerability Risk Assessment, ARL-TR-1045*. Washington, DC; DOD; U.S. Dept of Justice, (2002) *A method to Assess the Vulnerability of U.S. Chemical Facilities*. Washington, DC.

(c) the level of protection chosen (i.e., based on willingness or unwillingness to accept risk).

It is important to point out that post 9/11 all sectors have taken great strides to protect their critical infrastructure. For instance, government and industry have developed VA methodologies for critical infrastructure systems and trained thousands of auditors and others to conduct them.

The actual complexity of VAs will range based upon the design and operation of the financial services asset. The nature and extent of the VA will differ among systems based on a number of factors, including system size and potential population, and safety evaluations also vary based on knowledge and types of threats, available security technologies, and applicable local, state, and federal regulations. Preferably, a VA is “performance based,” meaning that it evaluates the risk to the financial services assets based on the effectiveness (performance) of existing and planned measures to counteract adversarial actions. According to USEPA (2002), the common elements of VA are as follows:

- Characterization of the CS sector, including its mission and objectives.
- Identification and prioritization of adverse consequences to avoid.
- Determination of critical assets that might be subject to malevolent acts that could result in undesired consequences.
- Assessment of the likelihood (qualitative probability) of such malevolent acts from adversaries.
- Evaluation of existing countermeasures.
- Analysis of current risk and development of a prioritized plan for risk reduction.

### **Benefits of Assessments**

CS sector members should routinely perform VAs to better understand threats and vulnerabilities, determine acceptable levels of risk, and stimulate action to mitigate identified vulnerabilities. These assessments are based upon the extensive knowledge of regulators and guidance issued, and takes into account physical, cyber, and human vulnerabilities, available redundancy, and the sector’s reliance on sector-sector assets, systems and processes, and cross-sector reliance on these factors. Consequence assessments include direct economic impacts and national confidence impacts, and are based on expert judgment and exercises. The direct benefits of performing a VA include:

- **Build and broaden awareness**—The assessment process directs senior management’s attention to security. Security issues, risks, vulnerabilities,

mitigation options, and best practices are brought to the surface. Awareness is one of the least expensive and most effective methods for improving the organization's overall security posture.

- **Establish or evaluate against a baseline**—If a baseline has been previously established, an assessment is an opportunity for a checkup to gauge the improvement or deterioration of an organization's security posture. If no previous baseline has been performed (or the work was not uniform or comprehensive), an assessment is an opportunity to integrate and unify previous efforts, define common metrics, and establish a definitive baseline. The baseline also can be compared against best practices to provide perspective on an organization's security posture.
- **Identify vulnerabilities and develop responses**—Generating lists of vulnerabilities and potential responses is usually a core activity and outcome of an assessment. Sometimes, due to budget, time, complexity, and risk considerations, the response selected for many of the vulnerabilities may be nonaction, but after completing the assessment process these decisions will be conscious ones, with a documented decision process and item-by-item rationale available for revisiting issues at scheduled intervals. This information can help drive or motivate the development of a risk management process.
- **Categorize key assets and drive the risk management process**—An assessment can be a vehicle for reaching corporate-wide consensus on a hierarchy of key asset. This ranking, combined with threat, vulnerability, and risk analysis, is at the heart of any risk management process. For many organizations, the Y2K that was the first time a company-wide inventory and ranking of key assets was attempted. An assessment allows any organization to revisit that list from a broader and more comprehensive perspective.
- **Develop and build internal skills and expertise**—A security assessment, when not implemented in an "audit" mode, can serve as an excellent opportunity to build security skills and expertise within an organization. A well-structure assessment can have elements that sever as a forum for crosscutting groups to come together and share issues, experiences, and expertise. External assessors can be instructed to emphasize "teaching and collaborating" rather than "evaluating" (the traditional role). Whatever the organization's current level of sophistication, a long-term goal should be to move the organization toward a capability for self-assessment.
- **Promote action**—Although disparate security efforts may be underway in an organization, an assessment can crystallize and focus management attention and resources on solving specific and systemic security

problems. Often the people in the trenches are well aware of security issues (and even potential solutions) but are unable to convert their awareness to action. An assessment provides an outlet for their concerns and the potential to surface these issues at appropriate levels (legal, financial, executive) and achieve action. A well-designed and executed assessment not only identifies vulnerabilities and makes recommendations; it also gains executive buy-in, identifies key players, and establishes a set of crosscutting groups that can convert those recommendations into action.

- **Kick off an ongoing security effort**—An assessment can be used as a catalyst to involve people throughout the organization in security issues, build crosscutting teams, establish permanent forums and councils, and harness the momentum generated by the assessment to build an ongoing institutional security effort. The assessment can lead to the creation of either an actual or a virtual (matrixed) security organization.

## VA Process

Table 6.1 provides an overview of the elements included in the assessment methodology. The elements included in this overview are based on actual in-field experience and lessons learned.

In table 6.1, step 3 deals with identification of asset criticality. This is an important step in any VA. Identifying asset criticality serves several functions:

- It enables more careful consideration of factors that affect risk, including threats, vulnerabilities, and consequences of loss or compromise of the asset.
- It enables more focused and thorough consideration of loss or compromise of the asset.
- It enables leaders to develop robust methods for managing consequences of asset loss (restoration).
- It provides a means to increase awareness of a broad range of employees to protect truly critical assets and to differentiate in policies and procedures the heightened protection they require.

As previously indicated, identifying the criticality of assets is used primarily to focus the vulnerability analysis efforts. It also assists with the ranking of various recommendations for reducing vulnerabilities. As an example, let's take a look at the criticality of electric power assets and operations included in the normal operation of financial services sector assets:

**Table 6.1 Basic Elements in Vulnerability Assessments**

<i>Element</i>	<i>Points to Consider</i>
1. Characterization of the communications entity, including its mission and objectives.	<ul style="list-style-type: none"> <li>• What are the important missions of the system to be assessed? Define the highest priority services provided by the utility. Identify the industry's customers:               <ul style="list-style-type: none"> <li>◦ General public</li> <li>◦ Government</li> <li>◦ Military</li> <li>◦ Industrial</li> <li>◦ Critical care</li> <li>◦ Retail operations</li> <li>◦ Firefighting</li> </ul> </li> <li>• What are the most important facilities, processes, and assets of the system for achieving the mission objectives and avoiding undesired consequences? Describe the:               <ul style="list-style-type: none"> <li>◦ Industry facilities</li> <li>◦ Operating procedures</li> <li>◦ Management practices that are necessary to achieve the mission objectives</li> <li>◦ How the industry operates</li> <li>◦ Treatment processes</li> <li>◦ Storage methods and capacity</li> <li>◦ Energy use and storage</li> <li>◦ Distribution system</li> </ul> </li> </ul> <p>In assessing those assets that are critical, consider critical customers, dependence on other infrastructures (e.g., chemical, transportation, communications), contractual obligations, single points of failure, chemical hazards and other aspects of the industry's operations, or availability of industry utilities that may increase or decrease the criticality of specific facilities, processes, and assets.</p>

2. Identification and prioritization of adverse consequences to avoid.
  - Take into account the impacts that could substantially disrupt the ability of the system to provide a safe and reliable supply of materials. CS sector systems should use the vulnerability assessment process to determine how to reduce risk associated with the consequences of significant concern.
  - Ranges of consequences or impacts for each of these events should be identified and defined. Factors to be considered in assessing the consequences may include:
    - Magnitude of service disruption
    - Economic impact (such as replacement and installation costs for damaged critical assets or loss of revenue due to service outage)
    - Number of illnesses or deaths resulting from an event
    - Impact on public confidence in the material supply
    - Chronic problems arising from specific events
    - Other indicators of the impact of each event as determined by the financial services sector.

Risk reduction recommendations at the conclusion of the vulnerability assessment strive to prevent or reduce each of these consequences.
3. Determination of critical assets that might be subject to malevolent acts that could result in undesired consequences.
  - What are the malevolent acts that could reasonably cause undesired?
    - Electronic, computer, or other automated systems which are utilized by the financial sector entities (e.g., Supervisory Control and Data Acquisition (SCADA))
    - The use, storage, or handling of various financial services supplies
    - The operation and maintenance of such systems
4. Assessment of the likelihood (qualitative probability) of such malevolent acts from adversaries.
  - Determine the possible modes of attack that might result in consequences of significant concern based on critical assets of the financial services sector entity. The objective of this step of the assessment is to move beyond what is merely possible and determine the likelihood of a particular attack scenario. This is a very difficult task as there is often insufficient information to determine the likelihood of a particular event with any degree of certainty.
  - The threats (the kind of adversary and the mode of attack) selected for consideration during a vulnerability assessment will dictate, to a great extent, the risk reduction measures that should be designed to counter the threat(s). Some vulnerability assessment methodologies refer to this as a “Design Basis Threat” (DBT) where the threat serves as the basis for the design of countermeasures, as well as the benchmark against which vulnerabilities are assessed. It should be noted that there is no single DBT or threat profile for all financial systems in the United States. Differences in geographic location, size of the utility, previous attacks in the local area, and many other factors will influence the threat(s) that the financial services sector entity should consider in their assessments. Financial services sector entities should consult with the local FBI and/or other law enforcement agencies, public officials, and others to determine the threats upon which their risk reduction measures should be based.

(Continued)

**Table 6.1 Basic Elements in Vulnerability Assessments—Continued**

<i>Element</i>	<i>Points to Consider</i>
<p>5. Evaluation of existing countermeasures. (Depending on countermeasures already in place, some critical assets may already be sufficiently protected. This step will aid in identification of the areas of greatest concern and help to focus priorities for risk reduction.)</p>	<ul style="list-style-type: none"> <li>• What capabilities does the system currently employ for detection, delay, and response?               <ul style="list-style-type: none"> <li>◦ Identify and evaluate current detection capabilities such as intrusion detection systems, energy quality monitoring, operational alarms, guard post orders, and employee security awareness programs.</li> <li>◦ Identify current delay mechanisms such as locks and key control, fencing, structure integrity of critical assets, and vehicle access checkpoints.</li> <li>◦ Identify existing policies and procedures for evaluation and response to intrusion and system malfunction alarms, and cyber system intrusions.</li> </ul> </li> <li><b>It is important to determine the performance characteristics. Poorly operated and maintained security technologies provide little or no protection.</b></li> <li>• What cyber protection system features does the facility have in place? Assess what protective measures are in place for the SCADA and business-related computer information systems such as:               <ul style="list-style-type: none"> <li>◦ Firewalls</li> <li>◦ Modem access</li> <li>◦ Internet and other external connections, including wireless data and voice communications.</li> <li>◦ Security policies and protocols</li> </ul> </li> </ul> <p><b>It is important to identify whether vendors have access rights and/or “backdoors” to conduct system diagnostics remotely.</b></p> <ul style="list-style-type: none"> <li>• What security policies and procedures exist, and what is the compliance record for them? Identify existing policies and procedures concerning:               <ul style="list-style-type: none"> <li>◦ Personal security</li> <li>◦ Physical security</li> <li>◦ Key and access badge control</li> <li>◦ Control of system configuration and operational data</li> <li>◦ Vendor deliveries</li> <li>◦ Security training and exercise records</li> </ul> </li> </ul>

6. Analysis of current risk and development of a prioritized plan for risk reduction.
- Information gathered on threat, critical assets, financial services sector operations, consequences, and existing countermeasures should be analyzed to determine the current level of risk. The utility should then determine whether current risks are acceptable or risk reduction measures should be pursued.
  - Recommended actions should measurably reduce risks by reducing vulnerabilities and/or consequences through improved deterrence, delay, detection, and/or response capabilities or by improving operational policies or procedures. Selection of specific risk reduction actions should be completed prior to considering the cost of the recommended action(s). Facilities should carefully consider both short- and long-term solutions. An analysis of the cost of short- and long-term risk reduction actions may impact which actions the utility chooses to achieve its security goals.
  - Facilities may also want to consider security improvements. Security and general infrastructure may provide significant multiple benefits. For example, improved treatment processes or system redundancies can both reduce vulnerabilities and enhance day-to-day operation.
  - Generally, strategies for reducing vulnerabilities fall into three broad categories:
    - Sound business practices—affect policies, procedures, and training to improve the overall security-related culture at the chemical facility. For example, it is important to ensure rapid communication capabilities exist between public health authorities and local law enforcement and emergency responders.
    - System upgrades—include changes in operations, equipment, processes, or infrastructure itself that make the system fundamentally safer.
    - Security upgrades—improve capabilities for detection, delay, or response.
-



*Physical*

- Generators
- Substations
- Transformers
- Transmission lines
- Distribution lines
- Control center
- Warehouses
- Office buildings
- Internal and external infrastructure dependencies

*Cyber*

- SCADA systems
- Networks
- Databases
- Business systems
- Telecommunications

*Interdependencies*

- Single-point nodes of failures
- Critical infrastructure components of high reliance

## VA METHODOLOGY

VA methodology consists of ten elements. Each element along with a description of each is listed below (US DOE, 2002).

1. Network architecture
2. Threat environment
3. Penetration testing
4. Physical security
5. Physical asset analysis
6. Operations security
7. Policies and procedures
8. Impact analysis
9. Infrastructure interdependencies
10. Risk characterization

### Network Architecture

This element provides an analysis of the information assurance features of the information network(s) associated with the organization's critical

information systems. Information examined should include network topology and connectivity (including subnets), principal information assets, interface and communication protocols, function and lineage of major software and hardware components (especially those associated with information security such as intrusion detectors), and policies and procedures that govern security features of the network.

Procedures for information assurance in the system, including authentication of access and management of access authorization, should be reviewed. The assessment should identify any obvious concerns related to architectural vulnerabilities, as well as operating procedures. Existing security plans should be evaluated, and the results of any prior testing should be analyzed. Results from the network architecture assessment should include potential recommendations for changes in the information architecture, functional areas and categories where testing is needed, and suggestions regarding system design that would enable more effective information and information system protection.

Three techniques are often used in conducting the network architecture assessment:

1. Analysis of network and system documentation during and after the site visit.
2. Interview with facility staff, managers, and chief information officer.
3. Tours and physical inspections of key facilities.

## **Threat Environment**

Development of a clear understanding of the threat environment is a fundamental element of risk management. When combined with an appreciation of the value of the information assets and systems, and the impact of unauthorized access and subsequent malicious activity, an understanding of threats provides a basis for better defining the level of investment needed to prevent such access.

The threat of a terrorist attack to CS sector infrastructure is real and could come from several areas, including physical, cyber, and interdependency. In addition, threats could come from individuals or organizations motivated by financial gain or persons who derive pleasure from such penetration (e.g., recreational hackers, disgruntled employees). Other possible sources of threats are those who want to accomplish extremist goals (e.g., environmental terrorists, antinuclear advocates) or embarrass one or more organizations.

This element should include a characterization of these and other threats, identification of trends in these threats, and ways in which vulnerabilities are exploited. To the extent possible, characterization of the threat environment should be localized, that is, within the organization's service area.

## Penetration Testing

The purpose of network penetration testing is to utilize active scanning and penetration tools to identify vulnerabilities that a determined adversary could easily exploit. Penetration testing can be customized to meet the specific needs and concerns of the financial services sector unit. In general, penetration testing should include a test plan and details on the rules of engagement (ROE). It should also include a general characterization of the access points of the critical information systems and include a general characterization of the access points to the critical information systems and communication interface connections, modem network connections, access points to principal network routers, and other external connections. Finally, penetration testing should include identified vulnerabilities and, in particular, whether access could be gained to the control network or specific subsystem or devices that have a critical role in assuring continuity of service.

Penetration testing consists of an overall process of establishing the ground rules or ROE for the test; establishing a white cell for continuous communication; developing a format or methodology for the test; conducting the test; and generating a final report that details methods, findings, and recommendations.

Penetration testing methodology consists of three phases: reconnaissance, scenario development, and exploitation. A one-time penetration test can provide the utility with valuable feedback; however, it is far more effective if performed on a regular basis. Repeated testing is recommended because new threats develop continuously, and the networks, computers, and architecture of the financial services sector unit or utility are likely to change over time.

## Physical Security

A critical dependency for the CS sector as well as the other sectors is related to the physical security of the facilities. The purpose of physical security assessment is to examine and evaluate the systems in place (or being planned) and to identify potential improvements in this area for the sites evaluated. Physical security systems include access controls, barriers locks and keys, badges and passes, intrusion detection devices and associated alarm reporting and display, closed-circuit television (assessment and surveillance), communications equipment (telephone, two-way radio, intercom, cellular), lighting (interior and exterior), power sources (line, battery, generator), inventory control, postings (signs), security system wiring, and protective force. Physical security systems are reviewed for design, installation operation, maintenance, and testing.

The physical security assessment should focus on those sites directly related to the critical facilities, including information systems and assets required for

operation. Typically included are facilities that house critical equipment or information assets or networks dedicated to the operation of electric, oil, or gas transmission, storage, or delivery systems. Other facilities can be included on the basis of criteria specified by the organization being assessed. Appropriate levels of physical security are contingent upon the value of company assets, the potential threats to these assets, and the cost associated with protecting the assets. Once the cost of implementing/maintaining physical security programs is known, it can be compared to the value of the company assets, thus providing the necessary information for risk management decisions. The focus of the physical security assessment task is determined by prioritizing the company assets; that is, the most critical assets receive the majority of the assessment activity.

At the start of the assessment, survey personnel should develop a prioritized listing of company assets. This list should be discussed with company personnel to identify areas of security strengths and weaknesses. During these initial interviews, assessment area that would provide the most benefit to the company should be identified; once known, they should become the major focus of the assessment activities.

The physical security assessment of each focus area usually consists of the following:

- Physical security program (general)
- Physical security program (planning)
- Barriers
- Access controls/badges
- Locks/keys
- Intrusion detection systems
- Communications equipment
- Protective force/local law enforcement agency

The key to reviewing the above topics is not to just identify if they exist but to determine the appropriate level that is necessary and consistent with the value of the asset being protected. The physical security assessment worksheets provide guidance on appropriate levels of protection.

Once the focus and content of the assessment task have been identified, the approach to conduction the assessment can be either at the “implementation level” or at the “organizational level.” The approach taken depends on the maturity of the security program.

For example, a company with a solid security infrastructure (staffing plans/procedures, funding) should receive a cursory review of these items; however, facilities where the security programs are being implemented should receive a detailed review. The security staff can act upon deficiencies found at the facilities, once reported.

For companies with an insufficient security organization, the majority of time spent on the assessment should take place at the organizational level to identify the appropriate staffing/funding necessary to implement security programs to protect company assets. Research into specific facility deficiencies should be limited to finding just enough examples to support any staffing/funding recommendations.

## Physical Asset Analysis

The purpose of the physical asset analysis is to examine the systems and physical operational assets to ascertain whether vulnerabilities exist. Included in this element is an examination of asset utilization, system redundancies, and emergency operating procedures. Consideration should also be given to the topology and operating practices for electric and gas transmission, processing, storage, and delivery, looking specifically for those elements that either singly or in concert with other factors provides a high potential for disrupting service. This portion of the assessment determines company and industry trends regarding these physical assets. Historic trends, such as asset utilization, maintenance, new infrastructure investments, spare parts, SCADA linkages, and field personnel are part of the scoping element.

The proposed methodology for physical assets is based on a macro-level approach. The analysis can be performed with company data, public data, or both. Some companies might not have readily available data or might be reluctant to share that data.

Key output from analysis should be graphs that show trends. The historic data analysis should be supplemented with on-site interviews and visits. Items to focus on during a site visit include the following:

- Trends in field testing
- Trends in maintenance expenditures
- Trends in infrastructure investments
- Historic infrastructure outages
- Critical system components and potential system bottlenecks
- Overall system operation controls
- Use and dependency of SCADA systems
- Linkages of operation staff with physical and IT security
- Adequate policies and procedures
- Communications with other regional financial assets
- Communications with external infrastructure providers
- Adequate organizational structure

## Operations Security

Operations security (OPSEC) is the systematic process of denying potential adversaries (including competitors or their agents) information about capabilities and intentions of the host organization. OPSEC involves identifying, controlling, and protecting generally nonsensitive activities concerning planning and execution of sensitive activities. The OPSEC assessment reviews the processes and practices employed for denying adversary access to sensitive and nonsensitive information that might inappropriately aid or abet an individual's or organization's disproportionate influence over system operation. This assessment should include a review of security training and awareness programs, discussions with key staff, and tours of appropriate principal facilities. Information that might be available through public access should also be reviewed.

## Policies and Procedures

The policies and procedures by which security is administered (1) provide the basis for identifying and resolving issues; (2) establish the standards of reference for policy implementation; and (3) define and communicate roles, responsibilities, authorities, and accountabilities for all individuals and organizations interface with critical systems. They are the backbone for decisions and day-to-day security operations. Security policies and procedures become particularly important at times when multiple parties must interact to effect a desired level of security and when substantial legal ramifications could result from policy violations. Policies and procedures should be reviewed to determine whether they (1) address the key factors affecting security; (2) enable effective compliance, implementation, and enforcement; (3) reference or conform to established standards; (4) provide clear and comprehensive guidance; and (5) effectively address the roles, responsibilities, accountabilities, and authorities.

The objective of the policies and procedures assessment task is to develop a comprehensive understanding of how a facility protects its critical assets through the development and implementation of policies and procedures. Understanding and assessing this area provide a means of identifying strengths and areas for improvements that can be achieved through:

- Modification of current policies and procedures
- Implementation of current policies and procedures
- Development and implementation of new policies and procedures
- Assurance of compliance with policies and procedures
- Cancellation of policies and procedures that are no longer relevant, or are inappropriate, for the facility's current strategy and operations

## Impact Analysis

A detailed analysis should be conducted to determine the influence that exploitation of unauthorized access to critical facilities or information systems might have on an organization's operations (e.g., market and/or physical operations). In general, such an analysis would require thorough understanding of (1) the applications and their information processing, (2) decisions influenced by this information, (3) independent checks and balances that might exist regarding information upon which decisions are made, (4) factors that might mitigate the impact of unauthorized access, and (5) secondary impacts of such access. Similarly, the physical chain of events following disruption, including the primary, secondary, and tertiary impacts of disruption, should be examined.

The purpose of the impact analysis is to help estimate the impact that detrimental impacts could have on financial services sector units. The impact analysis provides an introduction to risk characterization by providing quantitative estimates of these impacts so that the CS sector unit can implement a risk management program and weigh the risks and costs of various mitigation measures.

## Infrastructure Interdependencies

The term “infrastructure interdependencies” refers to the physical and electronic (cyber) linkages within communications and among our nation's critical infrastructures—energy (electric power, oil, natural gas), telecommunications, transportation, water supply systems, banking and finance, emergency services, and government services. This task identifies the direct infrastructure linkages between and among the infrastructures that support critical facilities as recognized by the organization. Performance of this task requires a detailed understanding of an organization's functions, internal infrastructures, and how these link to external infrastructures.

The purpose of the infrastructure interdependencies assessment is to examine and evaluate the infrastructures (internal and external) that support critical facility functions, along with their associated interdependencies and vulnerabilities.

## Risk Characterization

Risk characterization provides a framework for prioritizing recommendations across all task areas. The recommendations for each task area are judged against a set of criteria to help prioritize the recommendations and assist the organization in determining the appropriate course of action. It provides a

framework for assessing vulnerabilities, threats, and potential impacts (determined in the other tasks). In addition, the existing risk analysis and management process at the organization should be reviewed and, if appropriate, utilized for prioritizing recommendations. The degree to which corporate risk management includes security factors is also evaluated.

## VA PROCEDURES

VA procedures can be conducted for CS sector assets using various methodologies. For example, the checklist analysis is an effective technology. In addition, Pareto analysis (80/20 principle), relative ranking, pre-removal risk assessment (PRRA), change analysis, failure mode and effects analysis (FMEA), fault tree analysis, event tree analysis, what-if analysis, and Hazard and Operability (HAZOP) can be used in conducting the assessment.

Based on personal experience, the what-if analysis and HAZOP seem to be the most user-friendly methodologies to use. A sample what-if analysis procedural outline is presented below, followed by a brief explanation and outline for conducting HAZOP.

### *What-If Analysis Procedure/Sample What-If Questions*

The steps in a what-if checklist analysis are as follows:

1. Select the team (personnel experienced in the process)
2. Assemble information (piping and instrumentation drawings (P&IDs), process flow diagrams (PFDs), operating procedures, equipment drawings, etc.)
3. Develop a list of What-If questions
4. Assemble your team in a room where each team member can view the information
5. Ask each What-If question in turn and determine:
  - What can cause the deviation from design intent that is expressed by the question?
  - What adverse consequences might follow?
  - What are the existing design and procedural safeguards?
  - Are these safeguards adequate?
  - If these safeguards are not adequate, what additional safeguards does the team recommend?
6. As the discussion proceeds, record the answers to these questions in tabular format.



7. Do not restrict yourself to the list of questions that you developed before the project started. The team is free to ask additional questions at any time.
8. When you have finished the What-If questions, proceed to examine the checklist. The purpose of this checklist is to ensure that the team has not forgotten anything. While you are reviewing the checklist, other What-If questions may occur to you.
9. Make sure that you follow up all recommendations and action items that arise from the hazards evaluation.

## HAZOP Analysis

The HAZOP analysis technique uses a systematic process to (1) identify possible deviations from normal operations and (2) ensure that safeguards are in place to help prevent accidents. The HAZOP uses special adjectives (speed, flow, pressure, etc.) combined process conditions ( “more,” “less,” “no,” etc.) to systematically consider all credible deviations from normal conditions. The adjectives, called guide words, are a unique feature of HAZOP analysis.

In this approach, each guide word is combined with relevant process parameters and applied at each point (study node, process section, or operating step) in the process that is being examined (tables 6.2 and 6.3).

**Table 6.2 Guide Words**

<i>Guide Words</i>	<i>Meaning</i>
No	Negation of the Design Intent
Less	Quantitative Decrease
More	Quantitative Increase
Part Of	Other Material Present by Intent
As Well As	Other Materials Present Unintentionally
Reverse	Logical Opposite of the Intent
Other Than	Complete Substitution

**Table 6.3 Common HAZOP Analysis Process Parameters**

<i>Flow</i>	<i>Time</i>	<i>Frequency</i>	<i>Mixing</i>
Pressure	Composition	Viscosity	Addition
Temperature	pH	Voltage	Separation
Level	Speed	Information	Reaction

The following is an example of creating deviations using guide words and process parameters:

<i>Guide Words</i>		<i>Parameter</i>		<i>Deviation</i>
NO	+	FLOW	=	NO FLOW
MORE	+	PRESSURE	=	HIGH PRESSURE
AS WELL AS	+	ONE PHASE	=	TWO PHASE
OTHER THAN	+	OPERATION	=	MAINTENANCE
MORE	+	LEVEL	=	HIGH LEVEL

Guide words are applied to both the more general parameters (e.g., react, mix) and the more specific parameters (e.g., pressure, temperature). With the general parameters, it is not unusual to have more than one deviation from the application of one guide word. For example, “more reaction” could mean either that a reaction takes place at a faster rate or that a greater quantity of product results. On the other hand, some combination of guide words and parameters will yield no sensible deviation (e.g., “as well as” with “pressure”).

## HAZOP Procedure

1. Select the team.
2. Assemble information (P&IDs, PFDs, operating procedures, equipment drawings, etc.).
3. Assemble your team in a room where each team member can view P&IDs.
4. Divide the system you are reviewing into nodes (you can present the nodes, or the team can choose them as you go along).
5. Apply appropriate deviations to each node. For each deviation, address the following questions:
  - What can cause the deviation from design intent?
  - What adverse consequences might follow?
  - What are the existing design and procedural safeguards?
  - Are these safeguards adequate?
  - If these safeguards are not adequate, what does the team recommend?
6. As the discussion proceeds, record the answers to these questions in tabular format.

## VULNERABILITY ASSESSMENT: CHECKLIST PROCEDURE

In performing the VA of any CS sector unit or facility, one of the simplest methodologies to employ is the checklist. The Building Vulnerability

Assessment Checklist developed by the Department of Veterans Affairs (VA) and part of EEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks against Buildings*, is highly recommended. It is an excellent guide for conducting a viable Checklist-Type Vulnerability Assessment. This checklist will help you to prepare your Threat Assessment because it allows a consistent security evaluation of designs at various levels. The checklist can be used as screening tool for preliminary design VA and supports the preparation of all steps for use by the assessment teams during preparation for interviews with facility representatives to help assure that all relevant aspects of the financial services assets are considered in the survey.

Through the VA, the financial services sector has determined that some of its greatest challenges are its dependence on the telecommunications network and the power grid.

## REFERENCES AND RECOMMENDED READING

- Congressional Budget Office (CBO). 2004. "Homeland Security and the Private Sector." <https://www.cbo.gov/ft>.
- Computer Security Institute (CSI). 2011. "2010/2011 Computer Crime and Security Survey." Orlando, FL.
- Department of Homeland Security (DHS). 2009. "National Infrastructure Protection Plan." <https://www.dhs.gov/cisa/national-infrastructure-protection-plan>.
- Department of Homeland Security (DHS). 2003. "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets." [https://www.dhs.gov/xlibrary/assets/Physical\\_Strategy.pdf](https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf).
- Department of Homeland Security (DHS). 2013. "Homeland Security Directive 7: Critical Infrastructure Identification, Prioritization, and Protection." <https://www.dhs.gov/homeland-security-presidential-directive-7>.
- Department of Homeland Security (DHS). 2015. "Commercial Facilities Sector—Specific Plan." Washington, DC.
- Department of Defense Directive (DoDD). 2010. "Department of Defense (DoD) Policy and Responsibility for Critical Infractions—DODD 3020.40." Washington, DC.
- Federal Bureau of Investigation (FBI). 2012. "Insider Espionage. Report before the House Committee on Homeland Security Subcommittee on Counter Terrorism and Intelligence." Washington, DC.
- Federal Emergency Management Agency (FEMA). 2015. "Protecting Critical Infrastructure Against Insider Threats." <https://training.fema.gov/is/courseoverview.aspx?code=is-915>.
- Intelligence and National Security Alliance (INSA). 2017. "Building a Stronger Intelligence Community." Arlington, VA. <https://www.insaonline.org/>.

- National Infrastructure Advisory Council. 2008. *First Report and Recommendations on the Insider Threat to Critical Infrastructure*. Washington, DC.
- Spellman, F.R. 1997. *A Guide to Compliance for PSM/RMP*. Lancaster, PA: Technomic Publishing Company.
- U.S. Department of Energy (DOE). 2010. "Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan." Washington, DC.
- U.S. Department of Energy (DOE). 2002. "Vulnerability Assessment Methodology: Electric Power Infrastructure." Washington, DC.



## Chapter 7

# Preparation

## *When is Enough, Enough?*

Question: When preparing to respond to terrorist acts against people, malls, schools, sports stadiums, libraries, communications systems, government facilities and financial services assets when is enough, enough?

Answer: Until we can read the terrorists' minds, enough preparation is never enough. Simply, preparation is ongoing and never-ending.

—Frank R. Spellman

### INTRODUCTION

The possibility of terrorism—attacks on U.S. CS sector infrastructure—doesn't generate the same attention as potential nuclear, biological, or chemical terrorism. Why? Simply, when you ask a citizen about U.S. CS sector assets, he or she just looks at you like you are some kind of wacko. I know, I have asked. Anyway, however, because of the seriousness of the threat of terrorism to the nation's CS sector and the enormous economic and security implications of such attacks, the Federal Communications Commission, the Department of Energy, the Environmental Protection Agency, the DHS, and other agencies have worked nonstop since 9/11 in gathering and providing as much advice and guidance as possible to aid CS securities sector personnel in protecting CS sector assets and associated critical support infrastructure. In this chapter, we provide an overview of important tools that can be used in protecting CS sector to guard against the threat of terrorism. In the discussion, keep in mind that even though a CS sector issue the guidance provided could be used to protect the other critical infrastructure sectors.

## THREATS AND INCIDENTS

Based on evidence of potential losses from past accidents, indication of the potential human and environmental losses and economic costs from an attack on a CS sector facility or producer comes from major incidents that have occurred both abroad and in the United States. Those events indicate that the human and environmental losses could be significant (CBO, 2004).

CS sector threats and incidents may be of particular concern due to the range of potential consequences:

- Creating an adverse impact on public health within a population.
- Disrupting system operations and interrupting the supply of critical military components.
- Causing physical damage to system infrastructure.
- Reducing public confidence in the financial services system.
- Long-term denial of basic security and protection and the cost of replacement.

Keep in mind that some of these consequences would only be realized in the event of a successful terrorist incident; however, the mere threat of terrorism can also have an adverse impact on industries that depend on a safe, steady supply of commercial and financial services. In addition, the economic implications of such attacks are potentially enormous. For example, many believe that the reason we are looking at oil at more than \$60 a barrel is the fact that we have a “terror premium” factored into the price of a barrel of oil.

While it is important to consider the range of possibilities associated with a particular threat, assessments are typically based on the probability of a particular occurrence. Determining probability is somewhat subjective, and is often based on intelligence and previous incidents. As mentioned, there are historical accounts of accidental incidents that have caused tremendous death and destruction.

### Threat Warning Signs

A threat warning is an occurrence or discovery that indicates a potential threat that triggers an evaluation of the threat. It is important to note that these warnings must be evaluated in the context of typical industry activity and previous experience in order to avoid false alarms. Following is a brief description of potential warnings.

- *Security Breach.* Physical security breaches, such as unsecured doors, open hatches, and unlocked/forced gates, are probably the most common threat

warnings. In most cases, the security breach is likely related to lax operations or typical criminal activity such as trespassing, vandalism, and theft. However, it may be prudent to assess any security breach with respect to the possibility of attack.

- *Witness Account.* Awareness of an incident may be triggered by a witness account of tampering. CS sector sites/facilities should be aware that individuals observing suspicious behavior near CS sector facilities will likely call 911. In this case, the incident warning technically might come from law enforcement, as described below. **Note:** the witness may be a commercial service employee engaged in their normal duties.
- *Direct Notification by Perpetrator.* A threat may be made directly to the CS sector site, plant, or facility, either verbally or in writing. Historical incidents would indicate that verbal threats made over the phone are more likely than written threats. While the notification may be a hoax, threatening a CS sector unit is a crime and should be taken seriously.
- *Notification by Law Enforcement.* A CS sector site/facility may receive notification about a threat directly from law enforcement, including local, country, state, or federal agencies. As discussed previously, such a threat could be a result of suspicious activity reported to law enforcement, either by a perpetrator, a witness, or by the news media. Other information, gathered through intelligence or informants, could also lead law enforcement to conclude that there may be a threat to the CS sector site/facility. While law enforcement will have to lead in the criminal investigation, the CS sector site/facility has primary responsibility for the safety of its equipment and processes. Thus, the plant's role will likely be to help law enforcement to appreciate the public health implications of a particular threat as well as the technical feasibility of carrying out a particular threat.
- *Notification by News Media.* A threat to destroy a CS site/facility might be delivered to the news media or the media may discover a threat. A conscientious reporter would immediately report such a threat to the police, and either the reporter or the police would immediately contact the CS sector site/facility. This level of professionalism would provide an opportunity for the asset to work with the media and law enforcement to assess the credibility of the threat before any broader notification is made.

## RESPONSE TO THREATS

*Note:* This section is not designed to discuss what specific steps to take in responding to a terrorist threat. Rather, the questions addressed in this section are “Why is it necessary to plan to respond to Commercial Services sector threats at all?” and “When have I done enough?”



Federal, state, and local programs already exist that—with varying degrees of effectiveness—encourage or require the operators of CS sector sites/facilities to boost their efforts, to promote safety and security, and to share information that can help local governments plan for emergencies.

Proper planning is a delicate process because public health measures are rarely noticed or appreciated (like buried utility pipes, they are often hidden functions except when they fail)—then they are very visible. The result of too little action, including no response at all, can have disastrous consequences potentially resulting in public injuries or fatalities. One overriding question is “When has a Commercial Services producer done enough?” This question may be particularly difficult to address when considering the wide range of agencies that may be involved in a threat situation. Other organizations, such as public health departments, law enforcement agencies, and federal agencies such as the Federal Communications Commission, the Environmental Protection Agency, the Defense Health Agency, the Department of Energy, the Centers for Disease Control, and the Department of Transportation, will each have unique obligations or interests in responding to a severe release or explosion threat.

### **When is Enough, Enough?**

The guiding principle for responding to severe release or explosion threats is one of “due diligence” or “what is a suitable and sensible response to a threat?” As discussed above, some response to CS sector failures is warranted due to the public health implications of an actual dangerous incident.

Ultimately, the answer to the question of “due diligence” must be decided at the local level and will depend on a number of considerations. Among other factors, local authorities must decide what level of risk is reasonable in the context of a perceived threat. Careful planning is essential to developing an appropriate response to terrorist threats, and in fact, one primary objective of USEPA’s *Response Protocol Tool Boxes* (RPTBs) is to aid users in the development of their own site-specific plans that are consistent with the needs and responsibilities of the user. Beyond planning, the RPTB considers a careful evaluation of any terrorist threat, and an appropriate response based on the evaluation, to be the most important element of due diligence.

In the RPTB, the threat management process is considered in three successive stages: “possible,” “credible,” and “confirmed.” Thus, as the threat escalates through these three states, the actions that might be considered due diligence expand accordingly. The following paragraphs describe, in general terms, actions that might be considered as due diligence at these various stages.

- Stage 1: “Is the threat possible?” If a CS facility is faced with a terrorism threat, they should evaluate the available information to determine whether or not the threat is “possible” (i.e., could something have actually happened). If the threat is “possible,” immediate operational response actions might be implemented, and activities such as site characterization would be initiated to collect additional information to support the next stage of the threat evaluation.
- Stage 2: “Is the threat credible?” Once a threat is considered “possible,” additional information will be necessary to determine if the threat is “credible.” The threshold at the credible stage is higher than that at the possible stage, and in general there must be information to corroborate the threat in order for it to be considered “credible.”
- Stage 3: “Has the incident been confirmed?” Confirmation implies that definitive evidence and information have been collected to establish the presence of a threat to the CS sector. Obviously, at this stage the concept of due diligence takes on a whole new meaning since authorities are now faced with death and destruction and a potential public health crisis. Response actions at this point include all steps necessary to protect public health, property, and the environment.

## PREPARATION

CS sector facility managers and employees must know their facilities. For these persons, there is no excuse for not knowing every square inch of the facility site. In particular, workers should know about any and all construction activities underway on the site; the actual construction parameters of the facility; and especially operation of all transactional unit processes. In addition, management must not only know their operating staff but also know their customers.

### Construction and Operation

Each CS sector facility is unique with respect to age, operation, and complexity. This is important, particularly in evaluating the potential of a commercial service failure or malicious action causing a commercial service failure.

### Personnel

CS sector employees are generally its most valuable asset in preparing for and responding to threats and incidents. They have knowledge of the system and potential problem areas. The importance of knowledgeable and experienced

personnel is highlighted by the complexity of most commercial financial service systems. This complexity makes a specific terrorist target contingent upon detailed knowledge of the system configuration and usage patterns. If perpetrators have somehow gained a sophisticated understanding of a CS communications network system, the day-to-day experience of network production will prove an invaluable tool to countering any attacks. For instance, personnel may continually look for unusual aspects of daily operation that might be interpreted as a potential threat warning, and may also be aware of specific characteristics of the system that make it vulnerable to malware attacks or worse.

## **Customers**

A customer's knowledge of CS availability, functionality, and delivery is an important component of preventing and managing system intrusion incidents. Prevention is based largely on understanding potential types of malware attacks and the type of target facility. Steps taken to protect the customer's financial services tie-ins and in addition its employees and property, such as enhancements to the physical security of the sender's and receiver's financial services systems, may deter the attack itself.

CS customers vary significantly with regard to their expectations of what constitutes acceptable service, so it is necessary to consider the manner in which CS sector services are used in a particular system. Planning, preparation, and allocation of CS resources should be directed toward protecting the public at large, beyond specific demographic groups or individual users.

## **Perform Training and Desk/Field Exercises**

In addition to a lack of planning, another reason that emergency response plans fail is lack of training and practice. Training provides the necessary means for everyone involved to acquire the skills to fulfill their role during an emergency. It may also provide important "buy-in" to the response process from both management and staff, which is essential to the success of any response plan. Desk exercise (also known as "tabletops" or "sand lot" or "dry runs") along with field exercises allow participants to practice their skills. Also, these exercises will provide a test of the CS security plan itself, revealing strengths and weakness that may be used to improve the overall plan.

### *Enhance Physical Security*

Where possible deny physical access to non-pedestrian sites; within the CS sector system this may act as a deterrent to a perpetrator. When we consider

that many of the CS sector backup support units such as power generating and tower transmission systems are often in remote, wide-open spaces, this can be a huge challenge. Terrorists often seek the easiest route of attack, just like a burglar prefers a house with an open window or an open automobile with keys in the ignition. Aside from deterring actual attacks, enhancing physical security has other benefits. For example, security cameras can be used to review security breaches and determine if the incident was simply due to trespassing or is a potential contamination threat. The costs of enhancing physical security may be justified by comparison to the cost of responding to just one “credible” munitions explosion or contamination threat involving site characterization and lab analysis for potential contaminants.

### THE BOTTOM LINE

This chapter has emphasized the importance of ensuring the physical security of CS sector facilities and equipment. But it is important to point out that true CS sector security goes beyond the physical plant; the sector requires security of a different kind. This is the case of course because commercial service facilities are wide-open, soft targets that can be accessed by just about anyone. Placing a fence, barricades, and locking systems around a Wal-Mart or a sports stadium to prevent entry makes little sense when the purpose of these facilities, and other like facilities, is to provide convenient access for customers. However, cyber security is a different matter; much of the CS infrastructure, including control architecture, is vulnerable to cyberattack from either inside or outside of the network. The fact is that perhaps the largest vulnerability and dependency of the CS infrastructure as well as the infrastructure for other sectors is on cyber security. The control of CS networks and all of its functional components are vulnerable to various degrees of cyberattacks on the software operating systems by either the idle hacker or the more malicious intruder participating in information warfare. This is also true of all the networks within others sectors. The bottom line, the networks must be protected and guard from attack.

### REFERENCES AND RECOMMENDED READING

- Department of Homeland Security (DHS). “National Infrastructure Protection Plan.” <https://www.dhs.gov/cisa/national-infrastructure-protection-plan>.
- Department of Homeland Security (DHS). “The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.” [https://www.dhs.gov/xlibrary/assets/Physical\\_Strategy.pdf](https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf).

- Department of Homeland Security (DHS). “Homeland Security Directive 7: Critical Infrastructure Identification, Prioritization, and Protection.” <https://www.dhs.gov/homeland-security-presidential-directive-7>.
- Department of Homeland Security (DHS). 2015. *Commercial Facilities Sector—Specific Plan*. Washington, DC: U.S. Department of Homeland Security. <https://www.dhs.gov/publication/nipp-ssp-commercial-facilities-2015>.
- Henry, K. 2002. “New Face of Security.” *Gov. Security*, pp. 30–37.
- United States Environmental Protection Agency (U.S. EPA). 2004. “Response Protocol Toolbox: Planning for and Responding to Drinking Water Contamination Threats and Incidents.” Washington, DC.
- United States Environmental Protection Agency (U.S. EPA). 2011. “Response Protocol Toolbox: Planning for and Responding to Wastewater Contamination Threats and Incidents.” Washington, DC.

## Chapter 8

# Cybersecurity

What will you do when you are hacked?

What will you do when the power goes out?

Nobody has ever been killed by a cyberterrorist.

Unless people are injured, there is also less drama and emotional appeal.

—Dorothy Denning

Cyber criminals can significantly threaten the finances and reputations of US businesses and financial institutions. Given the abundance of potential victims and profits, cyber criminals will likely continue to target these entities.

—Gordon M. Snow, FBI

### INTRODUCTION

On April 23, 2000, police in Queensland, Australia, stopped a car on the road and found a stolen computer and radio inside. Using commercially available technology, a disgruntled former employee had turned his vehicle into a pirate command center of sewage treatment along Australia's Sunshine Coast. The former employee's arrest solved a mystery that had troubled the Maroochy Shire wastewater system for two months. Somehow the system was leaking hundreds of thousands of gallons of putrid sewage into parks, rivers, and the manicured grounds of a Hyatt Regency hotel—marine life died, the creek water turned black, and the stench was unbearable for residents. Until the former employee's capture—during his 46th successful intrusion—the utility's managers did not know why.

Specialists study this case of cyberterrorism because, at the time, it was the only one known in which someone used a digital control system deliberately to cause harm. The former employee's intrusion shows how easy it is to break in—and how restrained he was with his power.

To sabotage the system, the former employee set the software on his laptop to identify itself as a pumping station, and then suppressed all alarms. The former employee was the “central control station” during his intrusions, with unlimited command of 300 SCADA nodes governing sewage and drinking water alike.

The bottom line: as serious as the former employee's intrusions were they pale in comparison with what he could have done to the fresh water system—he could have done anything he liked.

—Barton Gellman, 2002

Other reports of cyber exploits illustrate the debilitating effects such attacks can have on the nation's security, economy, and on public health and safety. Here are just a few:

- In May 2015, media sources reported that data belonging to 1.1 million health insurance customers in the Washington, D.C., area were stolen in a cyberattack on a private insurance company. Attackers accessed a database containing names, birth dates, e-mail addresses, and subscriber ID numbers of customers.
- In December 2014, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT; works to reduce risks within and across all critical infrastructure sectors by partnering with law enforce agencies) issued an updated alert on a sophisticated malware camping compromising numerous industrial control system environments. Their analysis indicated that this campaign had been ongoing since at least 2011.
- In the January 2014 to April 2014 release of its monitor report, ICS-CERT reported that a public utility had been compromised when a sophisticated threat actor gained unauthorized access to its control system network through a vulnerable remote access capability configured on the system. The incident highlighted the need to evaluate security controls employed at the perimeter and ensure that potential intrusion vectors are configured with appropriate security controls and monitoring and detection capabilities.

**IN THE WORDS OF MASTER SUN TZU  
FROM “THE ART OF WAR”**

Those who are first on the battlefield and await the opponents are at ease;  
those who are last and head into battle are worn out.

- In December 2016, a Wisconsin couple was charged after the duo allegedly defrauded Enterprise Credit Union in Brookfield out of more than \$300,000, after one of the defendants, who managed the bank’s accounts, had her co-conspirator cash bank checks worth \$980 several times each week beginning in May 2015. The charges allege that the couple used the money to buy drugs.

In 2000, the FBI identified and listed threats to critical infrastructure. These threats are listed and described in table 8.1. In 2015, the GAO described the sources of cyber-based threats. These threats are listed and described in detail in table 8.2.

**Table 8.1 Threats to Critical Infrastructure Observed by the FBI**

<i>Threat</i>	<i>Description</i>
Criminal groups	There is an increased use of cyber intrusions by criminal group who attack systems for purposes of monetary gain.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities.
Hackers	Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use.
Hacktivism	Hacktivism refers to politically motivated attacks on publicly accessible web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into websites to send a political message.
Information warfare	Several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that, according to the Director of Central Intelligence, can affect the daily lives of Americans across the country.
Inside threat	The disgruntled organization insider is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors.
Virus writers	Virus writers are posing an increasingly serious threat. Several destructive computer viruses and “worms” have harmed files and hard drives, including the Melissa Macro Virus, the Explore. Zip worm, the CIH (Chernobyl) Virus, Nimda, and Code Red.

Source: FBI, 2000; 2014.



**Table 8.2 Common Cyber Threat Sources**

<i>Source</i>	<i>Description</i>
<i>Non-adversarial-malicious</i>	
Failure in information technology equipment	Failures in displays, sensors, controllers, and information technology hardware responsible for data storage, processing, and communications
Failure in environmental controls	Failures in temperature/humidity controllers or power supplies
Software coding errors	Failures in operating systems, networking, and general purpose and mission-specific applications
Natural or man-made disaster	Events beyond an entity's control such as fires, floods/tsunamis, tornadoes, hurricanes, and earthquakes
Unusual or natural event	Natural events beyond the entity's control that are not considered to be disasters (e.g., sunspots)
Infrastructure failure or outage	Failure or outage of telecommunications or electrical power
Unintentional user errors	Failures resulting from erroneous, accidental actions taken by individuals (both system users and administrators) in the course of executing their everyday responsibilities
<i>Adversarial</i>	
Hackers or hacktivists	Hackers break networks for the challenge, revenge, stalking, or monetary gain, among other reasons. Hacktivists are ideologically motivated actors who use cyber exploits to further political goals
Malicious insiders	Insiders (e.g., disgruntled organization employees, including contractors) may not need a great deal of knowledge about computer intrusions because their position with the organization often allows them to gain unrestricted access and cause damage to the target system or to steal system data. These individuals engage in purely malicious activities and should not be confused with non-malicious insider accidents
Nations	Nations, including nation-state, state-sponsored, and state-sanctioned programs use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities
Criminal groups and organize crime	Criminal groups seek to attack systems for monetary gain. Specifically, organized criminal groups use cyber exploits to commit identity theft, online fraud, and computer extortion
Terrorist	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence
Unknown malicious outsiders	Unknown malicious outsiders are threat sources or agents that, due to a lack of information, agencies are unable to classify as being one of the five types of threat sources or agents listed above

Source: GAO analysis of unclassified government and nongovernmental data. GAO 16-79.

## DID YOU KNOW?

Presidential Policy Directive 21 defined “All hazards” as a threat to an incident natural or man-made that warrants action to protect life, property, the environment, and public health or safety, and to minimize disruptions of government, social, or economic activities.

Threats to systems supporting critical infrastructure are evolving and growing. As shown in table 8.2, cyber threats can be unintentional or intentional. Unintentional or non-adversarial threats include equipment failures, software coding errors, and the actions of poorly trained employees. They also include natural disasters and failures of critical infrastructure on which the organization depends but are outside of its control. Intentional threats include both targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled employees, foreign nation engaged in espionage and information warfare, and terrorists. These threat adversaries vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include seeking monetary gain or seeking an economic, political or military advantage (GAO, 2015).

## CYBERSPACE

Today’s developing “information age” technology has intensified the importance of critical infrastructure protection, in which cyber security has become as critical as physical security to protecting virtually all critical infrastructure sectors. The DOD determined that cyber threats to contractors’ unclassified information systems represented an unacceptable risk of compromise to DOD information and posed a significant risk to U.S. national security and economic security interests.

In the past few years, especially since 9/11, it has been somewhat routine for us to pick up a newspaper, magazine, or view a television news program where a major topic of discussion is cyber security or the lack thereof. For example, recently there has been discussion about Russian hackers trying to influence the U.S. 2016 elections. Many of the cyber intrusion incidents we read or hear about have added new terms or new uses for old terms to our vocabulary. For example, old terms such as Botnets (short for robot networks, also balled bots, zombies, botnet fleets, and many others) are groups of computers that have been compromised with malware such as Trojan horses, worms, backdoors, remote control software, and viruses that have taken on new connotations in regard to cyber security issues. Relatively new terms such as scanners, Windows NT

hacking tools, ICQ hacking tools, mail bombs, sniffer, logic bomb, nukers, dots, backdoor Trojan, key loggers, hackers' Swiss knife, password crackers, blended threats, Warhol Worms, Flash Threats, Targeted Attacks, and BIOS crackers are now commonly read or heard. New terms have evolved along with various control mechanisms. For example, because many control systems are vulnerable to attacks of varying degrees, these attack attempts range from telephone line sweeps (wardialing), to wireless network sniffing (wardriving), to physical network port scanning, and to physical monitoring and intrusion. When wireless network sniffing is performed at (or near) the target point by a pedestrian (warwalking), meaning that instead of a person being in an automotive vehicle, the potential intruder may be sniffing the network for weaknesses or vulnerabilities on foot, posing as a person walking, but they may have a handheld PDA device or laptop computer (Warwalking, 2003). Further, adversaries can leverage common computer software programs, such as Adobe Acrobat and Microsoft Office, to deliver a threat by embedding exploits within software files that can be activated when a user opens a file within its corresponding program. Finally, the communications infrastructure and the utilities are extremely dependent on the IT sector. This dependency is due to the reliance of the communications systems on the software that runs the control mechanism of the operations systems, the management software, the billing software, and any number of other software packages is used by industry. Table 8.3 provides descriptions of common exploits or techniques, tactics, and practices used by cyber adversaries.

Not all relatively new and universally recognizable cyber terms have sinister connotation or meaning, of course. Consider, for example, the following digital terms backup, binary, bit byte, CD-ROM, CPU, database, e-mail, HTML, icon, memory, cyberspace, modem, monitor, network, RAM, Wi-Fi (wireless fidelity), record, software, World Wide Web—none of these terms normally generate thoughts of terrorism in most of us.

## THE BOTTOM LINE

U.S. Department of Homeland Security, in collaboration with the CS sector stakeholders, identified cyber risk as significant to the sector. Specifically, the 2010 financial and CS sector-specific plan stated that all of the sector's services rely on its cyber infrastructure, which necessitates that cybersecurity be factored into all of the sector's critical infrastructure protection activities. In addition, as a highly regulated sector, the CS sector has been required to undergo risk assessments by financial regulators to satisfy regulatory requirements.

**Table 8.3 Common Methods of Cyber Exploits**

<i>Exploit</i>	<i>Description</i>
Watering hole	A method by which threat actors exploit the vulnerabilities of carefully selected websites frequented by users of the targeted system. Malware is then injected to the targeted system via the compromised websites.
Phishing and spear phishing	A digital form of social engineering that uses authentic-looking e-mails, websites, or instant messages to get users to download malware, open malicious attachments, or open links that direct them to a website that requires information or executes malicious code.
Credentials based	An exploit that takes advantage of a system's insufficient user authentication and/or any elements of cyber-security supporting it, to include not limiting the number of failed login attempts, the use of hard-coded credentials, and the use of a broken or risky cryptographic algorithm.
Trusted third parties	An exploit that takes advantage of the security vulnerabilities of trusted third parties to gain access to an otherwise secure system.
Classic buffer overflow	An exploit that involves the intentional transmission of more data than a program's input buffer can hold, leading to the deletion of critical data and subsequent execution of malicious code.
Cryptographic weakness	An exploit that takes advantage of a network employing insufficient encryption when either storing or transmitting data, enabling adversaries to read and/or modify the data stream.
Unintentional user errors	Failures resulting from erroneous, accidental actions taken by individuals (both system users and administrators) in the course of executing their everyday responsibilities
Structured Query Language (SQL) Injection	An exploit that involves the alteration of a database search in a web-based application, which can be used to obtain unauthorized access to sensitive information in a database, resulting in data loss at corruption, denial of service, or complete host takeover.
Operating system command injection	An exploit that takes advantage of a system's inability to properly neutralize special elements used in operating system commands, allowing the adversaries to execute unexpected commands on the system by either modifying already evoked commands or evoking their own.
Cross-site scripting	An exploit that uses third-party web resources to run lines of programming code (referred to as scripts) within the victim's web browser or scriptable application. This occurs when a user, using a browser, visits a malicious website or clicks a malicious link. The most dangerous consequences can occur when this method is used to exploit additional vulnerabilities that may permit an adversary to steal cookies (data exchanged between a web server and a browser), log keystrokes, capture screen shots, discover and collect network information, or remotely access and control the victim's machine.

*(Continued)*

**Table 8.3 Common Methods of Cyber Exploits—Continued**

<i>Exploit</i>	<i>Description</i>
Cross-site request forgery	An exploit takes advantage of an application that cannot, or does not, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request, tricking the victim into executing a falsified request that results in the system or data being compromised.
Path traversal	An exploit that seeks to gain access to files outside of a restricted directory by modifying the directory pathname in an application that does not properly neutralize special elements (e.g., <code>'..'</code> , <code>'/'</code> , <code>'..\'</code> , etc.)
Integer overflow	An exploit where malicious code is inserted that leads to unexpected integer overflow, or wraparound, which can be used by adversaries to control looping or make security decisions in order to cause program crashes, memory corruption, or the execution of arbitrary code via buffer overflow.
Uncontrolled format string	An exploit where the victim is tricked into selecting a URL (website location) that has been modified to direct them to an external, malicious site which may contain malware that can compromise the victim's machine.
Heap-based buffer overflow	Similar to classic buffer overflow, but the buffer that is overwritten is allocated in the heap portion of memory, generally meaning that the buffer was allocated using a memory allocation routine, such as <code>"malloc ()"</code> .
Unrestricted upload of files	An exploit that takes advantage of insufficient upload restrictions, enabling adversaries to upload malware (e.g., <code>.php</code> ) in place of the intended file type (e.g., <code>.jpg</code> ).
Inclusion of functionality from un-trusted sphere	An exploit that uses trusted, third-party executable functionality (e.g., web widget or library) as a means of executing malicious code in software whose protection mechanism are unable to determine whether functionality is from a trusted source, modified in transit, or being spoofed.
Certificate and certificate authority compromise	Exploits facilitated via the issuance of fraudulent digital certificates (e.g., transport layer security and Secure Socket Layer). Adversaries use these certificates to establish secure connections with the target organization or individual by mimicking a trusted third party.
Hybrid of others	An exploit which combines elements of two or more of the aforementioned techniques.

Source: GAO, (2015).

## REFERENCES AND RECOMMENDED READING.

Department of Energy. 2001. "21 Steps to Improve Cyber Security of SCADA Networks." Washington, DC. [https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21\\_Steps\\_-\\_SCADA.pdf](https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf).

- Department of Homeland Security (DHS). 2009. "National Infrastructure Protection Plan." <https://www.dhs.gov/cisa/national-infrastructure-protection-plan>.
- Department of Homeland Security (DHS). "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets." [https://www.dhs.gov/xlibrary/assets/Physical\\_Strategy.pdf](https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf).
- Department of Homeland Security (DHS). 2013. "Homeland Security Directive 7: Critical Infrastructure Identification, Prioritization, and Protection." <https://www.dhs.gov/homeland-security-presidential-directive-7>.
- Department of Homeland Security (DHS). 2015. "Commercial Facilities Sector—Specific Plan." Washington, DC.
- Federal Emergency Management Agency (FEMA). 2008. "FEMA452: Risk Assessment A How to Guide." <https://www.fema.gov/fema-452-risk-assessment-how-guide-mitigate-potential-terrorist-attacks-against-buildings>.
- Federal Emergency Management Agency (FEMA). 2015. "Protecting Critical Infrastructure Against Insider Threats." <https://training.fema.gov/is/courseoverview.aspx?code=is-915>.
- Federal Bureau of Investigation (FBI). 2000. "Threat to Critical Infrastructure." Washington, DC.
- Federal Bureau of Investigation (FBI). 2007. "Ninth Annual Computer Crime and Security Survey." Washington, DC.
- Federal Bureau of Investigation (FBI). 2014. "Protecting Critical Infrastructure and the Importance of Partnerships." <https://www.fbi.gov/news/speeches/protecting-critical-infrastructure-and-the-importance-of-partnerships>.
- Government Accountability Office (GAO). 2015. "Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress." <https://www.gao.gov/assets/680/673779.pdf>.
- Minter, J.G. September 1996. "Prevention Chemical Accidents Still A Challenge." *Occupational Hazards*.
- National Infrastructure Protection Center (NIPC). 2002. *Cybersecurity*. Washington, DC.
- Spellman, F.R. 1997. *A Guide to Compliance for PSM/RMP*. Lancaster, PA: Technomic Publishing Company.
- Stamp, J. et al. 2003. *Common Vulnerabilities in Critical Infrastructure Control Systems*. 2nd Edition. Sandia National Laboratories.
- United States Department of Energy. 2002. "Vulnerability Assessment Methodology: Electric Power Infrastructure." Washington, DC.
- United States Environmental Protection Agency (EPA). 2005. "EPA Needs to Determine What Barriers Prevent Water Systems from Securing Known SCADA Vulnerabilities." Report Number: 2005-P-00002. Washington, DC.



## Chapter 9

# Emergency Response

We're in uncharted territory.

—Rudi Giuliani (9/11/01)

When New York mayor Rudi Giuliani made the above statement to Police Commissioner Bernard Kerik at the World Trade Center Site, September 11, 2001, to a point and to a degree, one of the first (and not to be forgotten) gross understatements of the twenty-first century had been uttered. Indeed, for citizens of the United States, the 9/11 events placed our level of consciousness, awareness, fear, and questions of what to do next in “uncharted territory.” Actually, when you get right down to it, 9/11 generated more questions than anything else. Many are still asking the following questions today:

Why?

Why would anyone have the audacity to attack the United States?

What kind of cold-blooded killers would even think of conducting such an event?

Who were those Islamic radicals who perpetrated 9/11?

What were the terrorists' goal(s)?

Why?

Why were we not ready for such an attack?

Why had we not foreseen such an event?

Why were our emergency responders so undermanned, ill-prepared, and ill-equipped to handle such a disaster?

What took the military fighter planes so long to respond?

What did our government really know (if anything) before the events occurred?



Could anyone have prevented it?

Bottom line questions: Why us? Hell, why anyone?

Why?

These and several other questions continue to resonate today; no doubt they will continue to haunt us for some time to come.

Maybe we ask post-9/11-related questions because of who we are, what we are, and what we are not. That is, because we are Americans we are free, uninhibited thinkers who think what we say and say what we think—isn't America great! Most Americans are softhearted and sympathetic to those in need—compassion is the very nature and soul of being American. Americans are not born terrorists; they are not born into a terrorist regime; they are not raised with fear in their hearts—they are not afraid every time they leave their homes and go about their daily business. Suicide bombers and other like terrorists are those that occupy some other faraway place; definitely not America, and they are definitely not American. Right?

Notwithstanding exceptions to the rule, such as Timothy McVeigh (a so-called red-blooded American, born and raised in America) and that other idiot (whether a national or foreigner) who mailed the anthrax, terrorism was foreign to us.

Today, from a safety/security point of view, based on the events of 9/11 and the anthrax events, we should no longer be asking why. Instead, we should not waste our time, money, and energy asking why or in pointing a finger of blame at our government, military, 9/11 emergency responders, and/or the terrorists. We should stop asking why and shift our mindset to asking what-if. The point is we need to stop feeling sorry for ourselves and except the fact that there are folks out there who do not share our view of the American way of life. Earlier, in regard to security preparedness, we pointed to the need to ask what-if questions. Simply, what-if analysis is a proactive approach used to prevent or mitigate certain disasters, extreme events—those human- or nature-generated. Obviously, asking and properly answering what-if questions has little effect on preventing the actions of Mother Nature, such as earthquakes, tornadoes, hurricanes (Katrina-type events), and others. On the other hand, it is true that what-if questions, when properly posed and answered (with results), can reduce the death toll and overall damage caused by these natural disasters. We are certainly aware that these natural events are possible, probable, and likely, and their effects can be horrendous—beyond tragic. The irony is apparent, however, especially when we ask: how many of us are actually willing to move away from or out of earthquake zones, hurricane and tornado allies, and floodplains to live somewhere else?

The fact is we do not possess a crystal ball to foretell the future. What-if questions prepare us to react and respond to certain contingencies. And we

must respond, because there are certain events we simply can't prevent. The best response to an event we can't prevent is summed up by the Boy Scouts Motto: Be Prepared!

## CS SECTOR CONTINGENCY PLANNING

Emergency response planning or contingency planning for extreme events has long been standard practice for emergency planners and safety professionals in industrial systems operations. For many years, prudent practices have required consideration of the potential impact of severe natural events (forces of nature), including earthquakes, tornadoes, volcanoes, floods, hurricanes, and blizzards. These possibilities have been included in CS sector industry infrastructure emergency preparedness and disaster response planning. In addition, many CS sector production and cyber distribution facilities have considered the potential consequences of man-caused disasters such as operator error and manufacturer's industrial equipment defects. Currently, CS sector managers and operators must also consider violence in the workplace. Moreover, at present, as this text has pointed out, there is a new focus of concern: the potential effects of intentional acts by domestic (home-grown—in-house) or international (foreign) terrorists.

As a result, the security paradigm has not necessarily changed but instead has been radically adjusted—reasonable, necessary, and sensible accommodation for and mitigation of just about any emergency situation imaginable have been and continue to be made. Because we cannot foresee all future domestic or intentional acts of terrorism, we must be prepared to shift from the proactive to reactive mode on short notice—in some cases, on very short notice. Accordingly, we must be prepared to respond to, react to, and mitigate what we can't prevent. Unfortunately, there is more we can't prevent than we can prevent. In light of this, in this section we present in outline form a reactive mitigation procedure, the template example for a standard CS sector Crisis Communications Plan (CCP), dealing with natural and man-caused disasters, which could also be applied in response to acts of terrorism.

## CRISIS COMMUNICATIONS PLAN

*Note:* The following criteria have not been established as anything other than guidelines and are offered not as definitive or official regulations or procedures but rather as informed advice (based on more than thirty years of safety, industrial hygiene, emergency contingency planning, and security experience) insofar as to the subject matter specific to both public and private sectors.

*Note:* This emergency action plan applies to locations and facilities that are occupied by CS sector personnel performing their designated work activities.

The fact is well known: When an emergency occurs, the need to communicate is immediate. The goals of a CCP are to document and understand the steps needed to:

- rapidly restore CS processing activities after an emergency;
- minimize CS sector equipment damage;
- minimize impact and loss to customers;
- minimize negative impacts on public health and employee safety;
- minimize adverse effects on the environment;
- provide emergency public information concerning customer service.

Although we are concerned with the CS sector in this text, the USEPA developed *Large Water System Emergency Response Outline: Guidance to Assist Community Water Systems in Complying with the Public Health and Bioterrorism Preparedness and Response Act of 2002* (dated July 2003), with minor adjustments, can be applied as a template for any critical infrastructure sector, including the financial services sector. This template provides guidance and recommendations to aid facilities in the preparation of emergency response plans under the PL 107–188. The template is provided below.

## CCP Template

### I. Introduction

Safe and reliable operation is vital to every industrial operation. CCP is an essential part of managing a CS sector process or entity. The introduction should identify the requirement to have a documented CCP, the goal(s) of the plan (e.g., be able to quickly identify an emergency and initiate timely and effective response action, be able to quickly respond and repair damages to minimize system downtime), and how access to the plan is limited. Plans should be numbered for control. Recipients should sign and date a statement that includes (1) their CCP number, (2) their agreement not to reproduce the CCP, and (3) they have read the CCP.

CCPs do not necessarily need to be one document. They may consist of an overview document, individual Emergency Action Procedures, check lists, additions to existing operations manuals, appendices, and so on. There may be separate, more detailed plans for specific incidents. There may be plans that do not include particularly sensitive information and those that do. Existing applicable documents should be referenced in the CCP.

## II. Emergency Planning Process

### A. Planning Partnerships

The planning process should include those parties who will need to help the CS sector in an emergency situation (e.g., first responders, law enforcement, public health officials, nearby utilities, local emergency planning committees, testing labs). Partnerships should track from the CS sector operation up through local, state, regional, and federal agencies, as applicable and appropriate, and could also document, compliance with governmental requirements.

### B. General Emergency Response Policies, Procedures, Actions, Documents

A short synopsis of the overall emergency management structure, how other industrial emergency response, contingency, and risk management plans fit into the Crisis Communication Plan for CS sector emergencies, and applicable policies, procedures, actions plans, and reference documents should be cited. Policies should include interconnect agreements with adjacent communities and just how the CCP may affect them.

### C. Scenarios

Use your VA findings to identify specific emergency action steps required for response, recovery, and remediation for applicable incident types. In Section V of this plan, specific emergency action procedures addressing each of the incident types should be addressed.

## III. Emergency Response Plan and Policies

### A. System-Specific Information

In an emergency, CS sector industries need to have basic information for system personnel and external parties such as law enforcement, emergency responders, repair contractors/vendors, the media, and others. The information needs to be clearly formatted and readily accessible so system staff can find and distribute it quickly to those who may be involved in responding to the emergency. Basic information that may be presented in the emergency response plan are the system's ID number, system name, system address or location, directions to the system, population served, number of service connections, system owner, and information about the person in charge of managing the emergency. Distribution maps, detailed plant drawings, site plans, source/storage/production energy locations, and operations manuals may be attached to this plan as appendices or referenced.

1. PWS ID, owner, contact person
2. Population served and service connections

3. System components
  - a) Conduits and constructed conveyances
  - b) Physical barriers
  - c) Electronic, computer, or other automated systems which are utilized by the CS sector
  - d) Emergency power generators (on-site and portable)
  - e) The operation and maintenance of such system components
- B. Chain-of-Command Chart Developed in Coordination with Local Emergency Planning Committee (Internal and/or External Emergency Responders, or Both)
  1. Contact name
  2. Organization and emergency response responsibility
  3. Telephone number(s) (hardwire, cell phones, faxes, e-mail)
  4. State Twenty-four-hour Emergency Communications Center Telephone
- C. Communications Procedures: Who, What, When

During most emergencies, it will be necessary to quickly notify a variety of parties both internal and external to the financial services sector entity. Using the Chain-of-Command Chart and all appropriate personnel from the lists below indicate who activates the plan, the order in which notification occurs, and the members of the Emergency Response Team. All contact information should be available for routine updating and readily available. The following lists are not intended to be all inclusive—they should be adapted to your specific needs.

1. Internal Notification Lists
  - a) Operations dispatch
  - b) CS sector manager
  - c) Data (IT) manager
  - d) Maintenance manager
  - e) Other
2. Local Notification
  - a) Head of local government (i.e., mayor, city manager, chairman of board)
  - b) Public safety officials—fire, local law enforcement (LLE), police, EMS, safety. If a malevolent act is suspected LLE should be immediately notified and in turn will notify the FBI, if required. The FBI is the primary agency for investigating sabotage
  - c) Other government entities: health, schools, parks, finance, electric, and so on

3. External Notification Lists
  - a) State Department of Environmental Quality (DEQ)
  - b) USEPA/USDOE/DHS/FCC
  - c) State police
  - d) State Health Department (lab)
  - e) Critical customers (special considerations for hospitals, federal, state, and country government centers, etc.).
  - f) Service aid
  - g) Mutual aid
  - h) Commercial customers not previously notified

4. Public/Media Notification: When and How to Communicate

Effective communications is a key element of emergency response, and a media or communications plan is essential to good communications. Be prepared by organizing basic facts about the crisis and your chemical system. Develop key messages to use with the media that are clear, brief, and accurate. Make sure your messages are carefully planned and have been coordinated with local and state officials. Considerations should be given to establishing protocols for both field and office staff to respectfully defer questions to the utility spokesperson.

Be prepared to list geographic boundaries of the affected area, (e.g., west of highway a, east of highway b, north of highway c, and south of highway d to ensure the public clearly understand the system boundaries.)

- E. Personnel Safety

This should provide direction as to how operations staff, emergency responders, and the public should respond to a potential toxic chemical release, including facility evacuation, personnel accountability, proper Personnel Protective Equipment as dictated by the Risk Management Program, and whether the nearby public should be “in-place sheltered” or evacuated.

- F. Equipment

The ERP should identify equipment that can obviate or significantly lessen the impact of terrorist attacks or other intentional actions on the public health and protect the safety and supply of communities and individuals. The CS sector facility should maintain an updated inventory of current equipment and repair parts for normal maintenance work.

Because of the potential for extensive or catastrophic damage that could result from a malevolent act, additional equipment sources should be identified for the acquisition and installation of equipment

and repair parts in excess of normal usage. A certain number of “long-lead” procurement equipment should be inventoried and the vendor information for such unique and critical equipment maintained. In addition, mutual aid agreements with other industries, and the equipment available under the agreement, should be addressed. Inventories of current equipment, repair parts, and associated vendors should be indicated.

#### G. Property Protection

A determination should be made as to what CS sector producing, processing, distribution operation/facility should be immediately “locked down,” specific access control procedures implemented, initial security perimeter established, a possible secondary malevolent event considered. The initial act may be a divisionary act.

#### H. Training, Exercises, and Drills

Emergency response training is essential. The purpose of the training program is to inform employees or what is expected of them during an emergency situation. The level of training on a CCP directly affects how well a financial services sector facility’s employees can respond to an emergency. This may take the form of orientation scenarios, tabletop workshops, functional exercises, and son.

#### I. Assessment

To evaluate the overall CCP’s effectiveness and to ensure that procedures and practices developed under the CCP are adequate and are being implemented, CS sector industry staff should audit the program on a periodic basis.

### IV. Emergency Action Procedures

These are detailed procedures used in the event of an operation emergency or malevolent act. Emergency Action Procedures (EAPs) may be applicable across many different emergencies and are typically common core elements of the overall municipality Emergency Response Plan (ERP) (responsibilities, notifications lists, security procedures, etc.) and can be referenced.

- A. Event classification/severity of emergency
- B. Responsibilities of emergency director
- C. Responsibilities of incident commander
- D. Emergency Operations Center (EOC) activation
- E. Division internal communications and reporting
- F. External communications and notifications
- G. Emergency telephone list (division internal contacts)
- H. Emergency telephone list (off-site responders, agencies, state twenty-four-hour emergency phone number, and others to be notified)
- I. Mutual aid agreements

- J. Contact list of available emergency contractor services/equipment
- K. Emergency equipment list (including inventory for each facility)
- L. Security and access control during emergencies
- M. Facility evacuation and lockdown and personnel accountability
- N. Treatment and transport of injured personnel (including electrocution and petrochemical exposure)
- O. Petrochemical records—to compare against historical results for base line
- P. List of available labs for emergency use
- Q. Emergency sampling and analysis (petrochemical)
- R. Water use restrictions during emergencies
- S. Alternate temporary chemical supplies during emergencies
- T. Isolation plans for chemical supply, treatment, storage, and distribution systems
- U. Mitigation plans for neutralizing, flushing, and collecting spilled chemicals
- V. Protection of vital records during emergencies
- W. Record keeping and reporting (FCC, FEMA, DHS, DOT, OSHA, EPA, and other requirements) (it is important to maintain accurate financial records of expenses associated with the emergency event for possible federal reimbursement.)
- X. Emergency program training, drills/and tabletop exercises
- Y. Assessment of emergency management plan and procedures
- Z. Crime scene preservation training and plans
- AA. Communication plans:
  - 1. Police
  - 2. Fire
  - 3. Local government
  - 4. Media
  - 5. And so forth
- BB. Administration and logistics, including EOC, when established
- CC. Equipment needs/maintenance of equipment
- DD. Recovery and restoration of operations
- EE. Emergency event closeout and recovery
- V. Incident-Specific EAPs
  - Incident-specific EAPs are action procedures that identify specific steps in responding to an operational emergency of malevolent act.
  - A. General response to terrorist threats (other than bomb threat and incident-specific threats)
  - B. Incident-specific response to man-made or technological emergencies
    - 1. Contamination event (articulated threat with unspecified materials)



2. Contamination threat at a major event
  3. Notification from health officials of potential contamination
  4. Intrusion through SCADA
- C. Significant structural damage resulting from intentional act
  - D. Customer complaints
  - E. Severe weather response (snow, ice, temperature, lightning)
  - F. Flood response
  - G. Hurricane and/or tornado response
  - H. Fire response
  - I. Explosion response
  - J. Major vehicle accident response
  - K. Electrical power outage response
  - L. Water supply interruption response
  - M. Transportation accident response—barge, plane, train, semi-trailer/  
tanker
  - N. Contaminated/tampered with water treatment chemicals
  - O. Earthquakes response
  - P. Disgruntled employees response (i.e., workplace violence)
  - Q. Vandals response
  - R. Bomb threat response
  - S. Civil disturbance/riot/strike
  - T. Armed intruder response
  - U. Suspicious mail handling and reporting
- VI. Next Steps
- A. Plan Review and Approval
  - B. Practice and Plan to Update (as necessary, once every year recommended)
    1. Training requirements
    2. Who is responsible for conducting training, exercises, and emergency drills?
    3. Update and assessment requirements
    4. Incident-specific requirements
- VII. Annexes
- A. Facility and Location Information
    1. Facility maps
    2. Facility drawings
    3. Facility descriptions/layout
    4. And so on
- VIII. References and Links
- A. Department of Homeland Security—<https://www.dhs.gov/>
  - B. Environmental Protection Agency—<https://www.epa.gov/>

- C. Federal Emergency Management Agency—<https://www.fema.gov/>
- D. Local Emergency Planning Committees—<https://www.epa.gov/epcra/local-emergency-planning-committees>

## THE BOTTOM LINE

Because industrial emergencies (in less than extreme conditions) can seriously affect the surrounding community and environment, and because poor planning and/or panic can only make a bad situation worse, and can also lead to additional injury and death, your role as CS sector manager in emergency response is doubly important. A crisis out of hand can easily devastate a community—and your organization is (or should be) an active member of your community. By ensuring less than effective emergency response, CS site managers endanger not only themselves and their organizations but also their organization's community and standing as well.

## REFERENCES AND RECOMMENDED READING

- Brauer, R. L. 1994. *Safety and Health for Engineers*. New York: Van Nostrand Reinhold.
- CoVan, J. 1995. *Safety Engineering*. New York: John Wiley and Sons.
- Department of Homeland Security (DHS). 2009. "National Infrastructure Protection Plan." <https://www.dhs.gov/cisa/national-infrastructure-protection-plan>.
- Department of Homeland Security (DHS). 2003. "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets." [https://www.dhs.gov/xlibrary/assets/Physical\\_Strategy.pdf](https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf).
- Department of Homeland Security (DHS). 2013. "Homeland Security Directive 7: Critical Infrastructure Identification, Prioritization, and Protection." <https://www.dhs.gov/homeland-security-presidential-directive-7>.
- Department of Homeland Security (DHS). 2015. "Commercial Facilities Sector—Specific Plan." Washington, DC. <https://www.dhs.gov/publication/nipp-ssp-commercial-facilities-2015>.
- Healy, R. J. 1969. *Emergency and Disaster Planning*. New York: Wiley.
- Office of the Federal Register. 29 *CFR 1910.120*. Washington, DC.
- Smith, A. J. 1980. *Managing Hazardous Substances Accidents*. New York: McGraw-Hill.
- Spellman, F. R. 1997. *A Guide to Compliance for Process Safety Management Planning (PSM/RMP)*. Lancaster, PA: Technomic Publishing Company.
- United States Army Corps of Engineers. *Safety and Health Requirements Manual, Revised Edition*. EM 385-1-1, Washington, DC October 1987.
- United States Department of Energy (DOE). 2008. "Emergency Support Function #12—Energy Annex." Washington, DC.

- United States Department of Energy (DOE). 2010. "Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan." Washington, DC.
- United States Environmental Protection Agency (U.S. EPA). 2002. "Water Utility Response, Recovery & Remediation Guidance for Man-made and/or Technological Emergencies." Washington, DC.
- United States Environmental Protection Agency (U.S. EPA). 2003. "Large Water System Emergency Response Plan Outline: Guidance to Assist Community Water Systems in Complying with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002." Washington, DC. <https://www.epa.gov/sites/production/files/2015-03/documents/erp-long-outline.pdf>.

## *Chapter 10*

# **Security Techniques and Hardware**

There are but two powers in the world, the sword and the mind. In the long run the sword is always beaten by the mind.

—Napoleon Bonaparte

If your facility still uses keyed locks, does anyone in your facility control those keys? Does anyone in your facility know who has the keys? Does anyone know how many keys have been issued? Is there a recorded record of each key that has been issued?

I know your password, therefore, you belong to me.

### **SHOPPING IN THE BRICK AND MOTAR STORE**

Whenever we walk into a mall, store, or other pedestrian entry CS entity, we usually pay little attention to our surroundings. Why? Well, we become used to the surroundings and the ambience through our continued usage of such a place or from the perusal such services. And, more than likely we are in a hurry, as usual, and surroundings are not that important to us; instead, the business at hand is much more important.

Let's say, on the other hand, we are part of that group of people who take it all in, no matter where or when. Well, if this is the case, when we walk into the store there are a few things that stand out to us. First it is usually busy, crowded, and hectic. The standard cashier greets as we stand to pay for whatever goods we have purchased. While the cashier totals our purchases we might glance to our right or left or above the place we are standing; there we would probably notice the CCTV security cameras here and there with some pointed right at us.

And we presume that the teller behind the teller window is in close proximity and easy reach of an alarm or panic button, which will sound the alarm and hopefully send security and the police scrambling to respond.

These security devices are obvious to us or at least we assume they are present. However, it is what we do not see, anticipate, expect, comprehend, or assume is present (or should be) that is really what the emphasis is about herein. Note that there are many devices and security systems that are available to protect CS sector assets not open to pedestrian traffic and fewer available to CS facilities that are open to pedestrian traffic (malls, stores, music halls, sports stadium, etc.). In locations where a variety of security devices are viable, many of are not readily visible to most people. However, again, keep in mind that some of the devices and security techniques discussed in the following are only viable in CS assets that are not open to pedestrian traffic.

### THE MULTIPLE BARRIER APPROACH

Ideally, in a perfect world, all CS sector physical sites/facilities/assets would be secured in a layered fashion (aka the multiple barrier approach). Layered security systems are vital. Using the protection “in-depth” principle, requiring that an adversary defeat several protective barriers or security layers to accomplish its goal, financial services sector physical infrastructure can be made more secure. Protection in depth is a term commonly used by the military to describe security measures that reinforce one another, masking the defense mechanisms from view of intruders, and allowing the defender time to respond to intrusion or attack.

A prime example of the use of the multi-barrier approach to ensure security and safety is demonstrated by the practices of the bottled water industry. In the aftermath of 9/11 and the increased emphasis on Homeland Security, a shifted paradigm of national security and vulnerability awareness has emerged. Recall that in the immediate aftermath of the 9/11 tragedies, emergency responders and others responded quickly and worked to exhaustion. In addition to the emergency responders, bottled water companies responded immediately by donating several million bottles of water to the crews at the crash sites in New York, at the Pentagon, and in Pennsylvania. International Bottled Water Association (IBWA, 2004) reports that “within hours of the first attack, bottled water was delivered where it mattered most; to emergency personnel on the scene who required ample water to stay hydrated as they worked to rescue victims and clean up debris” (p. 2).

Bottled water companies continued to provide bottled water to responders and rescuers at the 9/11 sites throughout the post-event(s) process(es). These patriotic actions by the bottled water companies, however, beg the

question: How do we ensure the safety and security of the bottled water provided to anyone? IBWA (2004) has the answer: Using a multi-barrier approach, along with other principles, will enhance the safety and security of bottled water. IBWA (2004) describes its multi-barrier approach as follows:

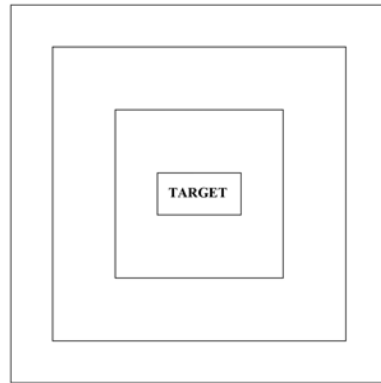
**A multi-barrier approach**—Bottled water products are produced utilizing a multi-barrier approach, from source to finished product, that helps prevent possible harmful contaminants (physical, chemical or microbiological) from adulterating the finished product as well as storage, production, and transportation equipment. Measures in a multi-barrier approach may include source protection, source monitoring, reverse osmosis, distillation, filtration, ozonation or ultraviolet (UV) light. Many of the steps in a multi-barrier system may be effective in safeguarding bottled water from microbiological and other contamination. Piping in and out of plants, as well as storage silos and water tankers are also protected and maintained through sanitation procedures. In addition, bottled water products are bottled in a controlled, sanitary environment to prevent contamination during the filling operation. (p. 3)

In CS sector infrastructure security, protection in depth is used to describe a layered security approach for not open to pedestrian traffic. A protection in depth strategy uses several forms of security techniques and/or devices against an intruder and does not rely on one single defensive mechanism to protect infrastructure. By implementing multiple layers of security, a hole or flaw in one layer is covered by the other layers. An intruder will have to intrude through each layer without being detected in the process—the layered approach implies that no matter how an intruder attempts to accomplish his goal, he will encounter effective elements of the physical protection system.

For example, as depicted in figure 10.1, an effective security layering approach requires that an adversary penetrate multiple, separate barriers to gain entry to a critical TARGET at a CS sector facility. As shown in figure 10.1, protection in depth (multiple layers of security) helps to ensure that the security system remains effective in the event of a failure or an intruder bypassing a single layer of security.

Again, as shown in figure 10.1, layered security starts with the outer perimeter (the fence—the first line of physical security) of the facility and goes inward to the facility, the buildings, structures, other individual assets, and finally to the contents of those buildings—the TARGETS.

The area between the outer perimeter and structures or buildings is known as the site. This open site area provides an incomparable opportunity for early identification of an unauthorized intruder and initiation of early warning/response. This open space area is commonly used to calculate the standoff distance; that is, it is the distance between the outside perimeter (public areas to the fence) to TARGET or critical assets (buildings/structures) inside the perimeter (inside the fence line—the restricted access area).



**Figure 10.1 Layered Approach to Security for Non-Pedestrian Traffic Commercial Facilities.**

The open area, between perimeter fence and target (e.g., operations center), if properly outfitted with various security devices, can also provide layered protection against intruders. For example, lighting is a deterrent. Based on personal experience, an open area within the plant site that is almost as well lighted at night as would be expected during daylight hours is the rule of thumb. In addition, strategically placed motion detectors along with crash barriers at perimeter gate openings and in front of vital structures are also recommended. Armed, mobile guards who roam the interior of the plant site on a regular basis provide the ultimate in site area security.

The next layer of physical security is the outside wall of the target structure(s) itself. Notwithstanding door, window, and/or skylight entry, walls prevent most intruders from easy entry. If doors can only be entered using card reader access, security is shored up or enhanced to an extent. The same can be said for windows and skylights that are fashioned small enough to prohibit normal human entry. These same “weak” spots in buildings can be bastioned with break-proof or reinforced security glass.

The final layer of security is provided by properly designed interior features of buildings. Examples of these types of features include internal doors and walls, equipment cages, and backup or redundant equipment.

In the preceding discussion, the conditions described referred to perfect world conditions; that is, to those conditions that we “would want” (i.e., the security manager’s proverbial wish list) to be incorporated into the design and installation of new financial services sector infrastructure. Post 9/11, in a not so perfect world, however, many of the peripheral (fence line) measures described above are more difficult to incorporate into financial services sector infrastructure. This is not to say that CS sector sites and facilities do not have fence lines or fences; many of them do. These fences are designed to

keep vandals, thieves, and trespassers out. The problem is not only the fact that many of these facilities were constructed several years ago before urban encroachment literally encircled the many sites, allowing, at present, little room for security stand backs or setbacks to be incorporated into electrical power stations, plants, and/or critical equipment locations. Based on personal observation, many of these fences face busy city streets or closely abut structures outside the fence line. The point is that when one sits down to plan a security upgrade, these factors must be taken into account.

The fly in the ointment for the CS sector assets is accessibility. People who use CS in person need to enter the facilities to conduct their business. Thus, the multiple barrier approach to security in a mall, for example, is unrealistic, at best.

Managers of CS sector infrastructure have four primary security areas to manage. These security areas are listed and described below.

- **Physical Security**—in the commercial sector, where practicable, physical security techniques and practices have the most effect at “fenced” locations. At such locations, a systems approach is best, where detection, assessment, communication, and response are planned and supported by resources, procedures, and policies.
- **Cyber/IT Security**—only the use of key operating systems that have been properly vetted and scrubbed of alleged Chinese and/or Russian Trojan horses hacked into the North American electrical grid is important. The only positive way to ensure the security of the North American Grid is to disconnect its cyber and other digital systems from the Internet. This step is impractical at the present time, but points to the need to conduct frequent audits of the system and install firewall protection in digital components and other systems to prevent hacking. Frequent third-party penetration testing is advised.
- **Employment Screening**—mitigates the threat from the enemy at the water cooler (inside the organization). We are always amazed whenever we conduct security audits for various companies. Often, a simple check such as reviewing an employee’s driving record often reveals that the employee has no license, is driving on a suspended license, or has a horrific driving record. Hiring standards and preemployment background investigations may help ensure the trustworthiness and reliability of personnel who have unescorted access to critical facilities.
- **Protecting Potentially Sensitive Information**—the old saying that goes—a secret can best be held between three people so long as two of the three are dead—makes the point that reducing the likelihood that information could be used by those intent on disrupting operations or causing death destruction in CS sector sites is crucial. Information should only be shared within an organization on a need-to-know basis only.



For existing facilities, security upgrades should be based on the results generated from the vulnerability assessment, which characterizes and prioritizes those assets that may be targeted. Those vulnerabilities identified must be protected.

In the following sections, various security hardware and/or devices are described. These devices serve the main purpose of providing security against physical and/or digital intrusion. That is, they are designed to delay and deny intrusion and are normally coupled with detection and assessment technology. Possible additional security measures, based on the vulnerability assessment that may be recommended (covered in this text), include the following (NAERC, 2002):

- Electronic security
- Closing nonessential perimeter and internal portals
- Physical barriers such as bollards or Jersey walls
- Fencing
- Lighting
- Security surveys
- Vulnerability assessments
- Availability of security resources
- General personnel and security officer training
- Law Enforcement Liaison
- Ensure availability of essential spare parts (machines, repair parts, wire, pipe, valves, transformers, etc.) for critical facilities

Keep in mind, however, and as mentioned previously, no matter the type of security device or system employed, financial services sector systems cannot be made immune to all possible intrusions or attacks. Whenever a facility safety/security manager tells us that he or she has secured their site 100 percent, we are reminded of Schneier's (2000) view of security: "You can't defend. You can't prevent. The only thing you can do is detect and respond." Simply, when it comes to making "anything" absolutely secure from intrusion or attack, there is inherently, or otherwise, no silver bullet."

In the next section, security hardware devices are discussed in detail. Before we describe these hardware devices, keep in mind that in addition to security hardware devices to help protect and monitor CS sector assets there are a few employee practices and actions that can be taken to protect CS assets. For example, when a commercial asset computer system fails and must be disposed of, how is it disposed of? Is there a procedure or practice in place to prevent the valuable information on the system's hard drive from being pulled from a trash heap or from a dumpster dive and used by potential enemies? Are shredders used? Are they state-of-the-art shredders that prevent scraps from being reassembled by enemies? Are building cleaning crews properly vetted and

supervised? Do you have a team that routinely inspects suspended ceilings for bugs, cameras, and listening recorders? Do you have key stroke reader capability; that is, can you record what messages are being sent by employees? Do you routinely check hardwired phone lines? Have you removed all door signs that tell anyone what is on the other side of the room? Have you trained your employees to be slightly suspicious of just about anything and everything? Have you opened your manholes lately to see what is inside?

All of these practices just mentioned do not require security hardware such as barriers, motion detectors, fences, locks, biometric systems, video cameras, armed guards, electrified fences. What they require instead is common sense, awareness, and alert and engaged supervisors and employees. The point is what is heard at the water cooler is sometimes more significant than any security alarm apparatus can provide.

Again, keep in mind that many of the security hardware devices described in the following are only applicable to non-pedestrian facilities only; we simply cannot barricade or fence in, for example, sports arenas and shopping malls.

## SECURITY HARDWARE DEVICES<sup>1</sup>

USEPA (2005) groups infrastructure security devices or products described below into four general categories:

- Physical asset monitoring and control devices
- Cyber protection devices
- Communication/integration
- Environmental monitoring devices

### Physical Asset Monitoring and Control Devices

#### *Aboveground, Outdoor Equipment Enclosures*

CS sector facilities and sites can consist of multiple structural components spread over a wide area and typically include a centralized production, storage, and distribution centers, as well component supply facilities that are typically distributed at multiple locations throughout the area. One of the primary reasons for constructing structural components that house operational equipment aboveground eliminates the safety risks associated with confined space entry, which is often required for the maintenance of equipment located

---

<sup>1</sup> It is important to point out that even though the following USEPA security asset and device recommendations were first made for the water/wastewater critical infrastructure, these recommendations are applicable to all other critical infrastructure sectors, including the CS sector where practicable.

belowground. In addition, space restrictions often limit the amount of equipment that can be located inside, and there are concerns that some types of equipment (such as backflow prevention devices—to prevent chemicals and fuel wastes from entering plant and off-site potable water systems) can, under certain circumstances, discharge fuel slurry or waste mixtures that could flood pits, vaults, or equipment rooms. In regard to electrical power, electrical substations are not usually suited for underground installation. Therefore, many pieces of critical electrical manufacturing equipment are located outdoors and aboveground in configurations that are properly fenced, insulated, or isolated to prevent accidental electrical shock or short circuits/fires in equipment.

Experience demonstrates that many different system components can be and are often installed outdoors and aboveground, many of them controlled by wireless communication devices. Following are the examples of the types of components that could be included in commercial facilities or its ancillaries are:

- Backflow prevention devices
- Air release and control valves
- Pressure vacuum breakers
- Oil and gas pumps and motors
- Petrochemical storage and feed equipment
- Meters
- Sampling equipment
- Instrumentation
- Electrical substations
- Oil and natural gas pipelines

One of the most effective security measures for protecting aboveground equipment, where feasible, is to place it inside a building or exterior fenced structure. When/where this is not possible, enclosing the equipment or parts of the equipment using some sort of commercial or homemade add-on structure may help to prevent tampering with the equipment. These types of add-on structures or enclosures, which are designed to protect people and animals from electrocution and to protect equipment both from the elements and from unauthorized access or tampering, typically consist of a box-like fenced structure that is placed over or around the entire component, or over/around critical parts of the component (i.e., valves), and is then secured to delay or prevent intruders from tampering with the equipment. The enclosures are typically locked or otherwise anchored to a solid foundation, which makes it difficult for unauthorized personnel to remove the enclosure and access the equipment.

Standardized aboveground enclosures are available in a wide variety of materials, sizes, and configurations. Many options and security features are also available for each type of enclosure, and this allows system operators

the flexibility to customize an enclosure for a specific application and/or price range. In addition, most manufacturers can custom-design enclosures if standard, off-the-shelf enclosures do not meet a user's needs.

Many of these enclosures are designed to meet certain standards. For example, the American Society of Sanitary Engineers (ASSE) has developed Standard #1060, *Performance Requirements for Outdoor Enclosures for Backflow Prevention Assemblies*. If an enclosure will be used to house backflow preventer, this standard specifies the acceptable construction materials for the enclosure, as well as the performance requirements that the enclosure should meet, including specifications for freeze protection, drainage, air inlets, access for maintenance, and hinge requirements. ASSE #1060 also states that the enclosure should be lockable to enhance security.

Electrical substation and electrical equipment enclosures must meet the requirements and recommendations of various OSHA Standards, National Fire Protection Association (NFPA), National Electrical Codes (NEC), Institute of Electrical and Electronic Engineers (IEEE), and local code requirements.

Equipment enclosures can generally be categorized into one of four main configurations, which include:

- One piece, drop over enclosures
- Hinged or removable top enclosures
- Sectional enclosures
- Shelters with access locks

All enclosures, including those with integral floors, must be secured to a foundation to prevent them from being moved or removed. Un- or poorly anchored enclosures may be blown off the equipment being protected, or may be defeated by intruders. In either case, this may result in the equipment beneath the enclosure becoming exposed and damaged. Therefore, ensuring that the enclosure is securely anchored will increase the security of the protected equipment.

The three basic types of foundations that can be used to anchor the above-ground equipment enclosure are concrete footers, concrete slabs-on-grade, or manufactured fiberglass pads. The most common types of foundations utilized for equipment enclosures are standard or slab-on-grade footers; however, local climate and soil conditions may dictate whether either of these types of foundations can be used. These foundations can be either precast or poured in place at the installation site. Once the foundation is installed and properly cured, the equipment enclosure is bolted or anchored to the foundation to secure it in place.

An alternative foundation, specifically for use with smaller Hot Box® enclosures, is a manufactured fiberglass pad known as the Glass Pad™. The

Glass Pad™ has the center cut out so that it can be dropped directly over the piece of equipment being enclosed. Once the pad is set level on the ground, it is backfilled over a 2-inch flange located around its base. The enclosure is then placed on top of the foundation and is locked in place with either a staple- or a slotted-anchor, depending on the enclosure configuration.

One of the primary attributes of a security enclosure is its strength and resistance to breaking and penetration. Accordingly, the materials from which the enclosure is constructed will be important in determining the strength of the enclosure and thus its usefulness for security applications. Enclosures are typically manufactured for either fiberglass or aluminum. With the exception of the one piece, drop over enclosure, which is typically fabricated from fiberglass, each configuration described above can be constructed from either material. In addition, enclosures can be custom-manufactured from polyurethane, galvanized steel, or stainless steel. Galvanized or stainless steel is often offered as an exterior layer, or “skin,” for an aluminum enclosure. Although they are typically utilized in underground applications, precast concrete structures can also be used as aboveground equipment enclosures. However, precast structures are much heavier and more difficult to maneuver than are their fiberglass and aluminum counterparts. Concrete is also brittle, and that can be a security concern, however, products can be applied to concrete structures to add strength and minimize security risks (i.e., epoxy coating). Because precast concrete structures can be purchased from any concrete producers, this document does not identify specific vendors for these types of products.

In addition to the construction materials, enclosure walls can be configured or reinforced to give them added strength. Adding insulation is one option that can strengthen the structural characteristics of an enclosure; however, some manufacturers offer additional features to add strength to exterior walls. For example, while most enclosures are fabricated with a flat wall construction, some vendors manufacture fiberglass shelters with ribbed exterior walls. These ribs increase the structural integrity of the wall and allow the fabrication of standard shelters up to 20 feet in length. Another vendor has developed a proprietary process that uses a series of integrated fiberglass beams that are placed throughout a foam inner core to tie together the interior and exterior walls and roof. Yet another vendor constructs aluminum enclosures with horizontal and vertical redwood beams for structural support.

Other security features that can be implemented on aboveground, outdoor equipment enclosures include locks, mounting brackets, tamper-resistant doors, and exterior lighting.

### *Active Security Barriers (Crash Barriers)*

Terrorist vehicle attacks are on the rise. Consider the Halloween 2017 truck attack in New York City that killed eight and injured many. There are steps we can take to lessen the possibility of many of these attacks. For example,

active security barriers (also known as crash barriers) are large structures that are placed in roadways at entrance and exit points to protect facilities to control vehicle access to these areas. These barriers are placed perpendicular to traffic to block the roadway, so that the only way that traffic can pass the barrier is for the barrier to be moved out of the roadway. These types of barriers are typically constructed from sturdy materials, such as concrete or steel, such that vehicles cannot penetrate through them. They are also designed at a certain height off the roadway so that vehicles cannot go over them.

The key difference between active security barriers—which include wedges, crash beams, gates, retractable bollards, and portable barricades, and passive security barriers, which include non-movable bollards, jersey barriers, and planters—is that active security barriers are designed so that they can be raised and lowered or moved out of the roadway easily to allow authorized vehicles to pass them. Many of these types of barriers are designed so that they can be opened and closed automatically (i.e., mechanized gates, hydraulic wedge barriers), while others are easy to open and close manually (swing crash beams, manual gates). In contrast to active barriers, passive barriers are permanent, non-movable barriers, and thus they are typically used to protect the perimeter of a protected facility, such as sidewalks and other areas that do not require vehicular traffic to pass them. Several of the major types of active security barriers such as wedge barriers, crash beams, gates, bollards, and portable/removable barricades are described below.

*Wedge barriers* are plated, rectangular steel buttresses approximately 2 to 3 feet high that can be raised and lowered from the roadway. When they are in the open position, they are flush with the roadway and vehicles can pass over them. However, when they are in the closed (armed) position, they project up from the road at a 45 degree angle, with the upper end pointing toward the oncoming vehicle and the base of the barrier away from the vehicle. Generally, wedge barriers are constructed from heavy gauge steel or concrete that contains an impact-dampening iron rebar core that is strong and resistant to breaking or cracking, thereby allowing them to withstand the impact from a vehicle attempting to crash through them. In addition, both of these materials help to transfer the energy of the impact over the barrier's entire volume, thus helping to prevent the barrier from being sheared off its base. In addition, because the barrier is angled away from traffic, the force of any vehicle impacting the barrier is distributed over the entire surface of the barrier and is not concentrated at the base, which helps prevent the barrier from breaking off at the base. Finally, the angle of the barrier helps hang up any vehicles attempting to drive over it.

Wedge barriers can be fixed or portable. Fixed wedge barriers can be mounted on the surface of the roadway ("surface-mounted wedges") or in a shallow mount in the road's surface, or they can be installed completely below the road surface. Surface-mounted wedge barricades operate by rising from a flat position on the surface of the roadway, while shallow-mount wedge barriers

rise from their resting position just below the road surface. In contrast, below-surface wedge barriers operate by rising from beneath the road surface. Both the shallow-mounted and surface-mounted barriers require little or no excavation, and thus do not interfere with buried utilities. All three barrier mounting types project above the road surface and block traffic when they are raised into the armed position. Once they are disarmed and lowered, they are flush with the road; thereby allowing traffic to pass portable wedge barriers that are moved into place on wheels that are removed after the barrier has been set into place.

Installing rising wedge barriers requires preparation of the road surface. Installing surface-mounted wedges does not require that the road be excavated; however, the road surface must be intact and strong enough to allow the bolts anchoring the wedge to the road surface to attach properly. Shallow-mount and below-surface wedge barricades require excavation of a pit that is large enough to accommodate the wedge structure, as well as any arming/disarming mechanisms. Generally, the bottom of the excavation pit is lined with gravel to allow for drainage. Areas not sheltered from rain or surface runoff can install a gravity drain or self-priming pump. Table 10.1 lists the pros and cons of wedge barriers.

*Crash beam barriers* consist of aluminum beams that can be opened or closed across the roadway. While there are several different crash beam designs, every crash beam system consists of an aluminum beam that is supported on each side of the road by a solid footing or buttress, which is typically constructed from concrete, steel, or some other strong material. Beams typically contain an interior steel cable (typically at least 1 inch in diameter) to give the beam added strength and rigidity. The beam is connected by a heavy duty hinge or other mechanism to one of the footings so that it can swing or rotate out of the roadway when it is open, and can swing back across the road when it is in the closed (armed) position, blocking the road and inhibiting access by unauthorized vehicles. The non-hinged end of the beam can be locked into its footing, thus providing anchoring for the beam on both sides of the road and increasing the beam's resistance to any vehicles attempting to penetrate through it. In addition, if the crash beam is hit by a vehicle, the aluminum beam transfers the impact energy to the interior cable, which in turn transfers the impact energy through the footings and into their foundation, thereby minimizing the chance that the impact will snap the beam and allow the intruding vehicle to pass through.

Crash beam barriers can employ drop-arm, cantilever, or swing beam designs. Drop-arm crash beams operate by raising and lowering the beam vertically across the road. Cantilever crash beams are projecting structures that are opened and closed by extending the beam from the hinge buttress to the receiving buttress located on the opposite side of the road. In the swing beam design, the beam is hinged to the buttress such that it swings horizontally across the road. Generally, swing beam and cantilever designs are used at locations where

**Table 10.1 Pros and Cons of Wedge Barriers**

<i>Pros</i>	<i>Cons</i>
Can be surface mounted or completely installed below the roadway surface.	Installations below the surface of the roadway will require construction that may interfere with buried utilities.
Wedge barriers have a quick response time (normally 3.5 to 10.5 seconds, but barrier can be 1 to 3 seconds in emergency situations. Because emergency activation of the barrier causes more wear and tear on the system than does normal activation, it is recommended for use only in true emergency situations	Regular maintenance is needed to keep wedge fully operational.
Surface or shallow-mount wedge barricades can be utilized in locations with a high water table and/or corrosive soils.	Improper use of the system may result in authorized vehicles being hung up by the barrier and damaged. Guards must be trained to use the system properly to ensure that this does not happen. Safety technologies may also be installed to reduce the risk of the wedge activating under an authorized vehicle.
All three wedge barrier designs have a high crash rating, thereby allowing them to be employed for higher security applications.	
These types of barrier are extremely visible, which may deter potential intruders.	

Source: USEPA, 2005.

a vertical lift beam is impractical. For example, the swing beam or cantilever designs are utilized at entrances and exits with overhangs, trees, or buildings that would physically block the operation of the drop-arm beam design.

Installing any of these crash beam barriers involves the excavation of a pit approximately 48 inch deep for both the hinge and the receiver footings. Due to the depth of excavation, the site should be inspected for underground utilities before digging begins. Table 10.2 lists the pros and cons of crash beams.

In contrast to wedge barriers and crash beams, which are typically installed separately from a fence line, *gates* are often integrated units of a perimeter fence or wall around a facility.

Gates are basically movable pieces of fencing that can be opened and closed across a road. When the gate is in the closed (armed) position, the leaves of the gate lock into steel buttresses that are embedded in concrete foundation located on both sides of the roadway, thereby blocking access to the roadway. Generally, gate barricades are constructed from a combination of heavy gauge



**Table 10.2 Pros and Cons of Crash Beams**

<i>Pros</i>	<i>Cons</i>
Requires little maintenance, while providing long-term durability.	Crash beams have a slower response time (normally 9.5 to 15.3 seconds, but can be reduced to 7 to 10 seconds in emergency situations) than do other types of active security barriers, such as wedge barriers. Because emergency activation of the barrier causes more wear and tear on the system than normal activation does, it is recommended for use only in true emergency situations.
No excavation is required in the roadway itself to install crash beams.	All three crash beam designs possess a low crash rating relative to other types of barriers, such as wedge barriers, and thus they typically are used for lower security applications. Certain crash barriers may not be visible to oncoming traffic and therefore may require additional lighting and/or other warning markings to reduce the potential for traffic to accidentally run into the beam.

Source: USEPA, 2005.

**Table 10.3 Pros and Cons of Gates**

<i>Pros</i>	<i>Cons</i>
All three gate designs possess an intermediate crash rating, thereby allowing them to be utilized for medium to higher security applications.	Gates have a slower response time (normally 10 to 15 seconds, but can be reduced to 7 to 10 seconds in emergency situations) than do other types of active security barriers, such as wedge barriers. Because emergency activation of the barrier causes more wear and tear on the system than normal activation does, it is recommended for use only in true emergency situations.
Requires very little maintenance.	
Can be tailored to blend in with perimeter fencing.	
Gate construction requires no roadway excavation.	
Cantilever gates are useful for roads with high crowns or drainage gutters.	
These types of barriers are extremely visible, which may deter intruders.	
Gates can also be used to control pedestrian traffic.	

Source: USEPA, 2005.

steel and aluminum that can absorb an impact from vehicles attempting to ram through them. Any remaining impact energy not absorbed by the gate material is transferred to the steel buttresses and their concrete foundation.

Gates can utilize a cantilever, linear, or swing design. Cantilever gates are projecting structures that operate by extending the gate from the hinge footing across the roadway to the receiver footing. A linear gate is designed to slide across the road on tracks via a rack and pinion drive mechanism. Swing gates are hinged so that they can swing horizontally across the road.

Installation of the cantilever, linear, or swing gate designs described above involve the excavation of a pit approximately 48 inch deep for both the hinge and receiver footings to which the gates are attached. Due to the depth of excavation, the site should be inspected for underground utilities before digging begins. Table 10.3 lists the pros and cons of gates.

*Bollards* are vertical barriers at least 3 feet tall and 0.4 to 2 feet in diameter that are typically set 4 to 5 feet apart from each other so that they block vehicles from passing between them (see figure 10.2). Smaller bollards, usually 4-inch-diameter pipe filled with concrete, are installed in parking areas



**Figure 10.2 Bollard Sequence Placed In Front of Store Fronts and Pedestrian Sidewalks in Order to Protect Store Property and Pedestrians from Rogue Terrorist Drivers using Vehicles of Death and Destruction.** *Source:* Illustration by F. R. Spellman and Katherin Welsh.

to prevent vehicles from striking walls or windows or to protect walkway areas. Bollards can either be fixed in place, removable, or retractable. Fixed and removable bollards are passive barriers that are typically used along building perimeters or on sidewalks to prevent vehicles from them, while allowing pedestrians to pass them. In contrast to passive bollards, retractable bollards are active security barriers that can easily be raised and lowered to allow vehicles to pass between them. Thus, they can be used in driveways or on roads to control vehicular access. When the bollards are raised, they project above the road surface and block the roadway; when they are lowered, they sit flush with the road surface, and thus allow traffic to pass over them. Retractable bollards are typically constructed from steel or other materials that have a low weight-to-volume ratio so that they require low power to raise and lower. Steel is also more resistant to breaking than is a more brittle material, such as concrete, and is better able to withstand direct vehicular impact without breaking apart.

Retractable bollards are installed in a trench dug across a roadway—typically at an entrance or gate. Installing retractable bollards requires preparing the road surface. Depending on the vendor, bollards can be installed either in a continuous slab of concrete or in individual excavations with concrete poured in place. The required excavation for a bollard is typically slightly wider and slightly deeper than the bollard height when extended aboveground. The bottom of the excavation is typically lined with gravel to allow drainage. The bollards are then connected to a control panel which controls the raising and lowering of the bollards. Installation typically requires mechanical, electrical, and concrete work; if utility personnel with these skills are available, then the utility can install the bollards themselves. Table 10.4 lists the pros and cons of retractable bollards.

**Table 10.4 Pros and Cons of Retractable Bollards**

<i>Pros</i>	<i>Cons</i>
Bollards have a quick response time (normally 3 to 10 seconds, but can be reduced to 1 to 3 seconds in emergency situations).	Bollard installations will require construction below the surface of the roadway, which may interfere with buried utilities.
Bollards have an intermediate crash rating, which allows them to be utilized for medium to higher security applications.	Some maintenance is needed to ensure barrier is free to move up and down.
	The distance between bollards must be decreased (i.e., more bollards must be installed along the same perimeter) to make these systems effective against small vehicles (i.e., motorcycles).

Source: USEPA, 2005.

*Portable/removable barriers*, which can include removable crash beams and wedge barriers, are mobile obstacles that can be moved in and out of position on a roadway. For example, a crash beam may be completely removed and stored off-site when it is not needed. An additional example would be wedge barriers that are equipped with wheels that can be removed after the barricade is towed into place.

When portable barricades are needed, they can be moved into position rapidly. To provide them with added strength and stability, they are typically anchored to buttress boxes that are located on either side of the road. These buttress boxes, which may or may not be permanent, are usually filled with sand, water, cement, gravel, or concrete to make them heavy and aid in stabilizing the portable barrier. In addition, these buttresses can help dissipate any impact energy from vehicles crashing into the barrier itself.

Because these barriers are not anchored into the roadway, they do not require excavation or other related construction for installation. In contrast, they can be assembled and made operational in a short period of time. The primary shortcoming to this type of design is that these barriers may move if they are hit by vehicles. Therefore, it is important to carefully assess the placement and anchoring of these types of barriers to ensure that they can withstand the types of impacts that may be anticipated at that location. Table 10.5 lists the pros and cons of portable/removable barricades.

Because the primary threat to active security barriers is that vehicles will attempt to crash through them, their most important attributes are their size, strength, and crash resistance. Other important features for an active security barrier are the mechanisms by which the barrier is raised and lowered to allow authorized vehicle entry, and other factors, such as weather resistance and safety features.

**Table 10.5 Pros and Cons of Portable/Removable Barricades**

<i>Pros</i>	<i>Cons</i>
Installing portable barricades requires no foundation or roadway excavation.	Portable barriers may move slightly when hit by a vehicle, resulting in a lower crash resistance.
Can be moved in and out of position in a short period of time.	Portable barricades typically require 7.75 to 16.25 seconds to move into place, and thus they are considered to have a medium response time when compared with other active barriers.
Wedge barriers equipped with wheels can be easily towed into place.	
Minimal maintenance is needed to keep barriers fully operational.	

Source: USEPA, 2005.

## Alarms

An *alarm system* is a type of electronic monitoring system that is used to detect and respond to specific types of events—such as unauthorized access to an asset, or a possible fire. In chemical processing systems, alarms are also used to alert operators when process operating or monitoring conditions go out of preset parameters (i.e., process alarms). These types of alarms are primarily integrated with process monitoring and reporting systems (i.e., SCADA systems). Note that this discussion does not focus on alarm systems that are not related to a facility's processes.

Alarm systems can be integrated with fire detection systems, intrusion detection systems (IDSs), access control systems, or closed-circuit television (CCTV) systems, such that these systems automatically respond when the alarm is triggered. For example, a smoke detector alarm can be set up to automatically notify the fire department when smoke is detected; or an intrusion alarm can automatically trigger cameras to turn on in a remote location so that personnel can monitor that location.

An alarm system consists of sensors that detect different types of events; an arming station that is used to turn the system on and off; a control panel that receives information, processes it, and transmits the alarm; and an annunciator that generates a visual and/or audible response to the alarm. When a sensor is tripped it sends a signal to a control panel, which triggers a visual or audible alarm and/or notifies a central monitoring station. A more complete description of each of the components of an alarm system is provided below.

*Detection devices* (also called *sensors*) are designed to detect a specific type of event (such as smoke, intrusion). Depending on the type of event they are designed to detect, sensors can be located inside or outside of the facility or other asset. When an event is detected, the sensors use some type of communication method (such as wireless radio transmitters, conductors, or cables) to send signals to the control panel to generate the alarm. For example, a smoke detector sends a signal to a control panel when it detects smoke.

Alarms use either normally closed (NC) or normally open (NO) electric loops, or “circuits,” to generate alarm signals. These two types of circuits are discussed separately below.

In NC loops or circuits, all of the system's sensors and switches are connected in series. The contacts are “at rest” in the closed (on) position, and current continually passes through the system. However, when an event triggers the sensor, the loop is opened, breaking the flow of current through the system and triggering the alarm. NC switches are used more often than are NO switches because the alarm will be activated if the loop or circuit is broken or cut, thereby reducing the potential for circumventing the alarm. This is known as a “supervised” system.

In NO loops or circuits, all of the system's sensors and switches are connected in parallel. The contacts are "at rest" in the open (off) position, and no current passes through the system. However, when an event triggers the sensor, the loop is closed. This allows current to flow through the loop, powering the alarm. NO systems are not "supervised" because the alarm will not be activated if the loop or circuit is broken or cut. However, adding an end-of-line resistor to an NO loop will cause the system to alarm if tampering is detected.

An *arming station*, which is the main user interface with the security system, allows the user to arm (turn on), disarm (turn off), and communicate with the system. How a specific system is armed will depend on how it is used. For example, while IDSs can be armed for continuous operation (twenty-four hours/day), they are usually armed and disarmed according to the work schedule at a specific location so that personnel going about their daily activities do not set off the alarms. In contrast, fire protection systems are typically armed 24 hours/day.

A *control panel* receives information from the sensors and sends it to an appropriate location, such as to a central operations station or to a twenty-four-hour monitoring facility. Once the alarm signal is received at the central monitoring location, personnel monitoring for alarms can respond (such as by sending security teams to investigate or by dispatching the fire department).

An *annunciator* responds to the detection of an event by emitting a signal. This signal may be visual, audible, electronic, or a combination of these three. For example, fire alarm signals will always be connected to audible annunciators, whereas intrusion alarms may not be.

Alarms can be reported locally, remotely, or both locally and remotely. Local and remotely (centrally) reported alarms are discussed in more detail below.

A *local alarm* emits a signal at the location of the event (typically using a bell or siren). A "local only" alarm emits a signal at the location of the event but does not transmit the alarm signal to any other location (i.e., it does not transmit the alarm to a central monitoring location). Typically, the purpose of a "local only" alarm is to frighten away intruders, and possibly to attract the attention of someone who might notify the proper authorities. Because no signal is sent to a central monitoring location, personnel can only respond to a local alarm if they are in the area and can hear and/or see the alarm signal.

Fire alarm systems must have local alarms, including both audible and visual signals. Most fire alarm signal and response requirements are codified in the National Fire Alarm Code, National Fire Protection Association (NFPA) 72. NFPA 72 discusses the application, installation, performance, and maintenance of protective signaling systems and their components. In contrast to fire alarms, which require a local signal when fire is detected,

many IDSs do not have a local alert device, because monitoring personnel do not wish to inform potential intruders that they have been detected. Instead, these types of systems silently alert monitoring personnel that an intrusion has been detected, thus allowing monitoring personnel to respond.

In contrast to systems that are set up to transmit “local only” alarms when the sensors are triggered, systems can also be set up to transmit signals to a *central location*, such as to a control room or guard post at the utility, or to a police or fire station. Most fire/smoke alarms are set up to signal both at the location of the event and at a fire station or central monitoring station. Many insurance companies require that facilities install certified systems that include alarm communication to a central station. For example, systems certified by the Underwriters Laboratory (UL) require that the alarm be reported to a central monitoring station.

The main differences between alarm systems lie in the types of event detection devices used in different systems. *Intrusion sensors*, for example, consist of two main categories: perimeter sensors and interior (space) sensors. *Perimeter intrusion sensors* are typically applied on fences, doors, walls, windows, and so on, and are designed to detect an intruder before he/she accesses a protected asset (i.e., perimeter intrusion sensors are used to detect intruders attempting to enter through a door, window). In contrast, *interior intrusion sensors* are designed to detect an intruder who has already accessed the protected asset (i.e., interior intrusion sensors are used to detect intruders once they are already within a protected room or building). These two types of detection devices can be complementary, and they are often used together to enhance security for an asset. For example, a typical intrusion alarm system might employ a perimeter glass-break detector that protects against intruders accessing a room through a window, as well as an ultrasonic interior sensor that detects intruders that have gotten into the room without using the window. Table 10.6 lists and describes types of perimeter and interior sensors.

*Fire Detection/Fire Alarm Systems* consist of different types of fire detection devices and fire alarm systems available. These systems may detect fire, heat, smoke, or a combination of any of these. For example, a typical fire alarm system might consist of heat sensors, which are located throughout a facility and which detect high temperatures or a certain change in temperature over a fixed time period. A different system might be outfitted with both smoke and heat detection devices. A summary of several different types of fire/smoke/heat detection sensors is provided in table 10.7.

Once a sensor in an alarm system detects an event, it must communicate an alarm signal. The two basic types of alarm communication systems are hardwired and wireless. Hardwired systems rely on wire that is run from

**Table 10.6 Perimeter and Interior Sensors**

<i>Types of Perimeter Sensor</i>	<i>Description</i>
Foil	Foil is a thin, fragile, lead-based metallic tape that is applied to glass windows and doors. The tape is applied to the window or door, and electric wiring connects this tape to a control panel. The tape functions as a conductor and completes the electric circuit with the control panel. When an intruder breaks the door or window, the fragile foil breaks, opening the circuit and triggering an alarm condition.
Magnetic switches (reed switches)	The most widely used perimeter sensor. They are typically used to protect doors, as well as windows that can be opened (windows that cannot be opened are more typically protected by foil alarms).
Glass break detectors	Placed on glass and sense vibrations in the glass when it is disturbed. The two most common types of glass-break detectors are shock sensors and audio discriminators.
<i>Types of Interior Sensor</i>	<i>Description</i>
Passive infrared (PIR)	Presently the most popular and cost-effective interior sensors. PIR detectors monitor infrared radiation (energy in the form of heat) and detect rapid changes in temperature within a protected area. Because infrared radiation is emitted by all living things, these types of sensors can be very effective.
Quad PIRs	Consist of two dual-element sensors combined in one housing. Each sensor has a separate lens and a separate processing circuitry, which allows each lens to be set up to generate a different protection pattern
Ultrasonic detectors	Emit high frequency sound waves and sense movement in a protected area by sensing changes in these waves. The sensor emits sound waves that stabilize and set a baseline condition in the area to be protected. Any subsequent movement within the protected area by a would-be intruder will cause a change in these waves, thus creating an alarm condition.
Microwave detectors	Emit ultra high frequency radio waves, and the detector senses any changes in these waves as they are reflected throughout the protected space. Microwaves can penetrate through walls, and thus a unit placed in one location may be able to protect multiple rooms.
Dual technology devices	Incorporate two different types of sensor technology (such as PIR and microwave technology) together in one housing. When both technologies sense an intrusion, an alarm is triggered.

Source: USEPA, 2005.



**Table 10.7 Fire/Smoke/Heat Detection Sensors**

<i>Types of Detectors</i>	<i>Description</i>
Thermal detector	Sense when temperatures exceed a set threshold (fixed temperature detectors) or when the rate of change of temperature increases over a fixed time period (rate-of-rise detectors).
Duct detector	Is located within the haring and ventilation ducts of the facility. This sensor detects the presence of smoke within the system's return or supply ducts. A sampling tube can be added to the detector to help span the width of the duct.
Smoke detectors	Sense invisible and/or visible products of combustion. The two principle types of smoke detectors are photoelectric and ionization detectors. The major differences between these devices are described below: <ul style="list-style-type: none"> <li>• Photoelectric smoke detectors react to visible particles of smoke. These detectors are more sensitive to the cooler smoke with large smoke particles that is typical of smoldering fires.</li> <li>• Ionization smoke detectors are sensitive to the presence of ions produced by the chemical reactions that take place with few smoke particle, such as those typically produced by fast burning/flaming fires.</li> </ul>
Multi-sensor detectors	Are a combination of photoelectric and thermal detectors. The photoelectric sensor serves to detect smoldering fires, while the thermal detector senses the eat give off from fast burning/flaming fires.
Carbon monoxide (CO) detectors	Are used to indicate the outbreak of fire by sensing the level of carbon monoxide in the air. The detector has an electrochemical cell which senses carbon monoxide but not some or other products of combustion.
Beam detectors	Are designed to protect large, open spaces such as industrial warehouses. These detectors consist of three parts: the transmitter, which projects a beam of infrared light; the receiver, which registers the light and produces an electrical signal; and the interface, which processes the signal and generates alarm of fault signals. In the event of a fire, smoke particles obstruct the beam of light. Once a preset threshold is exceeded, the detector will go into alarm.
Flame detectors	Sense either ultraviolet (UV) or infrared (IR) radiation emitted by a fire.
Air-sampling detectors	Actively and continuously sample the air from a protected space and are able to sense the precombustion stages of incipient fire.

Source: USEPA, 2005.

the control panel to each of the detection devices and annunciators. Wireless systems transmit signals from a transmitter to a receiver through the air—primarily using radio or other waves. Hardwired systems are usually lower cost, more reliable (they are not affected by terrain or environmental factors), and significantly easier to troubleshoot than are wireless systems. However, a major disadvantage of hardwired systems is that it may not be possible to hardwire all locations (e.g., it may be difficult to hardwire remote locations). In addition, running wires to their required locations can be both time consuming and costly. The major advantage to using wireless systems is that they can often be installed in areas where hardwired systems are not feasible. However, wireless components can be much more expensive when compared to hardwired systems. In addition, in the past, it has been difficult to perform self-diagnostics on wireless systems to confirm that they are communicating properly with the controller. Presently, the majority of wireless systems incorporate supervising circuitry, which allows the subscriber to know immediately if there is a problem with the system (such as a broken detection device or a low battery), or if a protected door or window has been left open.

### *Backflow Prevention Devices*

Backflow prevention devices are designed to prevent backflow, which is the reversal of the normal and intended direction of water flow in a water system. Backflow is a potential problem in a petrochemical processing system because if incorrectly cross-connected to potable water it can spread contaminated water back through a distribution system. For example, backflow at uncontrolled cross connections (cross connections are any actual or potential connection between the public water supply and a source of chemical contamination) or pollution can allow pollutants or contaminants to enter the potable water system. More specifically, backflow from private plumbing systems, industrial areas, hospitals, and other hazardous contaminant-containing systems, into public water mains and wells poses serious public health risks and security problems. Cross contamination from private plumbing systems can contain biological hazards (such as bacteria or viruses) or toxic substances that can contaminate and sicken an entire population in the event of backflow. The majority of historical incidences of backflow have been accidental, but growing concern that contaminants could be intentionally backfed into a system is prompting increased awareness for private homes, businesses, industries, and areas most vulnerable to intentional strikes. Therefore, backflow prevention is a major tool for the protection of water systems.

Backflow may occur under two types of conditions: backpressure and backsiphonage. *Backpressure* is the reverse from normal flow direction within a piping system that is the result of the downstream pressure being higher than the supply pressure. These reductions in the supply pressure occur whenever the amount of water being used exceeds the amount of water supplied, such as during water line flushing, firefighting, or breaks in water mains. *Backsiphonage* is the reverse from normal flow direction within a piping system that is caused by negative pressure in the supply piping (i.e., the reversal of normal flow in a system caused by a vacuum or partial vacuum within the water supply piping). Backsiphonage can occur where there is a high velocity in a pipe line; when there is a line repair or break that is lower than a service point; or when there is lowered main pressure due to high water withdrawal rate, such as during firefighting or water main flushing.

To prevent backflow, various types of backflow preventers are appropriate for use. The primary types of backflow preventers are as follows:

- Air gap drains
- Double check valves
- Reduced pressure principle assemblies
- Pressure vacuum breakers

### *Biometric Security Systems*

Biometrics involves measuring the unique physical characteristics or traits of the human body. In ancient times biometrics involved the judging of one's accent, body hair, or face to determine friend or foe. Presently, it is well known that any aspect of the body that is measurably different from person to person—for example, fingerprints or eye characteristics—can serve as a unique biometric identifier for that individual. Biometric systems recognizing fingerprints, palm shape, eyes, face, voice, and signature comprise the bulk of the current biometric systems that recognize other biological features do exist.

Biometric security systems use biometric technology combined with some type of locking mechanisms to control access to specific assets. In order to access an asset controlled by a biometric security system, an individual's biometric trait must be matched with an existing profile stored in a database. If there is a match between the two, the locking mechanisms (which could be a physical lock, such as at a doorway, an electronic lock, such as at a computer terminal or some other type of lock) are disengaged, and the individual is given access to the asset.

A biometric security system is typically comprised of the following components:

- A sensor, which measures/records a biometric characteristic or trait.
- A control panel, which serves as the connection point between various system components. The control panel communicates information back and forth between the sensor and the host computer, and controls access to the asset by engaging or disengaging the system lock based on internal logic and information from the host computer.
- A host computer, which processes and stores the biometric trait in a database.
- Specialized software, which compares an individual image taken by the sensor with a stored profile or profiles.
- A locking mechanism which is controlled by the biometric system.
- A power source to power the system.

### *Biometric Hand and Finger Geometry Recognition*

Hand and finger geometry recognition is the process of identifying an individual through the unique “geometry” (shape, thickness, length, width, etc.) of that individual’s hand or fingers. Hand geometry recognition has been employed since the early 1980s and is among the most widely used biometric technologies for controlling access to important assets. It is easy to install and use, and is appropriate for use in any location requiring use of two finger highly accurate, nonintrusion biometric security. For example, it is currently used in numerous workplaces, day care facilities, hospitals, universities, airports, refineries, and power plants.

A newer option within hand geometry recognition technology is finger geometry recognition (not to be confused with fingerprint recognition). Finger geometry recognition relies on the same scanning methods and technologies as does hand geometry recognition, but the scanner only scans two of the user’s fingers, as opposed to his entire hand. Finger geometry recognition has been in commercial use since the mid-1990s and is mainly used in time and attendance applications (i.e., to track when individuals have entered and exited a location). To date the only large-scale commercial use of two finger geometry for controlling access is at Disney World, where season pass holders use the geometry of their index and middle finger to gain access to the facilities.

To use a hand or finger geometry unit, an individual presents his or her hand or fingers to the biometric unit for “scanning.” The scanner consists

of a Charged Coupled Device (CCD), which is essentially a high-resolution digital camera; a reflective platen on which the hand is placed; and a mirror or mirrors that help capture different angles of the hand or fingers. The camera “scans” individual geometric characteristics of the hand or fingers by taking multiple images while the user’s hand rests on the reflective platen. The camera also captures “depth,” or three-dimensional information, through light reflected from the mirrors and the reflective platen. This live image is then compared to a “template” that was previously established for that individual when they were “enrolled” in the system. If the live scan of the individual matches the stored template, the individual is “verified” and is given access to that asset. Typically, verification takes about two seconds. In access control applications, the scanner is usually connected to some sort of electronic lock, which unlocks the door, turnstile, or other entry barrier when the user is verified. The user can then proceed through the entrance. In time and attendance applications, the time that an individual checks in or out of a location is stored for later use.

As discussed above, hand and finger geometry recognition systems can be used in several different types of applications, including access control and time and attendance tracking. While time and attendance tracking can be used for security, it is primarily used for operations and payroll purposes (i.e., clocking in and clocking out). In contrast, access control applications are more likely to be security related. Biometric systems are widely used for access control and can be used on various types of assets, including entryways, computers, vehicles, and so on. However, because of their size, hand/finger recognition systems are primarily used in entryway access control applications.

### *Biometric Overview-Iris Recognition*

The iris, which is the colored or pigmented area of the eye surrounded by the sclera (the white portion of the eye), is a muscular membrane that controls the amount of light entering the eye by contracting or expanding the pupil (the dark center of the eye). The dense, unique patterns of connective tissue in the human iris were first noted in 1936, but it was not until 1994, when algorithms for iris recognition were created and patented, that commercial applications using biometric iris recognition began to be used extensively. There are now two vendors producing iris recognition technology: both the original developer of these algorithms and the company, which has developed and patented a different set of algorithms for iris recognition.

The iris is an ideal characteristic for identifying individuals because it is formed in utero, and its unique patterns stabilize around eight months after birth. No two irises are alike; neither an individual’s right or left irises nor the

irises of identical twins. The iris is protected by the cornea (the clear covering over the eye), and therefore it is not subject to the aging or physical changes (and potential variation) that are common to some other biometric measures, such as the hand, fingerprints, and the face. Although some limited changes can occur naturally over time, these changes generally occur in the iris' melanin and therefore affect only the eye's color, and not its unique patterns (in addition, because iris scanning uses only black and white images, color changes would not affect the scan anyway). Thus, barring specific injuries or certain rare surgeries directly affecting the iris, the iris' unique patterns remain relatively unchanged over an individual's lifetime.

Iris recognition systems employ a monochromatic or black and white video camera that uses both visible and near infrared light to take video of an individual's iris. Video is used rather than still photography as an extra security procedure. The video is used to confirm the normal continuous fluctuations of the pupil as the eye focuses, which ensures that the scan is of a living human being, and not a photograph or some other attempted hoax. A high-resolution image of the iris is then captured or extracted from the video, using a device often referred to as a "frame grabber." The unique characteristics identified in this image are then converted into a numeric code, which is stored as a "template" for that user.

### *Card Identification/Access/Tracking Systems*

A card reader system is a type of electronic identification system that is used to identify a card and then perform an action associated with that card. Depending on the system, the card may identify where a person is or where they were at a certain time; it may authorize another action, such as disengaging a lock. For example, a security guard may use his card at card readers located throughout a facility to indicate that he has checked a certain location at a certain time. The reader will store the information and/or send it to a central location, where it can be checked later to ensure that the guard has patrolled the area. Other card reader systems can be associated with a lock, so that the cardholder must have their card read and accepted by the reader before the lock disengages.

A complete card reader system typically consists of the following components:

- Access cards that are carried by the user;
- Card readers that read the card signals and send the information to control units;
- Control units that control the response of the card reader to the card;
- A power source.

A “card” may be a typical card or another type of device, such as a key fob or wand. These cards store electronic information, which can range from a simple code (i.e., the alphanumeric code on a proximity card) to individualized personal data (i.e., biometric data on a Smartcard). The card reader reads the information stored on the card and sends it to the control unit, which determines the appropriate action to take when a card is presented. For example in a card access system, the control unit compares the information on the card versus stored access authorization information to determine if the card holder is authorized to proceed through the door. If the information stored in the card reader system indicates that the key is authorized to allow entrance through the doorway, the system disengages the lock and the key holder can proceed through the door.

There are many different types of card reader systems on the market. The primary differences between card reader systems are different in the way that data is encoded on the cards and in the way these data are transferred between the card and the card reader, and in the types of applications for which they are best suited. However, all card systems are similar in the way that the card reader and control unit interact to respond to the card.

While card readers are similar in the way that the card reader and control unit interact to control access, they are different in the way data is encoded on the cards and the way these data are transferred between the card and the card reader. There are several types of technologies available for card reader systems. These include:

- Proximity
- Wiegand
- Smartcard
- Magnetic stripe
- Bar code
- Infrared
- Barium ferrite
- Hollerith
- Mixed technologies

Table 10.8 below summarizes various aspects of card reader technologies. The determination for the level of security rate (low, moderate, or high) based on the level of technology a given card reader system has and how simple it is to duplicate that technology, and thus bypass the security. Vulnerability ratings were based on whether the card reader can be damaged easily due to frequent use or difficult working conditions (i.e., weather conditions if the reader is located outside). Often this is influenced by the number of moving parts in the system—the more the moving parts, then

**Table 10.8 Card Reader Technology**

<i>Types of Card Readers</i>	<i>Technology</i>	<i>Life Cycle</i>	<i>Vulnerability</i>	<i>Level of Security</i>
Proximity	Embedded radio frequency circuits encoded with unique information	Long	Virtually none	Moderate-high
Wiegand	Short lengths of small-diameter, special alloy wire with unique magnetic properties.	Long	Low susceptibility to damage; high durability due to embedded wires.	Moderate-expensive
Magnetic stripe	Electromagnetic charges to encode information on a piece of tape attached to back of card.	Moderate	Moderately susceptible to damage due to frequency of use.	Low-moderate
Bar code	Series of narrow and wide bars and spaces.	Short	High; easily damaged.	Low
Hollerith	Holes punched in a plastic or paper card and read optically.	Short	High; easily damaged from frequent use.	Low
Infrared	An encoded shadow pattern within the card, read using an infrared scanner.	Moderate	IR scanners are optical and thus, vulnerable to contamination.	High
Barium ferrite	Uses small bits of magnetized barium ferrite, placed inside a plastic and location of the "spots" determines the coding.	Moderate	Low susceptibility to damage; durable since spots are embedded in the material.	Moderate-high
Smartcards	Patterns or series of narrow and wide bars and spaces.	Short	High susceptibility to damage, low durability.	Highest

*Source:* USEPA, 2005.



greater the system's potential susceptibility to damage. The life cycle rating is based on the durability of a given card reader system over its entire operational period. Systems requiring frequent physical contact between the reader and the card often have a shorter life cycle due to the wear and tear to which the equipment is exposed. For many card reader systems, the vulnerability rating and life cycle ratings have a reciprocal relationship. For instance, if a given system has a high vulnerability rating it will almost always have a shorter life cycle.

Card reader technology can be implemented for facilities of any size and with any number of users. However, because individual systems vary in the complexity of their technology and in the level of security they can provide to a facility, individual users must determine the appropriate system for their needs. The following are some important features that should be considered when selecting a card reader system:

- The technological sophistication and security level of the card system;
- The size and security needs of the facility;
- The frequency with which the card system will be used. For systems that will experience a high frequency of use it is important to consider a system that has a longer life cycle and lower vulnerability rating, thus making it more cost effective to implement;
- The conditions in which the system will be used (i.e., will it be used on the interior or exterior of buildings, does it require light or humidity controls). Most card reader systems can operate under normal environmental conditions, and therefore this would be a mitigating factor only in extreme conditions;
- System costs.

### *Exterior Intrusion-Buried Sensors*

Buried sensors are electronic devices that are designed to detect potential intruders. The sensors are buried along the perimeters of sensitive assets and are able to detect intruder activity both above- and belowground. Some of these systems are composed of individual, stand-alone sensor units, while other sensors consist of buried cables.

There are four types of buried sensors that rely on different types of triggers. These are pressure or seismic; magnetic field; ported coaxial cable; and fiber-optic cables. These four sensors are all covert and terrain-following, meaning they are hidden from view and follow the contour of the terrain. The four types of sensors are described in more detail below. Table 10.9 presents the distinctions between the four types of buried sensors.

**Table 10.9** Types of Buried Sensors

<i>Type</i>	<i>Description</i>
Pressure or seismic	Responds to disturbances in the soil.
Magnetic field	Responds to a change in the local magnetic field caused by the movement of nearby metallic material.
Ported coaxial cables	Responds to motion of a material with a high dielectric constant or high conductivity near the cables.
Fiber-optic cables	Responds to a change in the shape of the fiber that can be sensed using sophisticated sensors and computer signal processing.

*Source:* Adapted from Garcia, M.L., 2001.

### *Exterior Intrusion Sensors*

An exterior intrusion sensor is a detection device that is used in an outdoor environment to detect intrusions into a protected area. These devices are designed to detect an intruder, and then communicate an alarm signal to an alarm system. The alarm system can respond to the intrusion in many different ways, such as by triggering an audible or visual alarm signal, or by sending an electronic signal to a central monitoring location that notifies security personnel of the intrusion.

Intrusion sensor can be used to protect many kinds of assets. Intrusion sensors that protect physical space are classified according to whether they protect indoor, or “interior” space (i.e., an entire building or room within a building), or outdoor, or “exterior” space (i.e., a fence line or perimeter). Interior intrusion sensors are designed to protect the interior space of a facility by detecting an intruder who is attempting to enter, or who has already entered a room or building. In contrast, exterior intrusion sensors are designed to detect an intrusion into a protected outdoor/exterior area. Exterior protected areas are typically arranged as zones or exclusion areas placed so that the intruder is detected early in the intrusion attempt before the intruder can gain access to more valuable assets (e.g., into a building located within the protected area). Early detection creates additional time for security forces to respond to the alarm.

Exterior intrusion sensors are classified according to how the sensor detects the intrusion within the protected area. The three classes of exterior sensor technology include:

- Buried line sensors
- Fence-associated sensors
- Freestanding sensors

- (1) **Buried Line Sensors**—As the name suggests, buried line sensors are sensors that are buried underground and are designed to detect disturbances within the ground—such as disturbances caused by an intruder digging, crawling, walking, or running on the monitored ground. Because they sense ground disturbances, these types of sensors are able to detect intruder activity both on the surface and below ground. Individual types of exterior buried line sensors function in different ways, including, by detecting motion, pressure, or vibrations within the protected ground, or by detecting changes in some type of field (e.g., magnetic field) that the sensors generate within the protected ground. Specific types of buried line sensors include pressure or seismic sensors, magnetic field sensors, ported coaxial cables, and fiber-optic cables. Details on each of these sensor types are provided below.

*Buried line pressure or seismic sensors* detect physical disturbances to the ground—such as vibrations or soil compression—caused by intruders walking, driving, digging, or otherwise physically contacting the protected ground. These sensors detect disturbances from all directions and, therefore, can protect an area radially outward from their location; however, because detection may weaken as a function of distance from the disturbance, choosing the correct burial depth from the design area will be crucial. In general, sensors buried at a shallow depth protect a relatively small area but have a high probability of detecting intrusion within that area, while sensors buried at a deeper depth protect a wider area but have a lower probability of detecting intrusion into that area.

*Buried line magnetic field sensors* detect changes in a local magnetic field that are caused by the moment of metallic objects within that field. This type of sensor can detect ferric metal objects worn or carried by an intruder entering a protected area on foot as well as vehicles being driven into the protected area.

*Buried line ported coaxial cable sensors* detect the motion of any object (i.e., human body, metal) possessing high conductivity and located within close proximity to the cables. An intruder entering into the protected space creates an active disturbance in the electric field, thereby triggering an alarm condition.

*Buried line fiber-optic cable sensors* detect changes in the attenuation of light signals transmitted within the cable. When the soil around the cable is compressed, the cable is distorted, and the light signal transmitted through the cable changes, initiating an alarm. This type of sensor is easy to install because it can be buried at a shallow burial depth (only a few centimeters) and still be effective.

- (2) **Fence-Associated Sensors**—Fence-associated sensors are either attached to an existing fence, or are installed in such a way as to create a fence. These sensors detect disturbances to the fence—such as those caused by an intruder attempting to climb the fence, or by an intruder attempting to cut or lift the fence fabric. Exterior fence-associated sensors include fence-disturbance sensors, taut-wire sensor fences, and electric field or capacitance sensors. Details on each of these sensor types are provided below.

*Fence-disturbance sensors* detect the motion or vibration of a fence, such as that, that can be caused by an intruder attempting to climb or cut through the fence. In general, fence-disturbance sensors are used on chain link fences or on other fence types where a movable fence fabric is hung between fence posts.

*Taut-wire sensor fences* are similar to fence-disturbance sensors except that instead of attaching the sensors to a loose fence fabric, the sensors are attached to a wire that is stretched tightly across the fence. These types of systems are designed to detect changes in the tension of the wire rather than vibrations in the fence fabric. Taut-wire sensor fences can be installed over existing fences, or as stand-alone fence systems.

*Electric field or capacitance sensors* detect changes in capacitive coupling between wires that are attached to, but electrically isolated from, the fence. As opposed to other fence-associated intrusion sensors, both electric field and capacitance sensors generate an electric field that radiates out from the fence line, resulting in an expanded zone of protection relative to other fence-associated sensors, and allowing the sensor to detect an intruders' presence before they arrive at the fence line. Note: proper spacing is necessary during installation of the electric field sensor to detect a would-be intruder from slipping between largely spaced wires.

- (3) **Freestanding Sensors**—These sensors, which include active infrared, passive infrared, bistatic microwave, monostatic microwave, dual-technology, and video motion detection (VMD) sensors, consist of individual sensor units or components that can be set up in a variety of configurations to meet a user's needs. They are installed above-ground, and depending on how they are oriented relative to each other, they can be used to establish a protected perimeter or a protected space. More details on each of these sensor types are provided below.

*Active infrared sensors* transmit infrared energy into the protected space, and monitor for changes in this energy caused by intruders entering that space. In a typical application, an infrared light beam is transmitted from a transmitter unit to a receiver unit. If an intruder crosses the beam, the beam is blocked, and the receiver

unit detects a change in the amount of light received, triggering an alarm. Different sensors can see single- and multiple-beam arrays. Single-beam infrared sensors transmit a single infrared beam. In contrast, multiple-beam infrared sensors transmit two or more beams parallel to each other. This multiple-beam sensor arrangement creates an infrared “fence.”

*Passive infrared (PIR) sensors* monitor the ambient infrared energy in a protected area and evaluate changes in that ambient energy that may be caused by intruders moving through the protected area. Detection ranges can exceed 100 yards on cold days with size and distance limitations dependent upon the background temperature. PIR sensors generate a nonuniform detection pattern (or “curtain”) that has areas (or “zones”) of more sensitivity and areas of less sensitivity. The specific shape of the protected area is determined by the detector’s lenses. The general shape common to many detection patterns is a series of long “fingers” emanating from the PIR and spreading in various directions. When intruders enter the detection area, the PIR sensor detects differences in temperature due to the intruder’s body heat and triggers an alarm. While the PIR leaves unprotected areas between its fingers, an intruder would be detected if he passed from a non-protected area to a protected area.

*Microwave sensors* detect changes in received energy generated by the motion of an intruder entering into a protected area. Monostatic microwave sensors incorporate transmitter and a receiver in one unit, while bistatic sensors separate the transmitter and the receiver into different units. Monostatic sensors are limited to a coverage area of 400 feet, while bistatic sensors can cover an area up to 1,500 feet. For bistatic sensors, a zone of no detection exists in the first few feet in front of the antennas. This distance from the antennas to the point at which the intruder is first detected is known as the offset distance. Due to this offset distance, antennas must be configured so that they overlap one another (as opposed to being adjacent to each other), thereby creating long perimeters with a continuous line of detection.

*Dual-technology sensors* consist of two different sensor technologies incorporated together into one sensor unit. For example, a dual-technology sensor could consist of a passive infrared detector and a monostatic microwave sensor integrated into the same sensor unit.

*Video motion detection (VMD) sensors* monitor video images from a protected area for changes in the images. Video cameras are used to detect unauthorized intrusion into the protected area by comparing the most recent image against a previously established one. Cameras can be installed on towers or other tall structures so that they can monitor a large area.

## **Fences**

A fence is a physical barrier that can be set up around the perimeter of an asset. Fences often consist of individual pieces (such as individual pickets in a wooden fence, or individual sections of a wrought iron fence) that are fastened together. Individual sections of the fence are fastened together using posts, which are sunk into the ground to provide stability and strength for the sections of the fence hung between them. Gates are installed between individual sections of the fence to allow access inside the fenced area.

Many fences are used as decorative architectural features to separate physical spaces for each other. They may also be used to physically mark the location of a boundary (such as a fence installed along a property line). However, a fence can also serve as an effective means for physically delaying intruders from gaining access to a financial service sector asset. For example, many utilities install fences around their primary facilities, around remote pump stations, or around hazardous petrochemical materials storage areas or sensitive areas within a facility. Access to the area can be controlled through security at gates or doors through the fence (e.g., by posting a guard at the gate or by locking it). In order to gain access to the asset, unauthorized persons could have to go either around or through the fence.

Fences are often compared with walls when determining the appropriate system for perimeter security. While both fences and walls can provide adequate perimeter security, fences are often easier and less expensive to install than walls. However, they do not usually provide the same physical strength that walls do. In addition, many types of fences have gaps between the individual pieces that make up the fence (i.e., the spaces between chain links in a chain link fence or the space between pickets in a picket fence). Thus, many types of fences allow the interior of the fenced area to be seen. This may allow intruders to gather important information about the locations or defenses of vulnerable areas within the facility.

There are numerous types of materials used to construct fences, including chain link iron, aluminum, wood, or wire. Some types of fences, such as split rails or pickets, may not be appropriate for security purposes because they are traditionally low fences, and they are not physically strong. Potential intruders may be able to easily defeat these fences either by jumping or by climbing over them or by breaking through them. For example, the rails in a split fence may be able to be broken easily.

Important security attributes of a fence include the height to which it can be constructed, the strength of the material comprising the fence, the method and strength of attaching the individual sections of the fence together at the posts and the fence's ability to restrict the view of the assets inside the fence. Additional considerations should include the ease of installing the fence and the ease of removing and reusing sections of the fence. Table 10.10 provides

**Table 10.10 Comparison of Different Fence Types**

<i>Specifications</i>	<i>Chain Link</i>	<i>Iron</i>	<i>Wire (Wirewall)</i>	<i>Wood</i>
Height limitations	12'	12'	12'	8'
Strength	Medium	High	High	Low
Installation requirements	Low	High	High	Low
Ability to remove/reuse	Low	High	Low	High
Ability to replace/repair	Medium	High	Low	High

Source: USEPA, 2005.

a comparison of the important security and usability features of various fence types.

Some fences can include additional measures to delay, or even detect, potential intruders. Such measures may include the addition of barbed wire, razor wire, or other deterrents at the top of the fence. Barbed wire is sometimes employed at the base of fences as well. This can impede a would-be intruder's progress in even reaching the fence. Fences may also be fitted with security cameras to provide visual surveillance of the perimeter. Finally, some facilities have installed motion sensors along their fences to detect movement on the fence. Several manufacturers have combined these multiple perimeter security features into one product and offer alarms, and other security features.

The correct implementation of a fence can make it a much more effective security measure. Security experts recommend the following when a facility constructs a fence:

The fence should be at least 7 to 9 feet high.

- Any outriggers, such as barbed wire, that are affixed on top of the fence should be angled out and away from the facility, and not in toward the facility. This will make climbing the fence more difficult and will prevent ladders from being placed against the fence.
- Other types of hardware can increase the security of the fence. This can include installing concertina wire along the fence (this can be done in front of the fence or at the top of the fence), or adding intrusion sensors, camera, or other hardware to the fence.
- All undergrowth should be cleared for several feet (typically 6 feet) on both sides of the fence. This will allow for a clearer view of the fence by any patrols in the area.
- Any trees with limbs or branches hanging over the fence should be trimmed so that intruders cannot use them to go over the fence. Also, it should be noted that fallen trees can damage fences, and so management of trees around the fence can be important. This can be especially important in areas where fence goes through a remote area.
- Fences that do not block the view from outside the fence to inside the fence allow patrols to see inside the fence without having to enter the facility.

- “No Trespassing” signs posted along fence can be a valuable tool in prosecuting any intruders who claim that the fence was broken and that they did not enter through the fence illegally. Adding signs that highlight the local ordinances against trespassing can further persuade simple troublemakers for illegally jumping/climbing the fence. Electrical substation and other electrical component installations should have clearly visible signage warning of HIGH VOLTAGE and the dangers of electrical shock.

### *Films for Glass Shatter Protection*

Many financial services sector entities have numerous windows on the outside of buildings, in doors, and in interior offices. In addition, many facilities have glass doors or other glass structures, such as glass walls or display cases. These glass objects are potentially vulnerable to shattering when heavy objects are thrown or launched at them, when explosions occur near them, or when there are high winds (for exterior glass). If the glass is shattered, intruders may potentially enter an area. In addition, shattered glass projected into a room from an explosion or from an object being thrown through a door or window can injure and potentially incapacitate personnel in the room. Materials that prevent glass from shattering can help to maintain the integrity of the door, window, or other glass object, and can delay an intruder from gaining access. These materials can also prevent flying glass and thus reduce potential injuries.

Materials designed to prevent glass from shattering include specialized films and coatings. These materials can be applied to existing glass objects to improve their strength and their ability to resist shattering. The films have been tested against many scenarios that could result in glass breakage, including penetration by blunt objects, bullets, high winds, and simulated explosions. Thus, the films are tested against both simulated weather scenarios (which could include both the high winds themselves and the force of objects blown into the glass) and more criminal/terrorist scenarios where the glass is subject to explosives or bullets. Many vendors provide information on the results of these types of tests, and thus potential users can compare different product lines to determine which products best suit their needs.

The primary attributes of films for shatter protection are as follows:

- The materials from which the film is made;
- The adhesive that bonds the film to the glass surface;
- The thickness of the film.

Standard glass safety films are designed from high strength polyester. Polyester provides both strength and elasticity, which is important in absorbing the impact of an object, spreading the force of the impact over the entire film, and resisting tearing. The polyester is also designed to be resistant to



scratching, which can result when films are cleaned with abrasives or other industrial cleaners.

The bonding adhesive is important in ensuring that the film does not tear away from the glass surface. This can be especially important when the glass is broken, so that the film does not peel off the glass and allow it to shatter. In addition, films applied to exterior windows can be subject to high concentrations of UV light, which can break down bonding materials.

Film thickness is measured in gauge or mils. According to test results reported by several manufacturers, film thickness appears to affect resistance to penetration/tearing, with thicker films being more resistant to penetration and tearing. However, the appreciation of a thicker film did not decrease glass fragmentation.

Many manufacturers offer films in different thicknesses. The “standard” film is usually one 4 mil layer; thicker films are typically composed of several layers of the standard 4 mil sheet. However, newer technologies have allowed the polyester to be “microlayered” to produce a stronger film without significantly increasing its thickness. In this microlayering process, each laminate film is composed of multiple micro-thin layers of polyester woven together at an alternating angle. This provides increased strength for the film, while maintaining the flexibility and thin profile of one film layer.

As described above, many vendors test their products in various scenarios that would lead to glass shattering, including simulated bomb blasts and simulation of the glass being struck by wind-blown debris. Some manufacturers refer to the Government Services Administration standard for bomb blasts, which require resistance to tearing for a 4 PSI blast. Other manufacturers use other measures and test for resistance to tearing. Many of these tests are not “standard,” in that no standard testing or reporting methods have been adopted by any of the accepted standards-setting institutions. However, many of the vendors publish the procedure and the results of these tests on their websites, and this may allow users to evaluate the protectiveness of these films. For example, several vendors evaluate the “protectiveness” of their films and the “hazard” resulting from blasts near windows with and without protective films. Protectiveness is usually evaluated based on the percentage of glass ejected from the window, and the height at which that ejected glass travels during the blast (e.g., if the blasted glass tends to project upward in to a room—potentially toward people’s faces—it is a higher hazard than if it is blown downward into the room toward people’s feet). There are some standard measures of glass breakage. For example, several vendors indicated that their products exceed the American Society for Testing and Materials (ASTM) standard 64Z-95 “Standard Test Method for glazing and Glazing Systems Subject to Air Blast Loadings.” Vendors often compare the results of some sort of penetration or force test, ballistic tests, or simulated explosions with unprotected glass versus glass onto which their films have been applied. Results generally show that

applying films to the glass surfaces reduces breakage/penetration of the glass and can reduce the amount and direction of glass ejected from the frame. This in turn reduces the hazard from flying glass.

In addition to these types of tests, many vendors conduct standard physical tests on their products, such as tests for tensile strength and peel strength. Tensile strength indicates the strength per area of material, while the peel strength indicates the force it would take to peel the product from the glass surface. Several vendors indicate that their products exceed American National Standards Institute (ANSI) standard Z97.1 for tensile strength and adhesion.

Vendors typically have a warranty against peeling or other forms of deterioration of their products. However, the warranty requires that the films be installed by manufacturer-certified technicians to ensure that they are applied correctly and therefore that the warranty is in effect. Warranties from different manufacturers may vary. Some may cover the cost of replacing the material only, while others include material plus installation. Because installation costs are significantly greater than material costs, different warranties may represent large difference in potential costs.

### *Fire Hydrant Locks*

Fire hydrants are installed at strategic locations throughout a community's water distribution system to supply water for firefighting. However, because there are many hydrants in a system and they are often located in residential neighborhood, industrial districts, and other areas where they cannot be easily observed and/or guarded, they are potentially vulnerable to unauthorized access. Many municipalities, states, and EPA regions have recognized this potential vulnerability and have instituted programs to lock hydrants. For example, EPA Region 1 has included locking hydrants as number 7 on its "Drinking Water Security and Emergency Preparedness" Top Ten List for small groundwater suppliers.

A "hydrant lock" is a physical security device designed to prevent unauthorized access to the water supply through a hydrant. They can also ensure water and water pressure availability to fire fighters and prevent water theft and associated lost water revenue. These locks have been successfully used in numerous municipalities and in various climates and weather conditions.

Fire hydrant locks are basically steel covers or caps that are locked in place over the operating nut of a fire hydrant. The lock prevents unauthorized persons from accessing the operating nut and opening the fire hydrant valve. The lock also makes it more difficult to remove the bolts from the hydrant and access the system that way. Finally, hydrant locks shield the valve from being broken off. Should a vandal attempt to breach the hydrant lock by force and succeed in breaking the hydrant lock, the vandal will only succeed in bending the operating valve. If the hydrant's operating valve is

bent, the hydrant will not be operational, but the water asset remains protected and inaccessible to vandals. However, the entire hydrant will need to be replaced.

Hydrant locks are designed so that the hydrants can be operated by special “key wrenches” without removing the lock. These specialized wrenches are generally distributed to the fire department, public works department, and other authorized persons so that they can access the hydrants as needed. An inventory of wrenches and their serial numbers is generally kept by a municipality so that the location of all wrenches is known. These operating key wrenches may only be purchased by registered lock owners.

The most important features of hydrant are their strength and the security of their locking systems. The locks must be strong so that they cannot be broken off. Hydrant locks are constructed from stainless or alloyed steel. Stainless steel locks are stronger and are ideal for all climates; however, they are more expensive than alloy locks. The locking mechanisms for each fire hydrant locking system ensure that the hydrant can only be operated by authorized personnel who have the specialized key to work the hydrant.

### *Hatch Security*

A hatch is basically a door that is installed on a horizontal plane (such as in a floor, a paved lot, or a ceiling), instead of on a vertical plane (such as in a building wall). Hatches are usually used to provide access to assets that are either located underground (such as hatches to basements or underground vaults and storage areas) or to assets located above ceilings (such as emergency roof exits). At chemical industrial facilities, hatches are typically used to provide access to underground vaults containing pumps, meter chambers, valves, or piping, or to the interior of chemical tanks or covered water reservoirs. Securing a hatch by locking it or upgrading materials to give the hatch added strength can help to delay unauthorized access to any asset behind the hatch.

Like all doors, a hatch consists of a frame anchored to the horizontal structure, a door or doors, hinges connecting the door/doors to the frame, and a latching or locking mechanism that keeps the hatch door/doors closed.

It should be noted that improving hatch security is straightforward, and that hatches with upgraded security features can be installed new or they can be retrofit for existing applications. Depending on the application, the primary security-related attributes of a hatch are the strength of the door and frame, its resistance to the elements and corrosion, its ability to be sealed against water or gas, and its locking features.

Hatches must be both strong and lightweight so that they can withstand typical static loads (such as people or vehicles walking or driving over them) while still being easy to open.

In addition, because hatches are typically installed at outdoor locations, they are usually designed from corrosion-resistant metal that can withstand the elements. Therefore, hatches are typically constructed from high gauge steel or lightweight aluminum.

Aluminum is typically the material of choice for hatches because it is lightweight and more corrosion resistant relative to steel. Aluminum is not as rigid as steel, so aluminum hatch doors may be reinforced with aluminum stiffeners to provide extra strength and rigidity. The doors are usually constructed from single or double layers (or “leaves”) of material. Single-leaf designs are standard for smaller hatches, while double leaf designs are required for larger hatches. In addition, aluminum products do not require painting. This is reflected in the warranties available with different products. Product warranties range from ten years to lifetime.

Steel is heavier per square foot than aluminum, and thus steel hatches will be heavier and more difficult to open than aluminum hatches of the same size. However, heavy steel hatch doors may have spring-loaded, hydraulic, or gas openers or other specialized features that help in opening the hatch and in keeping it open.

Many hatches are installed in outdoor areas, often in roadways or pedestrian areas. Therefore, the hatch installed for any given application must be designed to withstand the expected load at that location. Hatches are typically solid to withstand either pedestrian or vehicle loading. Pedestrian loading hatches are typically designed to withstand either 150 or 300 pounds per square feet (psf) of loading. The vehicle loading standard is the American Association of State Highway and Transportation Officials (AASHTO) H-20 wheel loading standard of 16,000 lb over an 8 inch by 20-inch area. It should be noted that these design parameters are for static loads and not dynamic loads; thus, the loading capabilities may not reflect potential resistance to other types of loads that may be more typical of an intentional threat, such as repeated blows from a sledge hammer or pressure generated by bomb blasts or bullets.

The typical design for a watertight hatch includes a channel frame that directs water away from the hatch. This can be especially important in a hatch on a storage tank because this will prevent liquid contaminants from being dumped on the hatch and leaking through into the interior. Hatches can also be constructed with gasket seals that are air-, odor-, and gas-tight.

Typically, hatches for pedestrian loading applications have hinges located on the exterior of the hatch, while hatches designed for H-20 loads have hinges located in the interior of the hatch. Hinges located on the exterior of the hatch may be able to be removed; thereby allowing intruders to remove the hatch door and access the asset behind the hatch. Therefore, installing

H-20 hatches even for applications which do not require H-20 loading levels may increase security, because intruders will not be able to tamper with the hinges and circumvent the hatch this way.

In addition to the location of the hinges, stock hinges can be replaced with heavy duty or security hinges that are more resistant to tampering.

The hatch locking mechanism is perhaps the most important part of hatch security. There are a number of locks that can be implemented for hatches, including:

- Slam locks (internal locks that are located within the hatch frame)
- Recessed cylinder locks
- Bolt locks
- Padlocks

### *Ladder Access Control*

Financial services sector facilities have a number of assets that are raised above ground level, including electrical substations, transmitting stations, raised conduit systems, and roof access points into buildings. In addition, communications equipment, antennae, or other electronic devices may be located on the top of these raised assets. Typically, these assets are reached by ladders that are permanently anchored to the asset. For example, raised petrochemical/water tanks typically are accessed by ladders that are bolted to one of the legs of the tank. Controlling access to these raised assets by controlling access to the ladder can increase security at a financial services sector facility.

A typical ladder access control system consists of some type of cover that is locked or secured over the ladder. The cover can be a casing that surrounds most of the ladder, or a door or shield that covers only part of the ladder. In either case, several rungs of the ladder (the number of rungs depends on the size of the cover) are made inaccessible by the cover, and these rungs can only be accessed by opening or removing the cover. The cover is locked so that only authorized personnel can open or remove it and use the ladder. Ladder access controls are usually installed at several feet above ground level, and they usually extend several feet up the ladder so that they cannot be circumvented by someone accessing the ladder above the control system.

The important features of ladder access control are the size and strength of the cover and its ability to lock or otherwise be secured from unauthorized access.

The covers are constructed from aluminum or some type of steel. This should provide adequate protection from being pierced or cut through. The metals are corrosion resistant so that they will not corrode or become fragile from extreme

weather conditions in outdoor applications. The bolts used to install each of these systems are galvanized steel. In addition, the bolts for each cover are installed on the inside of the unit so they cannot be removed from the outside.

### *Locks*

A lock is a type of physical security device that can be used to delay or prevent a door, a gate, a window, a manhole, a filing cabinet drawer, or some other physical feature from being opened, moved, or operated. Locks typically operate by connecting two pieces together—such as by connecting a door to a door jamb or a manhole to its casement. Every lock has two modes—engaged (or “locked”), and disengaged (or “opened”). When a lock is disengaged, the asset on which the lock is installed can be accessed by anyone, but when the lock is engaged, only access to the locked asset.

Before discussing locks and their applicability it is important to discuss key control. Based on our experience, many financial services sector facilities (and others) have no idea how many keys for various site/equipment locks have been issued to employees over the years. Many facilities simply issue keys to employees at hiring with no accountability for the keys upon the employee’s departure. Needless to say this is not good security policy. You can have the best made locks available installed throughout your facilities but if you do not have proper key control, you do not have proper security.

Locks are excellent security features because they have been designed to function in many ways and to work on many different types of assets. Locks can also provide different levels of security depending on how they are designed and implemented. The security provided by a lock is dependent on several factors, including its ability to withstand physical damage (i.e., can it be cut off, broken, or otherwise physically disabled) as well as its requirements for supervision or operation (i.e., combinations may need to be changed frequently so that they are not compromised and the locks remain secure). While there is no single definition of the “security” of a lock, locks are often described as minimum, medium, or maximum security. Minimum security locks are those that can be easily disengaged (or “picked”) without the correct key or code, or those that can be disabled easily (such as small padlocks that can be cut with bolt cutters). Higher security locks are more complex and thus are more difficult to pick, or are sturdier and more resistant to physical damage.

Many locks, such as many door locks, only need to be unlocked from one side. For example, most door locks need a key to be unlocked only from the outside. A person opens such devices, called single-cylinder locks, from the inside by pushing a button or by turning a knob or handle. Double-cylinder locks require a key to be locked or unlocked from both sides.

### *Manhole Intrusion Sensors*

Manholes are found at some financial services sector sites. Manholes are designed to provide access to the underground utilities, meter vaults, petrochemical pumping rooms, and so on, and therefore they are potential entry points to a system. Because many utilities run under other infrastructure (roads, buildings), manholes also provide potential access points to critical infrastructure as well as petrochemical process assets. In addition, because the portion of the system to which manholes provide entry is primarily located underground, access to a system through a manhole increases the chance that an intruder will not be seen. Therefore, protecting manholes can be a critical component of guarding an entire plant site and a surrounding community.

There are multiple methods for protecting manholes, including preventing unauthorized personnel from physically accessing the manhole, and detecting attempts at unauthorized access to the manhole.

A manhole intrusion sensor is a physical security device designed to detect unauthorized access to the facility through a manhole. Monitoring a manhole that provides access to a chemical plant or processing system can mitigate two distinct types of threats. First, monitoring a manhole may detect access of unauthorized personnel to chemical systems or assets through the manhole. Secondly, monitoring manholes may also allow the detection of intruders attempting to place explosive or other destructive (WMD) devices into the petrochemical system.

Several different technologies have been used to develop manhole intrusion sensors, including mechanical systems, magnetic systems, and fiber-optic and infrared sensors. Some of these intrusion sensors have been specifically designed for manholes, while others consist of standard, off-the-shelf intrusion sensors that have been implemented in a system specifically designed for application in a manhole.

### *Manhole Locks*

A “manhole lock” is a physical security device designed to delay unauthorized access to the financial services sector facility or system through a manhole.

### *Passive Security Barriers*

One of the most basic threats facing any facility is from intruders accessing the facility with the intention of causing damage to its assets. These threats may include intruders actually entering the facility, as well as intruders attacking the facility from outside without actually entering it (i.e., detonating bomb near enough to the facility to cause damage within its boundaries).

Security barriers are one of the most effective ways to counter the threat of intruders accessing a facility or the facility perimeter. Security barriers are large, heavy structures that are used to control access through a perimeter by either vehicles or personnel. They can be used in many different ways depending on how/where they are located at the facility. For example, security barriers can be used on or along driveways or roads to direct traffic to a checkpoint (i.e., a facility may install jersey barriers in a road to direct traffic in certain direction). Other types of security barriers (crash beams, gates) can be installed at the checkpoint so that guards can regulate which vehicles can access the facility. Finally, other security barriers (i.e., bollards or security planters) can be used along the facility perimeter to establish a protective buffer area between the facility and approaching vehicles. Establishing such a protective buffer can help in mitigating the effects of the type of bomb blast described above, both by potentially absorbing some of the blast and also by increasing the “standoff” distance between the blast and the facility (the force of an explosion is reduced as the shock wave travels further from the source, and thus the further the explosion is from the target, the less effective it will be in damaging the target).

Security barriers can be either “active” or “passive.” “Active” barriers, which include gates, retractable bollards, wedge barriers, and crash barriers, are readily movable, and thus they are typically used in areas where they must be moved often to allow vehicles to pass—such as in roadways at entrances and exits to a facility. In contrast to active security barriers, “passive” security barriers, which include jersey barriers, bollards, and security planters, are not designed to be moved on a regular basis, and thus they are typically used in areas where access is not required or allowed—such as along building perimeters or in traffic control areas. Passive security barriers are typically large, heavy structures that are usually several feet high, and they are designed so that even heavy-duty vehicles cannot go over or through them. Therefore, they can be placed in a roadway parallel to the flow of traffic so that they direct traffic in a certain direction (such as to a guardhouse, a gate, or some other sort of checkpoint), or perpendicular to traffic such that they prevent a vehicle from using a road or approaching a building or area.

### *Security for Doorways-Side Hinged Doors*

Doorways are the main access points to a facility or to rooms within a building. They are used on the exterior or in the interior of buildings to provide privacy and security for the areas behind them. Different types of doorway security systems may be installed in different doorways depending on the needs or requirements of the buildings or rooms. For example, exterior doorways tend to have heavier doors to withstand the elements and to provide some security to the entrance of the building. Interior doorways in office



areas may have lighter doors that may be primarily designed to provide privacy rather than security. Therefore, these doors may be made of glass or lightweight wood. Doorways in industrial areas may have sturdier doors than other interior doorways and may be designed to provide protection or security for areas behind the doorway. For example, fireproof doors may be installed in chemical storage areas or in other areas where there is a danger of fire.

Because they are the main entries into a facility or a room, doorways are often prime targets for unauthorized entry into a facility or an asset. Therefore, securing doorways may be a major step in providing security at a facility.

A doorway includes four main components:

- The door, which blocks the entrance. The primary threat to the actual door is breaking or piercing through the door. Therefore, the primary security features of doors are their strength and resistance to various physical threats, such as fire or explosions.
- The door frame, which connects the door to the wall. The primary threat to a door frame is that the door can be pried away from the frame. Therefore, the primary security feature of a door frame is its resistance to prying.
- The hinges, which connect the door to the door frame. The primary threat to door hinges is that they can be removed or broken, which will allow intruders to remove the entire door. Therefore, security hinges are designed to be resistant to breaking. They may also be designed to minimize the threat of removal from the door.
- The lock, which connects the door to the door frame. Use of the lock is controlled through various security features, such as keys, combinations, such that only authorized personnel can open the lock and go through the door. Locks may also incorporate other security features, such as software or other systems to track overall use of the door or to track individuals using the door, and so on.

Each of these components is integral in providing security for a doorway, and upgrading the security of only one of these components while leaving the other components unprotected may not increase the overall security of the doorway. For example, many facilities upgrade door locks as a basic step in increasing the security of a facility. However, if the facilities do not also focus on increasing security for the door hinges or the door frame, the door may remain vulnerable to being removed from its frame, thereby defeating the increased security of the door lock.

The primary attribute for the security of a door is its strength. Many security doors are 4- to 20-gauge hollow metal doors consisting of steel plates over a hollow cavity reinforced with steel stiffeners to give the door extra stiffness and rigidity. This increases resistance to blunt force used to try to penetrate through the door. The space between the stiffeners may be filled with specialized materials to provide fire-, blast-, or bullet resistance to the door.

The Windows and Doors Manufacturers Association have developed a series of performance attributes for doors. These include:

- Structural resistance
- Forced entry resistance
- Hinge-style screw resistance
- Split resistance
- Hinge resistance
- Security rating
- Fire resistance
- Bullet resistance
- Blast resistance

The first five bullets provide information on a door's resistance to standard physical breaking and prying attacks. These tests are used to evaluate the strength of the door and the resistance of the hinges and the frame in a standardized way. For example, the Rack Load Test simulates a prying attack on a corner of the door. A test panel is restrained at one end, and a third corner is supported. Loads are applied and measured at the fourth corner. The Door Impact Test simulates a battering attack on a door and frame using impacts of 200 foot pounds by a steel pendulum. The door must remain fully operable after the test. It should be noted that door glazing is also rated for resistance to shattering, and so on. Manufacturers will be able to provide security ratings for these features of a door as well.

Door frames are an integral part of doorway security because they anchor the door to the wall. Door frames are typically constructed from wood or steel, and they are installed such that they extend for several inches over the doorway that has been cut into the wall. For added security, frames can be designed to have varying degrees of overlap with, or wrapping over, the underlying wall. This can make prying the frame from the wall more difficult. A frame formed from a continuous piece of metal (as opposed to a frame constructed from individual metal pieces) will prevent prying between pieces of the frame.

Many security doors can be retrofit into existing frames; that is, many security door installations including replacing the door frame as well as the door itself. For example, bullet resistance per UL 752 requires resistance of the door and frame assembly, and thus replacing the door only would not meet UL 752 requirements.

### *Valve Lockout Devices*

Valves are utilized as control elements in fuel oil/natural gas and petrochemical process piping networks. They regulate the flow of both liquids and gases by opening, closing, or obstructing a flow passageway. Valves are typically

located where flow control is necessary. They can be located in-line or at pipeline and tank entrance and exit points. They can serve multiple purposes in a process pipe network, including:

- Redirecting and throttling flow
- Preventing backflow
- Shutting off flow to a pipeline or tank (for isolation purposes)
- Releasing pressure
- Draining extraneous liquid from pipelines or tanks
- Introducing chemicals into the process network
- As access points for sampling process water

Valves may be located either aboveground or belowground. It is critical to provide protection against valve tampering. For example, tampering with a pressure relief valve could result in a pressure buildup and potential explosion in the piping network. On a larger scale, addition of a contaminant or non-compatible chemical substance to the chemical processing system through an unprotected valve could result in the catastrophic release of that contaminant to the general population.

Different security products are available to protect aboveground versus below ground valves. For example, valve lockout devices can be purchased to protect valves and valve controls located aboveground. Vaults containing underground valves can be locked to prevent access to these valves.

As described above, a lockout device can be used as a security measure to prevent unauthorized access to aboveground valves located within petrochemical processing systems. Valve lockout devices are locks that are specially designed to fit over valves and valve handles to control their ability to be turned or seated. These devices can be used to lock the valve into the desired position. Once the valve is locked, it cannot be turned unless the locking device is unlocked or removed by an authorized individual.

Various valve lockout options are available for industrial use, including:

- Cable lockouts
- Padlocked chains/cables
- Valve-specific lockouts

Many of these lockout devices are not specifically designed for use in financial services sector industry (i.e., chains, padlocks) but are available from a local hardware store or manufacturer specializing in safety equipment. Other lockout devices (e.g., valve-specific lockouts or valve box-locks) are more specialized and must be purchased from safety or valve-related equipment vendors.

The three most common types of valves for which lockout devices are available are gate, ball, and butterfly valves. Each is described in more detail below.

- **Gate Valve Lockouts**—Gate valve lockouts are designed to fit over the operating hand wheel of the gate valve to prevent it from being turned. The lockout is secured in place with a padlock. Two types of gate valve lockouts are available: diameter specific and adjustable. Diameter-specific lockouts are available for handles ranging from 1 inch to 13 inch in diameter. Adjustable gate valve lockouts can be adjusted to fit any handle ranging from 1 inch to 6+ inch in diameter.
- **Ball Valve Lockouts**—There are several different configurations available to lock out ball valves, all of which are designed to prevent rotation of the valve handle. The three major configurations available are a wedge shape for 1 inch to 3 inch valves, a lockout that completely covers 3/8 inch to 8 inch ball valve handles, and a universal lockout that can be applied to quarter-turn valves of varying sizes and geometric handle dimensions. All three types of ball valve lockouts can be installed by sliding the lockout device over the ball valve handle and securing it with a padlock.
- **Butterfly Valve Lockouts**—The butterfly valve lockout functions in a similar manner to the ball valve lockout. The polypropylene lockout device is placed over the valve handle and secured with a padlock. This type of lockout has been commonly used in the bottling industry.

A major difference between valve-specific lockout devices and the padlocked chain or cable lockouts discussed earlier is that they do not need to be secured to an anchoring device in the floor or the piping system. In addition, valve-specific lockouts eliminate potential tripping or access hazards that may be caused by chains or cable lockouts applied to valves located near walkways or frequently maintained equipment.

Valve-specific lockout devices are available in a variety of colors, which can be useful in distinguishing different valves. For example, different colored lockouts can be used to distinguish the type of liquid passing through the valve (i.e., treated, untreated, potable, petrochemical) or to identify the party responsible for maintaining the lockout. Implementing a system of different colored locks on operating valves can increase system security by reducing the likelihood of an operator inadvertently opening the wrong valve and causing a problem in the system.

### *Security For Vents*

Vents are installed in some aboveground financial services sector storage areas to allow safe venting of off-gases. The specific vent design for any given application will vary depending on the design of the chemical storage

vessel. However, every vent consists of an open air connection between the storage container and the outside environment. Although these air exchange vents are an integral part of covered or underground chemical storage containers, they also represent a potential security threat. Improving vent security by making the vents tamper resistant or by adding other security features, such as security screens or security covers can enhance the security of the entire petrochemical processing system.

Many municipalities already have specifications for vent security at their local chemical industrial assets. These specifications typically include the following requirements:

- Vent openings are to be angled down or shielded to minimize the entrance of surface and/or rainwater into the vent through the opening.
- Vent designs are to include features to exclude insects, birds, animals, and dust.
- Corrosion-resistant materials are to be used to construct the vents.

### *Visual Surveillance Monitoring*

Visual surveillance is used to detect threats through continuous observation of important or vulnerable areas of an asset. The observations can also be recorded for later review or use (e.g., in court proceedings). Visual surveillance system can be used to monitor various parts of production, distribution, or pumping/compressing systems, including the perimeter of a facility, outlying pumping stations, or entry or access points into specific buildings. These systems are also useful in recording individuals who enter or leave a facility, thereby helping to identify unauthorized access. Images can be transmitted live to a monitoring station, where they can be monitored in real time, or they can be recorded and reviewed later. Many financial services sector facilities have found that a combination of electronic surveillance and security guards provides an effective means of facility security.

Visual surveillance is provided through a closed-circuit television (CCTV) system, in which the capture, transmission, and reception of an image is localized within a closed "circuit." This is different than other broadcast images, such as over-the-air television, which is broadcast over the air to any receiver within range.

At a minimum, a CCTV system consists of:

- one or more cameras;
- a monitor for viewing the images;
- a system for transmitting the images from the camera to the monitor.

Specific attributes and features of camera systems, lenses, and lighting systems are presented in table 10.11.

**Table 10.11 Attributes of Camera, Lenses, and Lighting Systems**

<i>Attribute</i>	<i>Discussion</i>
<i>Camera Systems</i>	
Camera type	<p>Major factors in choosing the correct camera are the resolution of the image required and lighting of the area to be viewed.</p> <ul style="list-style-type: none"> <li>• <b>Solid state</b> (including charge coupled devices, charge priming device, charge injection device, and metal oxide substrate)—these cameras are becoming predominant in the marketplace because of their high resolution and their elimination of problems inherent in tube cameras.</li> <li>• <b>Thermal</b>—These cameras are designed for night vision. They require no light and use differences in temperature between objects in the field of view to produce a video image. Resolution is low compared to other cameras, and the technology is currently expensive relative to other technologies.</li> <li>• <b>Tube</b>—These cameras can provide high resolution burn out and must be replaced after one to two years. In addition, tube performance can degrade over time. Finally, tube cameras are prone to burn images in the tube replacement.</li> </ul>
Resolution (the ability to see fine details)	User must determine the amount of resolution required depending on the level of detail required for threat determination. A high definition focus with a wide field of vision will give an optimal viewing area.
Field of vision width	Cameras are designed to cover a defined field of vision, which is usually defined in degrees. The wider the field of vision, the more area a camera will be able to monitor.
Type of image produced (color, black and white, thermal)	Color images may allow the identification of distinctive markings, while black and white images may provide sharper contrast. Thermal imaging allows the identification of heat sources (such as human beings or other living creatures) from low light environments; however, thermal images are not effective in identifying specific individuals (i.e., for subsequent legal processes).
Pan/Tilt/Zoom (PTZ)	Panning (moving the camera in a horizontal plane), tilting (moving the camera in a vertical plane), and zooming (moving the lens to focus on objects that are at different distances from the camera) allow the camera to follow a moving object. Different systems allow these functions to be controlled manually or automatically. Factors to be considered in PTZ cameras are the degree of coverage for pan and tilt function and the power of the zoom lens.
<i>Lenses</i>	
Format	Lens format determines the maximum image size to be transmitted.

*(Continued)*

**Table 10.11 Attributes of Camera, Lenses, and Lighting Systems—Continued**

<i>Attribute</i>	<i>Discussion</i>
Focal length	This is the distance from the lens to the center of the focus. The greater the focal length, the higher the magnification, but the narrower the field of vision.
F number	F number is the ability to gather light. Smaller F numbers may be required for outdoor applications where light cannot be controlled as easily.
Distance and width approximation	The distance and width approximations are used to determine the geometry of the space that can be monitored at the best resolution.
<i>Lighting Systems</i>	
Intensity	Light intensity must be great enough for the camera type to produce sharp images. Light can be generated from natural or artificial sources. Artificial sources can be controlled to produce the amount and distribution of light required for a given camera and lens.
Evenness	Light must be distributed evenly over the field of view so that there are no darker or shadowy areas. If there are lighter versus darker areas, brighter areas may appear washed out (i.e., details cannot be distinguished) while no specific objects can be viewed from darker areas.
Location	Light sources must be located above the camera so that light does not shine directly into the camera.

Source: USEPA, 2005.

## COMMUNICATION INTEGRATION

In this section, those devices necessary for communication and integration of CS sector industrial processing operations, such as electronic controllers, two-way radios, and wireless data communications, are discussed. In regard to security applications, electronic controllers are used to automatically activate equipment (such as lights, surveillance cameras, audible alarms, or locks) when they are triggered. Triggering could be in response to variety of scenarios, including tripping of an alarm or a motion sensor; breaking of a window or a glass door; variation in vibration sensor readings; or simply through input from a timer.

Two-way wireless radios allow two or more users have their radios tuned to the same frequency to communicate instantaneously with each other without the radios being physically lined together with wires or cables.

Wireless data communications devices are used to enable transmission of data between computer systems, without individual components being physically linked together via wires or cables. In financial processing systems, these

devices are often used to link remote monitoring stations or portable computers (i.e., laptops) to computer networks without using physical wiring connections.

## **Electronic Controllers**

An electronic controller is a piece of electronic equipment that receives incoming electric signals and uses preprogrammed logic to generate electronic output signals based on the incoming signals. While electronic controllers can be implemented for any application that involves inputs and outputs (e.g., control of a piece of machinery in a factory), in a security application, these controllers essentially act as the system's "brain," and can respond to specific security-related inputs with preprogrammed output response. These systems combine the control of electronic circuitry with a logic function such that circuits are opened and closed (and thus equipment is turned on and off) through some preprogrammed logic. The basic principle behind the operation of an electrical controller is that it receives electronic inputs from sensors or any device generating an electrical signal (e.g., electrical signals from motion sensors), and then uses its preprogrammed logic to produce electrical outputs (e.g., these outputs could turn on power to a surveillance camera or to an audible alarm). Thus, these systems automatically generate a preprogrammed, logical response to a preprogrammed input scenario.

The three major types of electronic controllers are timers, electromechanical relays, and programmable logic controllers (PLCs), which are often called "digital relays." Each of these types of controller is discussed in more detail below.

Timers use internal signal/inputs (in contrast to externally—generated inputs) and generate electronic output signals at certain times. More specifically, timers control electric current flow to any application to which they are connected, and can turn the current on or off on a schedule prespecified by the user. Typical timer range (amount of time that can be programmed to elapse before the timer activates linked equipment) is from 0.2 seconds to 10 hours, although some of the more advanced timers have ranges of up to 60 hours. Timers are useful in fixed applications that don't require frequent schedule changes. For example, a timer can be used to turn on the lights in a room or building at a certain time every day. Timers are usually connected to their own power supply (usually 120–240 V).

In contrast to timers, which have internal triggers based on a regular schedule, electromechanical relays and PLCs have both external inputs and external outputs. However, PLCs are more flexible and more powerful than are electromechanical relays, and thus this section focuses primarily on PLCs as the predominant technology for security-related electronic control applications.



Electromechanical relays are simple devices that use a magnetic field to control a switch. Voltage applied to the relay's input coil creates a magnetic field, which attracts an internal metal switch. This causes the relay's contacts to touch, closing the switch and completing the electrical circuit. This activates any linked equipment. These types of systems are often used for high voltage applications, such as in some automotive and other manufacturing processes.

## Two-Way Radios

Two-way radios, as discussed here, are limited to a direct unit-to-unit radio communication, either via single unit-to-unit transmission and reception or via multiple handheld units to a base station radio contact and distribution system. Radio frequency spectrum limitations apply to all hand held units, and directed by the FCC. This also distinguishes a hand held unit from a base station or base station unit (such as those used by an amateur (ham) radio operator), which operate under different wave length parameters.

Two-way radios allow a user to contact another user or group of users instantly on the same frequency, and to transmit voice or data without the need for wires. They use "half-duplex" communications; or communication that can be only transmitted or received; it cannot transmit and receive simultaneously. In other words, only one person may talk, while other personnel with radio(s) can only listen. To talk, the user depresses the talk button and speaks into the radio. The audio then transmits the voice wirelessly to the receiving radios. When the speaker has finished speaking and the channel has cleared, users on any of the receiving radios can transmit; either to answer the first transmission or to begin a new conversation. In addition to carrying voice data, many types of wireless radios also allow the transmission of digital data, and these radios may be interfaced with computer networks that can use or track these data. For example, some two-way radios can send information such as GPS data or the ID of the radio. Some two-way radios can also send data through a SCADA system.

Wireless radios broadcast these voice or data communications over the airwaves from the transmitter to the receiver. While this can be an advantage in that the signal emanates in all directions and does not need a direct physical connection to be received at the receiver, it can also make the communications vulnerable to being blocked, intercepted, or otherwise altered. However, security features are available to ensure that the communications are not tampered with.

## Wireless Data Communications

A wireless data communication system consists of two components: a "Wireless Access Point" (WAP), and a "Wireless Network Interface Card"

(sometimes also referred to as a “Client”), which work together to complete the communications link. These wireless systems can link electronic devices, computers, and computer systems together using radio waves, thus eliminating the need for these individual components to be directly connected together through physical wires. While wireless data communications have widespread application in water and wastewater systems, they also have limitations. First, wireless data connections are limited by the distance between components (radio waves scatter over a long distance and cannot be received efficiently, unless special directional antenna are used). Secondly, these devices only function if the individual components are in a direct line of sight with each other, since radio waves are affected by interference from physical obstructions. However, in some cases, repeater units can be used to amplify and retransmit wireless signals to circumvent these problems. The two components of wireless devices are discussed in more detail below.

- (1) WAP: The WAP provides the wireless data communication service. It usually consists of a housing (which is constructed from plastic or metal depending on the environment it will be used in) containing a circuit board; flash memory that holds software; one of two external ports to connect to existing wired networks; a wireless radio transmitter/receiver; and one or more antenna connections. Typically, the WAP requires a one-time user configuration to allow the device to interact with the local area network (LAN). This configuration is usually done via a web-driven software application which is accessed via a computer.
- (2) Wireless Network Interface Card/Client: A wireless card is a piece of hardware that is plugged in to a computer and enables that computer to make a wireless network connection. The card consists of a transmitter, functional circuitry, and a receiver for the wireless signal, all of which work together to enable communication between the computer, its wireless transmitter/receiver, and its antenna connection. Wireless cards are installed in a computer through a variety of connections, including USB Adapters, or Laptop CardBus (PCMCIA) or Desktop Peripheral (PCI) cards. As with the WAP, software is loaded onto the user’s computer, allowing configuration of the card so that it may operate over the wireless network

Two of the primary applications for wireless data communications systems are to enable mobile or remote connections to a LAN and to establish wireless communications links between SCADA remote telemetry units (RTUs) and sensors in the field. Wireless car connections are usually used for LAN access from mobile computers. Wireless cards can also be incorporated into RTUs to allow them to communicate with sensing devices that are located remotely.

## CYBER PROTECTION DEVICES

Various cyber protection devices are currently available for use in protecting CS sector computer systems. These protection devices include antivirus and pest eradication software, firewalls, and network intrusion hardware/software. These products are discussed in the following section.

### Antivirus and Pest Eradication Software

Antivirus programs are designed to detect, delay, and respond to programs or pieces of code that are specifically designed to harm computers. These programs are known as “malware.” Malware can include computer viruses, worms, and Trojan Horse programs (programs that appear to be benign but which have hidden harmful effects).

Pest eradication tools are designed to detect, delay, and respond to “spyware” (strategies that websites use to track user behavior, such as by sending “cookies” to the user’s computer), and hacker tools that track keystrokes (keystroke loggers) or passwords (password crackers).

Viruses and pests can enter a computer system through the Internet or through infected floppy discs or CDs. They can also be placed onto a system by insiders. Some of these programs such as viruses and worms then move within a computer’s drives and files, or between computers if the computers are networked to each other. This malware can deliberately damage files, utilize memory and network capacity, crash application programs, and initiate transmissions of sensitive information from a PC. While the specific mechanisms of these programs differ, they can infect files, and even the basic operating program of the computer firmware/hardware.

The most important features of an antivirus program are its abilities to identify potential malware and to alert a user before infection occurs, as well as its ability to respond to a virus already resident on a system. Most of these programs provide a log so that the user can see what viruses have been detected and where they were detected. After detecting a virus, the antivirus software may delete the virus automatically, or it may prompt the user to delete the virus. Some programs will also fix files or programs damaged by the virus.

Various sources of information are available to inform the general public and computer system operators about new viruses being detected. Since antivirus programs use signatures (or snippets of code or data) to detect the presence of a virus, periodic updates are required to identify new threats. Many antivirus software providers offer free upgrades that are able to detect and respond to the latest viruses.

## Firewalls

A firewall is an electronic barrier designed to keep computer hackers, intruders, or insiders from accessing specific data files and information on a financial services sector's computer network or other electronic/computer systems. Firewalls are operated by evaluating and then filtering information coming through a public network (such as the Internet) into the utility's computer or other electronic system. This evaluation can include identifying the source or destination addresses and ports, and allowing or denying access based on this identification.

There are two methods used by firewalls to limit access to the utility's computers or other electronic systems from the public network:

- The firewall may deny all traffic unless it meets certain criteria.
- The firewall may allow all traffic through unless it meets certain criteria.

A simple example of the first method is to screen requests to ensure that they come from an acceptable (i.e., previously identified) domain name and Internet protocol address. Firewalls may also use more complex rules that analyze the application data to determine if the traffic should be allowed through. For example, the firewall may require user authentication (i.e., use of a password) to access the system. How a firewall determines what traffic to let through depends on which network layer it operates at and how it is configured. Some of the pros and cons of various methods to control traffic flowing in and out of the network are provided in table 10.12.

Firewalls may be a piece of hardware, a software program, or an appliance card that contains both.

Advanced features that can be incorporated into firewalls allow for the tracking of attempts to log on to the LAN system. For example, a report of successful and unsuccessful log in attempts may be generated for the computer specialist to analyze. For systems with mobile users, firewalls allow remote access in to the private network by the use of secure log-on procedures and authentication certificates. Most firewalls have a graphical user interface for managing the firewall.

In addition, new Ethernet firewall cards fit in the slot of an individual computer bundle additional layers of defense (like encryption and permit/deny) for individual computer transmissions to the network interface function. These new cards have only a slightly higher cost than traditional network interface cards.

**Table 10.12 Pros and Cons of Various Firewall Methods for Controlling Network Access**

<i>Method</i>	<i>Description</i>	<i>Pros</i>	<i>Cons</i>
Packet filtering	Incoming and outgoing packets (small chunks of data) are analyzed against a set of filters. Packets that make it through the filters are sent to the requesting system and all others are discarded. There are two types of packet filtering: static (the most common) and dynamic.	Static filtering is relatively inexpensive, and little maintenance is required. It is well suited for closed environments where access to or from multiple addresses is not allowed.	Leaves permanent open holes in the network; allows direct connection to internal hosts by external sources; offers no user authentication, method can be unmanageable in large networks.
Proxy service	Information from the Internet is retrieved by the firewall and then sent to the requesting system and vice versa. In this way, the firewall can limit the information made known to the requesting system, making vulnerabilities less apparent.	Only allows temporary open holes in the network perimeter. Can be used for all types of internal protocol services.	Allows direct connections to internal hosts by external clients; offers no user authentication
Stateful pattern recognition	This method examines and compares the contents of certain key parts of an information packet against a database of acceptable information. Information traveling from inside the firewall to the outside is monitored for specific defining characteristics, and then incoming information is compared to these characteristics. If the comparison yields a reasonable match, the information is allowed through. If not, the information is discarded.	Provides a limited time window to allow pockets of information to be sent; does not allow any direct connections between internal and external hosts; supports user-level authentication.	Slower than packet filtering; does not support all types of connections.

*Source:* USEPA, 2005.

## Network Intrusion Hardware/Software

Network intrusion detection and prevention systems are software- and hardware-based programs designed to detect unauthorized attacks on a computer network system.

While other applications, such as firewalls and antivirus software, share similar objectives with network intrusion systems, network intrusion systems provide a deeper layer of protection beyond the capabilities of these other systems because they evaluate patterns of computer activity rather than specific files.

It is worth noting that attacks may come from either outside or within the system (i.e., from an insider), and that network IDSs may be more applicable for detecting patterns of suspicious activity from inside a facility (i.e., accessing sensitive data) than are other IT solutions.

Network IDSs employ a variety of mechanisms to evaluate potential threats. The types of search and detection mechanisms are dependent upon the level of sophistication of the system. Some of the available detection methods include:

- **Protocol analysis**—Protocol analysis is the process of capturing, decoding, and interpreting electronic traffic. The protocol analysis method of network intrusion detection involves the analysis of data captured during transactions between two or more systems or devices, and the evaluation of these data to identify unusual activity and potential problems. Once a problem is isolated and recorded, problems or potential threats can be linked to pieces of hardware or software. Sophisticated protocol analysis will also provide statistics and trend information on the captured traffic.
- **Traffic anomaly detection**—Traffic anomaly detection identifies potential threatening activity by comparing incoming traffic to “normal” traffic patterns, and identifying deviations. It does this by comparing user characteristics against thresholds and triggers defined by the network administrator. This method is designed to detect attacks that span a number of connections, rather than a single session.
- **Network honeypot**—This method establishes nonexistent services in order to identify potential hackers. A network honeypot impersonates services that don’t exist by sending fake information to people scanning the network. It identifies the attacker when they attempt to connect to the service. There is no reason for legitimate traffic to access these resources because they don’t exist; therefore any attempt to access them constitutes an attack.
- **Anti-intrusion detection system evasion techniques**—These methods are designed to help attackers who may be trying to evade intrusion detection system scanning. They include methods called IP defragmentation, TCP streams reassembly, and deobfuscation.

While these detection systems are automated, they can only indicate patterns of activity and a computer administrator or other experienced individual must interpret activities to determine whether or not they are potentially harmful. Monitoring the logs generated by these systems can be time consuming, and there may be a learning curve to determine a baseline of “normal” traffic patterns from which to distinguish potential suspicious activity.

## REFERENCES AND RECOMMENDED READING

- Department of Homeland Security (DHS). 2009. “National Infrastructure Protection Plan.” <https://www.dhs.gov/cisa/national-infrastructure-protection-plan>.
- Department of Homeland Security (DHS). 2003. “The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.” [https://www.dhs.gov/xlibrary/assets/Physical\\_Strategy.pdf](https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf).
- Department of Homeland Security (DHS). 2013. “Homeland Security Directive 7: Critical Infrastructure Identification, Prioritization, and Protection.” <https://www.dhs.gov/homeland-security-presidential-directive-7>.
- Garcia, M.L. 2001. *The Design and Evaluation of Physical Protection Systems*. Butterworth-Heinemann.
- North American Electric Reliability Council (NERC). 2002. “Security Guidelines for the Electricity Sector.” Washington, DC. <https://www.nerc.com/comm/CIPC/Security%20Guidelines%20DL/Physical%20Security%20Guideline%202012-05-18-Final.pdf>.
- Schneier, B. 2011. *Secrets and Lies: Digital Security in a Networked World*. New York: Wiley.

## *Chapter 11*

# **The Paradigm Shift**

It takes disasters to trigger change because dangers that remain hypothetical fail to trigger appropriate sensory response.

—D. D. P. Johnson and E. M. P. Madin

The 9/11 shift: There is a new world view in the making.  
If men would learn from history, what lessons it might teach us!

—Samuel Coleridge

The events of 9/11 dramatically changed this nation and focused us on combating terrorism. As a result, in 2003 and subsequent years, the DHS, in conjunction with members from the general public, state and local agencies, and private groups concerned with the safety of critical infrastructures, established a Water Security Working Group (WSWG) to consider and make recommendations on infrastructure security issues. Although initially created to make recommendations for water/wastewater security, WSWG is an excellent template for use with other critical infrastructures, including CS assets. For example, the WSWG identified active and effective security practices for critical infrastructure and provided an approach for adopting these practices. It also recommended mechanisms to provide incentives that facilitate broad and receptive response among critical infrastructure sectors to implement active and effective security practices. Finally, WSWG recommended mechanisms to measure progress and achievements in implementing active and effective security practices and to identify barriers to implementation.

The WSWG recommendations on security are structured to maximize benefits to critical industries by emphasizing actions that have the potential both to improve the quality or reliability of service and to enhance security.



These recommendations, based on original recommendations from the 2003 National Drinking Water Advisor Council (NDWAC), were designed primarily, as the name suggests, for use by water systems of all types and sizes, including systems that serve less than 3,300 people. However, it is the author's opinion, based on personal experience, that NDWAC's recommendations, when properly adapted to applicable circumstances and locations, can be applied to any and all critical infrastructure sectors, including the financial services sector.

The NDWAC identified fourteen features of active and effective security programs that are important to increasing security and relevant across the broad range of utility circumstances and operating conditions. USEPA (2003) points out that the fourteen features are, in many cases, consistent with the steps needed to maintain technical, management, and operational performance capacity related to overall water quality; as pointed out earlier, these steps can be applied to other critical infrastructures as well. Many facilities may be able to adopt some of the features with minimal, if any, capital investment.

### **FOURTEEN FEATURES OF ACTIVE AND EFFECTIVE SECURITY**

It is important to point out that the fourteen features of active and effective programs emphasize that "one size does not fit all" and is not a cookie cutter approach to effective implementation of security measures. There will be variability in security approaches and tactics among commercial securities sector facilities, based on industry-specific circumstances and operating conditions. The fourteen features:

- are sufficiently flexible to apply to all CS assets, regardless of size;
- incorporate the idea that active and effective security programs should have measurable goals and time lines;
- allow flexibility for CS sector facilities to develop specific security approaches and tactics that are appropriate to industry-specific circumstances.

CS sector facilities can differ in many ways including:

- number of supply sources,
- energy capacity,
- operation risk,

- location risk,
- security budget,
- spending priorities,
- political and public support,
- legal barriers, and
- public versus private ownership.

CS sector facilities should address security in an informed and systematic way, regardless of these differences. Financial services sector facilities need to fully understand the specific, local circumstances and the conditions under which they operate and develop a security program tailored to those conditions. The goal in identifying common features of active and effective security programs is to achieve consistency in security program outcomes among CS sector facilities, while allowing for and encouraging facilities to develop utility-specific security approaches and tactics. The features are based on a comprehensive “security management layering system” approach that incorporates a combination of public involvement and awareness, partnerships, and physical, chemical, operational, and design controls to increase overall program performance. They address industry security in four functional categories: organization, operation, infrastructure, and external. These functional categories are discussed in greater detail in the following paragraphs.

- **Organizational**—There is always something that can be done to improve security. Even when resources are limited, the simple act of increasing organizational attentiveness to security may reduce vulnerability and increase responsiveness. Preparedness itself can help deter attacks. The first step to achieving preparedness is to make security a part of the organizational culture, so that it is in the day-to-day thinking of frontline employees, emergency responders, and management of every CS facility in this country. To successfully incorporate security into “business as usual,” there must be a strong commitment to security by organization leadership and by the supervising body, such as the board of stockholders. The next feature addresses how a security culture can be incorporated into an organization.
- **Operational**—In addition to having a strong culture and awareness of security within an organization, an active and effective security program makes security part of operational activities, from daily operations, such as monitoring of physical access controls, to scheduled annual reassessments. CS sector entities will often find that by implementing security into operations they can also reap cost benefits and improve the quality or reliability of the energy service.

- **Infrastructure**—These recommendations advise utilities to address security in all elements of the CS sector infrastructure—from source to distribution and through processing and product delivery.
- **External**—Strong relationships with response partners and the public strengthen security and public confidence. Two of the recommended features of active and effective security programs address this need.

## The Fourteen Features

### **Feature One. Make an explicit and visible commitment of the senior leadership to security.**

CS sector facilities should create an explicit, easily communicated, enterprise-wide commitment to security, which can be done through the following:

- incorporating security into a utility-wide mission or vision statement, addressing the full scope of an active and effective security program—that is, protection of worker/public health, worker/public safety, and public confidence—as part of core day-to-day operations;
- developing an enterprise-wide security policy or set of policies.

CS sector entities should use the process of making a commitment to security as an opportunity to raise awareness of security throughout the organization, making the commitment visible to all employees and customers, and to help every facet of the enterprise to recognize the contribution they can make to enhancing security.

### **Feature Two. Promote security awareness throughout the organization.**

The objective of a security culture should be to make security awareness a normal, accepted, and routine part of day-to-day operations. Examples of tangible efforts include:

- conducting employee training,
- incorporating security into job descriptions,
- establishing performance standards and evaluations for security,
- creating and maintaining a security tip line and suggestion box for employees,
- making security a routine part of staff meetings and organization planning, and
- creating a security policy.

**Feature Three. Assess vulnerabilities and periodically review and update vulnerability assessments to reflect changes in potential threats and vulnerabilities.**

Because circumstances change, CS sector facilities should maintain their understanding and assessment of vulnerabilities as a “living document” and continually adjust their security enhancement and maintenance priorities. CS sector facilities should consider their individual circumstances and establish and implement a schedule for review of their vulnerabilities.

Assessments should take place once every three to five years at a minimum. CS sector facilities may be well served by doing assessments annually.

The basic elements of sound vulnerability assessments are:

- characterization of the chemical processing system, including its mission and objectives,
- identification and prioritization of adverse consequences to avoid,
- determination of critical assets that might be subject to malevolent acts that could result in undesired consequences,
- assessment of the likelihood (qualitative probability) of such malevolent acts from adversaries,
- evaluation of existing countermeasures, and
- analysis of current risk and development of a prioritized plan for risk reduction.

**Feature Four. Identify security priorities and, on an annual basis, identify the resources dedicated to security programs and planned security improvements, if any.**

Dedicated resources are important to ensure a sustained focus on security. Investment in security should be reasonable considering utilities’ specific circumstances. In some circumstances, investment may be as simple as increasing the amount of time and attention that executives and managers give to security. Where threat potential or potential consequences are greater, higher investment is likely warranted.

This feature establishes the expectation that CS facilities should, through their annual capital, operations, maintenance, and staff resources plans, identify and set aside resources consistent with their specific identified security needs. Security priorities should be clearly documented and should be reviewed with utility executives at least once per year as part of the traditional budgeting process.

**Feature Five. Identify managers and employees who are responsible for security and establish security expectations for all staff.**

- Explicit identification of security responsibilities is important for development of a security culture with accountability.
- At minimum, communication sector facilities should identify a single, designated individual responsible for overall security, even if other security roles and responsibilities will likely be dispersed throughout the organization.
- The number and depth of security-related roles will depend on an asset's specific circumstances.

**Feature Six. Establish physical and procedural controls to restrict access to chemical industrial infrastructure to only those conducting authorized, official business and to detect unauthorized physical intrusions.**

Examples of physical access controls include fencing critical areas, locking gates and doors, and installing barriers at site access points. Monitoring for physical intrusion can include maintaining well-lighted facility perimeters, installing motion detectors, and utilizing intrusion alarms. The use of neighborhood watches, regular employee rounds, and arrangements with local police and fire departments can support identifying unusual activity in the vicinity of facilities.

Examples of procedural access controls include inventorying keys, changing access codes regularly, and requiring security passes to pass gates in access-sensitive areas. In addition, utilities should establish the means to readily identify all employees including contractors and temporary workers with unescorted access to facilities.

**Feature Seven. Employee protocols for detection of contamination consistent with the recognized limitations in current contaminant detection, monitoring, and surveillance technology.**

Until progress can be made in the development of practical and affordable online contaminant monitoring and surveillance systems, most CS sector facilities must use other approaches to contaminant monitoring and surveillance.

**Feature Eight. Define security-sensitive information; establish physical, electronic, and procedural controls to restrict access to security-sensitive information; detect unauthorized access; and ensure information and**

**communications systems will function during emergency response and recovery.**

Protecting IT systems largely involves using physical hardening and procedural steps to limit the number of individuals with authorized access and to prevent access by unauthorized individuals. Examples of physical steps to harden SCADA and IT networks include installing and maintaining fire walls and screening the network for viruses. Examples of procedural steps include restricting remote access to data networks and safeguarding critical data through backups and storage in safe places. Utilities should strive for continuous operation of IT and telecommunications systems, even in the event of an attack, by providing uninterruptible power supply and backup systems, such as satellite phones.

In addition to protecting IT systems, security-sensitive information should be identified and restricted to the appropriate personnel. Security-sensitive information could be contained within:

- facility maps and blueprints,
- operations details,
- hazardous material utilization and storage,
- tactical level security program details, and
- any other information on utility operations or technical details that could aid in planning or execution of an attack.

**Feature Nine. Incorporate security considerations into decisions about acquisition, repair, major maintenance, and replacement of physical infrastructure; include consideration of opportunities to reduce risk through physical hardening and adoption of inherently lower-risk design and technology options.**

Prevention is a key aspect of enhancing security. Consequently, consideration of security issues should begin as early as possible in a facility construction (i.e., it should be a factor in building plans and designs). However, to incorporate security considerations into design choices, CS facilities need information about the types of security design approaches and equipment that are available and the performance of these designs and equipment in multiple dimensions. For example, CS sector facilities would want to evaluate not just the way that a particular design might contribute to security but would also look at how that design would affect the efficiency of day-to-day plant operations and worker safety.

**Feature Ten. Monitor available threat-level information and escalate security procedures in response to relevant threats.**

Monitoring threat information should be a regular part of a security program manager's job, and utility-, facility-, and region-specific threat levels and information should be shared with those responsible for security. As part of security planning, financial services sector facilities should develop systems to access threat information—procedures that will be followed in the event of increased industry or facility threat levels—and should be prepared to put these procedures in place immediately, so that adjustments are seamless. Involving LLE and FBI is critical.

CS sector facilities should investigate what networks and information sources might be available to them locally and at the state and regional level. If a utility cannot gain access to some information networks, attempts should be made to align with those who can and will provide effective information to the financial services sector facility.

**Feature Eleven. Incorporate security considerations into emergency response and recovery plans, test and review plans regularly, and update plans to reflect changes in potential threats, physical infrastructure, chemical processing operations, critical interdependencies, and response protocols in partner organizations.**

CS sector facilities should maintain response and recovery plans as “living documents.” In incorporating security considerations into their emergency response and recovery plans, chemical facilities also should be aware of the National Incident Management System (NIMS) guidelines, established by DHS, and of regional and local incident management commands and systems, which tend to flow from the national guidelines.

CS sector facilities should consider their individual circumstances and establish, develop, and implement a schedule for review of emergency response and recovery plans. CS sector facility plans should be thoroughly coordinated with emergency response and recovery planning in the larger community. As part of this coordination, a mutual program should be established to arrange in advance for exchanging resources (personnel or physical assets) among agencies within a region, in the event of an emergency or disaster that disrupts operation. Typically, the exchange of resource is based on a written formal mutual agreement. For example, Florida's Water-Wastewater Agency Response Network (FlaWARN), deployed after Hurricane Katrina, which allowed the new “utilities helping utilities” network to respond to urgent requests from Mississippi for help to bring facilities back on line after the hurricane.

The emergency response and recovery plans should be reviewed and updated as needed annually. This feature also establishes the expectation that chemical facilities should test or exercise their emergency response and recovery plans regularly.

**Feature Twelve. Develop and implement strategies for regular, ongoing security-related communications with employees, response organizations, rate-setting organizations, and customers.**

An active and effective security program should address protection of public health, public safety (including infrastructure), and public confidence. CS sector facilities should create an awareness of security and an understanding of the rationale for their overall security management approach in the communities they reside in and/or serve.

Effective communication strategies consider key messages; who is best equipped/trusted to deliver the key messages; the need for message consistency, particularly during an emergency; and the best mechanisms for delivering messages and for receiving information and feedback from key partners. The key audiences for communication strategies are utility employees, response organizations, and customers.

**Feature Thirteen. Forge reliable and collaborative partnerships with the communities served, managers of critical interdependent infrastructure, response organizations, and other local utilities.**

Effective partnerships build collaborative working relationships and clearly define roles and responsibilities, so that people can work together seamlessly if an emergency should occur. It is important for CS sector facilities within a region and neighboring regions to collaborate and establish a mutual aid program with neighboring utilities, response organizations, and sectors, such as the power sector, on which the utilities rely or impact. Mutual aid agreements provide for help from other organizations that is prearranged and can be accessed quickly and efficiently in the event of a terrorist attack or natural disaster. Developing reliable and collaborative partnerships involves reaching out to managers and key staff and other organizations to build reciprocal understanding and to share information about the facility's security concerns and planning. Such efforts will maximize the efficiency and effectiveness of a mutual aid program during an emergency response effort, as the organizations will be familiar with each other's circumstances and thus will be better able to serve each other.

It is also important for CS sector facilities to develop partnerships with the communities and customers they serve. Partnerships help to build credibility



within communities and establish public confidence in utility operations. People who live near financial services sector facility structures can be the eyes and ears of the facility and can be encouraged to notice and report changes in operating procedures or other suspicious behaviors.

CS sector facilities and public health organizations should establish formal agreements on coordination to ensure regular exchange of information between facilities and public health organizations and outline roles and responsibilities during response to and recovery from an emergency. Coordination is important at all levels of the public health community—national public health, county health agencies, and healthcare providers such as hospitals.

**Feature Fourteen. Develop CS facility-specific measures of security activities and achievements and self-assess against these measures to understand and document program progress.**

Although security approaches and tactics will be different depending on CS-specific circumstances and operating conditions, we recommend that all financial services sector facilities monitor and measure a number of common types of activities and achievements, including the existence of program policies and procedures, training, testing, and implementing schedules and plans.

**The Fourteen Feature Matrix**

In the following, a matrix of recommended measures to assess the effectiveness of a CS sector facility’s security program is presented. Each feature is grouped according to its functional category: organization, operation, infrastructure, and external.

**Table 11.1 Fourteen Features of Active and Effective Security Matrix**

<i>Features</i>	<i>Checklist: Potential Measures of Progress</i>
<i>Organizational Features</i>	
Feature One—Explicit commitment to security	Does a written, enterprise-wide security policy exist, and is the policy reviewed regularly and updated as needed?
Feature Two—Promote security lessons awareness	Are incidents reported in a timely way, and are learned from incident responses reviewed and, as appropriate, incorporated into future utility security efforts?
Feature Five—Defined security roles and employee expectations	Are managers and employees who are responsible for security identified?

*(Continued)*

**Table 11.1 Fourteen Features of Active and Effective Security Matrix—Continued**

<i>Features</i>	<i>Checklist: Potential Measures of Progress</i>
<i>Operational Features</i>	
Feature Three—Vulnerability incidents, after assessment up to date	Are reassessments of vulnerabilities made and are lessons learned and other relevant information incorporated into security practices?
Feature Four—Security resources and implementation priorities	Are security priorities clearly identified, and to what extent do security priorities have resources assigned to them?
Feature Seven—Contamination detection	Is there a protocol/procedure in place to identify and respond to suspected contamination events?
Feature Ten—Threat-level based protocols	Is there a protocol/procedure of responses that will be made if threat levels change?
Feature Eleven—Emergency Response Plan tested and up to date	Does exercise address the full range of threats—physical, cyber, and contamination—and is there a protocol/procedure to incorporate lessons learned from exercises and actual response into updates to emergency response and recovery plans?
Feature Fourteen—Industry-specific measures and self-assessment	Does the utility perform self-assessment a least annually?
<i>Infrastructure Features</i>	
Feature Six—Intrusion detection and access control	To what extent are methods to control access to sensitive assets in place?
Feature Eight—Information protection and continuity	Is there a procedure to identify and control security-sensitive information, is information correctly categorized, and how to control measures perform under testing?
Feature Nine—Design and construction standards	Are security considerations incorporated into internal utility design and construction standards for new facilities/ infrastructure and major maintenance projects?
<i>External Features</i>	
Feature Twelve—Communications	Is there a mechanism for utility employees, partners, and the community to notify the utility of suspicious occurrences and other security concerns?
Feature Thirteen—Partnerships	Have reliable and collaborative partnerships with customers, managers of independent interrelated infrastructure, and response organizations been established?

Source: USEPA, 2003.

Ultimately, the goal of implementing the fourteen security features (and all other security provisions) is to create a significant improvement in CS sector facilities on a national scale, by reducing vulnerabilities, and therefore risk to public health from terrorist attacks and natural disasters. To create a sustainable effect, the CS sector as a whole must not only adopt and actively practice the features but also incorporate the features into “business as usual.”

## REFERENCES AND RECOMMENDED READING

- Department of Homeland Security (DHS). 2003. “The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.” [https://www.dhs.gov/xlibrary/assets/Physical\\_Strategy.pdf](https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf).
- Department of Homeland Security (DHS). 2009. “National Infrastructure Protection Plan.” <https://www.dhs.gov/cisa/national-infrastructure-protection-plan>.
- Department of Homeland Security (DHS). 2015. “Homeland Security Directive 7: Critical Infrastructure Identification, Prioritization, and Protection.” <https://www.dhs.gov/homeland-security-presidential-directive-7>.
- Department of Homeland Security (DHS). 2015. *Commercial Facilities Sector-Specific Plan*. Washington, DC: U.S. Department of Homeland Security.
- United States Environmental Protection Agency (U.S. EPA). 2006. “Active and Effective Water Security Programs: A Summary Report of the National Drinking Water Advisory Council Recommendations on Water Security.”

# Glossary

**Acid bomb** A crude bomb made by combining muriatic acid with aluminum strips in a 2-liter soda bottle.

**Aerosol** A fine mist or spray, which contains minute particles.

**Aflatoxin** A toxin created by bacteria that grow on stored foods, especially on rice, peanuts, and cotton seeds.

**Agency** A division of government with a specific function, or a nongovernmental organization (e.g., private contractor, business) that offers a particular kind of assistance.

**Air marshal** A federal marshal whose purpose is to ride commercial flights dressed in plain clothes and armed to prevent hijackings. Israel's use of air marshals on El Al is credited as the reason Israel has not had a single hijacking in thirty-one years. The United States started using air marshals after September 11.

**Airborne** Carried by or through the air.

**All-Hazards** A grouping classification encompassing all conditions, environmental or man-made, that have the potential to cause injury, illness, or death; damage to or loss of equipment, infrastructure services, or property, or alternatively causing functional degradation to social, economic, or environmental aspects.

**Al Jazeera** Satellite television station based in Qatar and broadcast throughout the Middle East. Al Jazeera has often been called the "CNN" of the Arab world.

**Al Qaeda** Meaning "the Base"—an international terrorist group founded in approximately 1989 and dedicated to opposing non-Islamic governments with force and violence. One of the principal goals of Al Qaeda was to drive the U.S. armed forces out of the Saudi Arabian peninsula and Somalia by violence.

**Al Tahwid** A Palestinian group based in London which professes a desire to destroy both Israel and the Jewish people throughout Europe. Eleven members of al Tahwid were arrested in Germany allegedly as they were about to begin attacking that country.

**Alpha radiation** The least penetrating type of nuclear radiation. Not considered dangerous unless particles enter the body.

**American Airlines Flight 11** The Boeing 767 carrying eighty-one passengers, nine flight attendants, and two pilots, which was hijacked and crashed into the north tower of the World Trade Center at 8:45 a.m. eastern time on September 11, 2001. Flight 11 was en route to Los Angeles from Boston.

**American Airlines Flight 77** The Boeing 757 carrying fifty-eight passengers, four flight attendants, and two pilots, which was hijacked and crashed into the Pentagon at 9:40 a.m. eastern time on September 11, 2001. Flight was en route to Los Angeles from Dulles International Airport in Virginia.

**Ammonium nitrate-fuel oil (ANFO)** A powerful explosive made by mixing fertilizer and fuel oil. The type of bomb used in the first World Trade Center attack as well as Oklahoma City bombing.

**Analyte** The name assigned to a substance or feature that describes it in terms of its molecular composition, taxonomic nomenclature, or other characteristic.

**Anthrax** An often fatal infectious disease contracted from animals. Anthrax spores have such a long survival period; the incubation period is short; disability is severe, making anthrax a bioweapon of choice by several nations.

**Antidote** A remedy to counteract the effects of poison.

**Antigen** A substance which stimulates an immune response by the body immune system recognizes such substances as foreign and produces antibodies to fight them.

**Antitoxin** An antibody which neutralizes a biological toxin.

**Armed Islamic Group (GIA)** An Algerian Islamic extremist group which aims to overthrow the secular regime in Algeria and replace it with an Islamic state. The GIA began its violent activities in early 1992 after Algiers voided the victory of the largest Islamic party, Islamic Salvation Front (FIS), in the December 1991 elections.

**Asset** A person, structure, facility, information, material, or process that has value. In the context of the National Infrastructure Protection Plan (NIPP), people are not considered assets.

**Asymmetric threat** The use of crude or low-tech methods to attack a superior or more high-tech enemy.

**Axis of Evil** Iran, Iraq, and North Korea as mentioned by President G. W. Bush during his State of the Union speech in 2002 as nations which were a threat to U.S. security due to harboring terrorism.

- Bioaccumulative** Substances that concentrate in living organisms as the breather contaminated air drink or live in contaminated water or eat contaminated food rather than being eliminated through natural processes.
- Biochemical warfare** Collective term for use of both chemical warfare and biological warfare weapons.
- Biological Ammunition** Ammunition designed specifically to release a biological agent used as the warhead for biological weapons. Biological ammunition may take many forms, such as a missile warhead or bomb.
- Biological Attacks** The deliberate release of germs or other biological substances that cause illness.
- Biosafety Level 1** Suitable for work involving well-characterized biological agents not known to consistently cause disease in healthy adult humans, and of minimal potential hazard to lab personnel and the environment. Work is generally conducted on open bench tops using standard microbiological practices.
- Biosafety Level 2** Suitable for work involving biological agents of moderate potential hazard to personnel and the environment. Lab personnel should have specific training in handling pathogenic agents and be directed by competent scientists.
- Biosafety Level 3** Suitable for work done with indigenous or exotic biological agents that may cause serious or potentially lethal disease as a result of exposure by inhalation. Lab personnel must have specific training in handling pathogenic and potentially lethal agents and be supervised by competent scientists who are experienced in working with these agents.
- Biosafety Level 4** Suitable for work with the most infectious biological agents. Access to the two Biosafety Level 4 labs in the United States is highly restricted.
- Bioterrorism** The use of biological agents in a terrorist operation. Biological toxin would include anthrax, ricin, botulism, the plague, smallpox, and tularemia.
- Bioterrorism Act** The Public Health Security and Bioterrorism Preparedness and Response Act of 2002.
- Biowarfare** The use of biological agents to cause harm to targeted people either, directly, by bringing the people into contact with the agents or, indirectly, by infecting other animals and plants, which would in turn cause harm to the people.
- Blister agents** Agents which cause pain and incapacitation instead of death and might be used to injure many people at once, thereby overloading medical facilities and causing fear in the population. Mustard gas is the best known blister agent.
- Blood agents** Agents based on cyanide compounds. More likely to be used for assassination than for terrorism.

**Botulism** An illness caused by the botulinum toxin, which is exceedingly lethal and quite simple to produce. It takes just a small amount of the toxin to destroy the central nervous system. Botulism may be contracted by the ingestion of contaminated food or through breaks or cuts in the skin. Food supply contamination and aerosol dissemination of the botulinum toxin are the two ways most likely to be used by terrorists.

**Bush Doctrine** The policy that holds responsible nations which harbor or support terrorist organizations and says that such countries are considered hostile to the United States. From President Bush's speech: "A country that harbors terrorists will either deliver the terrorist or share in their fate. . . . People have to choose sides. They are either with the terrorists, or they're with us."

**Business continuity** The ability of an organization to continue to function before, during, and after a disaster.

**BWC** Officially known as the "Convention on the Prohibition of Development, Production, and Stockpiling of Bacteriological (Biological) and Toxin Weapons and Destruction." The BWC works toward general and complete disarmament, including the prohibition and elimination of all types of weapons of mass destruction.

**Camp X-Ray** The Guantanamo Bay, Cuba, which houses al Qaeda and Taliban prisoners.

**Carrier** A person or animal that is potentially a source of infection by carrying on infectious agent without visible symptoms of the disease.

**Cascading event** The occurrence of one event that causes another event.

**Causative agent** The pathogen, chemical, or other substance that is the cause of disease or death in an individual.

**Cell** The smallest unit within a guerrilla or terrorist group. A cell generally consists of two to five people dedicated to a terrorist cause. The formation of cells is born of the concept that an apparent "leaderless resistance" makes it hard for counter-terrorists to penetrate.

**Chain of custody** The tracking and documentation of physical control of evidence.

**Chemical agent** A toxic substance intended to be used for operations to debilitate, immobilize, or kill military or civilian personnel.

**Chemical ammunition** A munition, commonly a missile, bomb, rocket, or artillery shell, designed to deliver chemical agents.

**Chemical attack** The intentional release of toxic liquid, gas, or solid in order to poison the environment or people.

**Chemical warfare** The use of toxic chemicals as weapons, not including herbicide, used to defoliate battlegrounds or riot control agents such as gas or mace.

**Chemical weapons** Weapons that produce effects on living targets via toxic chemical properties. Examples would be sarin, VX nerve gas, or mustard gas.

**Chemterrorism** The use of chemical agents in a terrorist operation. Well-known chemical agents include sarin and VX nerve gas.

**Choking agent** Compounds that injure primarily in the respiratory tract (i.e., nose, throat, and lungs). In extreme cases membranes swell up, lungs become filled with liquid, and death results from lack of oxygen.

**Cipro** A Bayer antibiotic that combats inhalation anthrax.

**Communications architecture elements** Assets, systems, and networks that make up the communications architecture. The following are just a few sample categories of architectures elements:

- *access*—primarily the local portion of the network connecting end users to the backbone that enables users to send or receive communications.
- *broadcasting*—broadcasting systems consist of free, over-the-air radio, and television stations that offer analog and digital audio and video programming services and data services. Broadcasting has been the principal means of providing emergency alerting services to the public for six decades.
- *cable*—this wireline network offers television Internet and voice services that interconnect with the PSTN through end offices.
- *customer equipment*—equipment owned and operated by the end user or located at the end user's facility.
- *satellite*—this is a space vehicle launched into orbit to relay audio, data, or video signals as part of a telecommunications network. Signals are transmitted to the satellite from earth station antennas, amplified, and sent back to earth for reception by other earth station antennas.
- *wireless*—refers to telecommunication in which electromagnetic waves (rather than some form of wire) carry the signal over part of or the entire communication path. Consists of cellular phone, paging, personal communication services, high-frequency radio, unlicensed wireless, and other commercial and private radio services.
- *wireline*—consists primarily of the PSTN but also includes enterprise networks. The PSTN is a domestic communications network accessed by telephones, key telephone systems, private branch exchange (PBX) trunks, and data arrangements. Despite industry's transition to packet-based networks, the traditional PSTN remains the backbone of the communications infrastructure includes landline telephone, the Internet, and submarine cable infrastructure.

**Confirmed** In the context of the threat evaluation process, a water contamination incident is definitive evidence that the water has been contaminated.



**Consequence** The effect of an event, incident, or occurrence. For the purposes of the NIPP, consequences are divided into four main categories: public health and safety, economic, psychological, and governance impacts.

**Control center** A sophisticated monitoring and control system responsible for balancing power generation and demand; monitoring flows over transmission lines to avoid overloading; planning and configuring the system to operate reliably; maintaining system stability; preparing for emergencies; and placing equipment in and out of service for maintenance and emergencies.

**Control systems** Computer-based systems used within many infrastructures and industries to monitor and control sensitive processes and physical functions. These systems typically collect measurement and operation data from the field, process and display the information, and relay control commands to local or remote equipment or human-machine interfaces (operators). Examples of types of control systems include SCADA system, process control systems, and distributed control systems.

**Counterterrorism** Measures used to prevent preempt or retaliate against terrorist attacks.

**Critical infrastructure** Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any federal, state, regional, territorial, or local jurisdiction.

**Cutaneous** Related to or entering through the skin.

**Cutaneous anthrax** Anthrax that is contracted via broken skin. The infection spreads through the bloodstream causing cyanosis, shock, sweating, and finally death.

**Cyanide agent** Used by Iraq in the Iran war against the Kurds in the 1980s, and also by the Nazis in the gas chambers of concentration camps, cyanide agents are colorless liquid which is inhaled in its gaseous form while liquid cyanide and cyanide salts are absorbed by the skin. Symptoms are headache, palpitations, dizziness, and respiratory problems followed later by vomiting, convulsions, respiratory failure and unconsciousness, and eventually death.

**Cybersecurity** The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Cybersecurity includes protection and restoration, when needed, or information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems.

- Cyber system** Any combination of facilities, equipment, personnel, procedures, and communications integrated to provide cyber services. Examples include business systems, control systems, and access control systems.
- Cyberterrorism** Attacks on computer networks or systems, generally by hackers working with or for terrorist groups. Some forms of cyberterrorism include denial of service attacks, inserting viruses or stealing data.
- Defense Industrial Base Sector** The DOD, U.S. Government (USG), and private sector worldwide industrial complex with capabilities to perform research, development, and design and to product and maintain military weapon systems, subsystems, components, or parts to meet military requirements.
- Defensive critical asset** An asset of such extraordinary important to operations in peace crisis, and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the Department of Defense to fulfill its missions.
- Dependency** The one-directional reliance of an asset, system network, or collection thereof, within or across sectors, in input, interaction, or other requirement from other sources in order to function properly.
- Dirty bomb** A makeshift nuclear device which is created from radioactive nuclear waste material. While not a nuclear blast, an explosion of a dirty bomb causes localized radioactive contamination as the nuclear waste material is carried into the atmosphere where it is dispersed by the wind.
- Ebola** Ebola hemorrhagic fever (Ebola EF) is a severe, often fatal disease in nonhuman primates such as monkeys, chimpanzees, gorillas, and in humans. Ebola has appeared sporadically since 1976 when it was first recognized.
- eBomb** (for e-bomb) Electromagnetic bomb which produces a brief pulse of energy which affects electronic circuitry. At low levels, the pulse temporarily disables electronics systems, including computers, radios, and transportation systems. High levels completely destroy circuitry, causing mass disruption of infrastructure while sparing life and property.
- Ecotage** Is the portmanteau of the “eco-” prefix and “sabotage.” It is used to describe illegal acts of vandalism and violence, committed in the name of environmental protection.
- Ecoterrorism** A neologism for terrorism that includes sabotage intended to hinder activities that are considered damaging to the environment.
- Electromagnetic Pulse (EMP)** A burst of electromagnetic radiation by deliberate means, such as nuclear attack, or through natural means, such as a large-scale geomagnetic storm. Magnetic and electric fields resulting from EMP have the potential to disrupt electrical and electronic systems by causing destructive current and voltage surges.

**Energy Asset and System Parameters** Six general asset or system characteristics that are important parameters for evaluating the vulnerabilities of energy infrastructure and developing risk management programs. They include physical and location attributes, cyber attributes, volumetric or throughput attributes, temporal/load profile attributes, human attributes, and the important of an asset of system to the energy network.

**Euroterrorism** Associated with left-wing terrorism of the 1960s, 1970s, and 1980s involving the Red Brigade, Red Army Faction, and November 17th Group, among other groups which targeted American interests in Europe and NATO. Other groups include Orange Volunteers, Red Hand Defenders, Continuity IRA, Loyalist Volunteer Force, Ulster Defense Association, and First of October Anti-Fascist Resistance Group.

**Fallout** The descent to the earth's surface of particles contaminated with radioactive material from a radioactive cloud. The term can also be applied to the contaminated particulate matter itself.

**Fatah** Meaning "conquest by means of jihad"; a political organization created in the 1960s and led by Yasser Arafat. With both a military and intelligence wing, it has carried out terrorist attacks on Israel since 1965. It joined the PLO in 1968. Since 9/11, the Fatah was blamed for attempting to smuggle 50 tons of weapons into Israel.

**Fatwa** A legal ruling regarding Islamic Law.

**Fedayeen Saddam** Iraq's paramilitary organization said to be an equivalent to the Nazi's "SS." The militia is loyal to Saddam Hussein and is responsible for using brutality on civilians who are not loyal to the policies of Saddam. They do not dress in uniform.

**Filtrate** In ultrafiltration, the water that passes through the membrane and which contains particles smaller than the molecular weight cutoff of the membrane.

***frustration-aggression hypothesis*** a hypothesis that every frustration leads to some form of aggression and every aggressive act results from some prior frustration. As defined by Gurr: "The Necessary precondition for violent civil conflict is relative deprivation, defined as actors' perception of discrepancy between their value expectations and their environment's apparent value capabilities. This deprivation may be individual or collective."

**Function** A service, process, capability, or operation performed by an asset, system, network, or organization.

**Fundamentalism** Conservative religious authoritarianism. Fundamentalism is not specific to Islam; it exists in all faiths. Characteristics include literal interpretation of scriptures and a strict adherence to traditional doctrines and practices.

**Geneva Protocol 1925** The first treaty to prohibit the use of biological weapons. The 1925 Geneva Protocol for the Prohibition of the Use In War of Asphyxiating, Poisonous or Other Gases and Bacteriological Methods of Warfare.

**Germ warfare** The use of biological agents to cause harm to targeted people either, directly, by bringing the people into contact with the agents or, indirectly, by infecting other animals and plants, which would in turn cause harm to the people.

**Glanders** An infectious bacterial disease known to cause inflammation in horses, donkeys, mules, goats, dogs and cats. Human infection has not been seen since 1945, but because so few organisms are required to cause disease, it is considered a potential agent for biological warfare.

**Government Coordinating Council (GCC)** The government counterpart to the SCC of each sector established to enable interagency coordination. The GCC comprises representatives across various levels of government (federal, state, local, tribal, and territorial) as appropriate to the security and operations landscape of each individual sector.

**Grab sample** A single sample collected at a particular time and place that represents the composition of the water, air, or soil only at that time and location.

**Ground zero** From 1946 until 9/11, ground zero was the point directly above, below, or at which a nuclear explosion occurs or the center or origin of rapid, intense, or violent activity or change. After 9/11, the term, when used with initial capital letters, refers to the ground at the epicenter of the World Trade Center attacks.

**Guerrilla warfare** The term was invented to describe the tactics Spain used to resist Napoleon, though the tactic itself has been around much longer. Literally, it means “little war.” Guerilla warfare features cells and utilizes no front line. The oldest form of asymmetric warfare, guerilla warfare is based on sabotage and ambush with the objective of destabilizing the government through lengthy and low-intensity confrontation.

**Hamas** A radical Islamic organization which operates primarily in the West Bank and Gaza Strip whose goal is to establish an Islamic Palestinian state in place of Israel. On the one hand, Hamas operates overtly in their capacity as social services deliverers, but its activists have also conducted many attacks, including suicide bombings, against Israeli civilians and military targets.

**Hazard** An inherent physical or chemical characteristic that has the potential for causing harm to people, the environment, or property.

**Hazard assessment** The process of evaluating available information about the site to identify potential hazards that might pose a risk to the site characterization team. The hazard assessment results in assigning one of four

levels to risk: lower hazard, radiological hazard, high chemical hazard, or high biological hazard.

**Hemorrhagic fevers** In general, the term viral hemorrhagic fever is used to describe severe multisystem syndrome wherein the overall vascular system is damaged, and the body becomes unable to regulate itself. These symptoms are often accompanied by hemorrhage; however, the bleeding itself is not usually life threatening. While some types of hemorrhagic fever viruses can cause relatively mild illnesses.

**High-Impact, Low-Frequency (HILF)** HILF events are occurrences that are relatively unusual, but have the potential to cause catastrophic disruption. Examples include pandemic disease, terrorist attack, and electromagnetic pulse.

**Hizbollah (Hezbollah)** Meaning “The Party of God.” One of many terrorist organizations which seek the destruction of Israel and of the United States. They have taken credit for numerous bombings against civilians and have declared that civilian targets are warranted. Hezbollah claims it sees no legitimacy for the existence of Israel, and that their conflict becomes one of legitimacy that is based on religious ideals.

**Homeland Security Office** An agency organized after 9/11, with former Pennsylvania Governor Tom Ridge heading it up. The Office of Homeland Security is at the top of approximately forty federal agencies charged with protecting the United States against terrorism.

**Homicide bombings** A term the White House coined to replace the old “suicide bombings.”

**Incident** A confirmed occurrence that requires response actions to prevent or minimize loss of life or damage to property and/or natural resources. A drinking water contamination incident occurs when the presence of a harmful contaminant has been confirmed.

**Infrastructure** The framework of interdependent networks and systems comprising identifiable industries, (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense of economic security of the United States, the smooth functioning of government at all levels, and society as a whole. Consistent with the definition in the Homeland Security Act, infrastructure includes physical, cyber, and/or human elements.

**Inhalation anthrax** A form of anthrax that is contracted by inhaling anthrax spores. This results in pneumonia, sometimes meningitis, and finally death.

**ISIS (ISIL) Islamic State of Iraq and the Levant** Islamic extremist rebel group that presently controls territory and brutalizes and/or murders various groups in various countries, including Syria, Iraq, Libya, and Nigeria, and others.

**Interdependency** Mutually reliant relationship between entities (objects, individuals, or groups). The degree of interdependency does not need to be equal in both directions.

**Intifada** (intifadah) (alternatively Intifadah, from Arabic “shaking off”) The two intifadas are similar in that both were originally characterized by civil disobedience by the Palestinians which escalated into the use of terror. In 1987, following the killing of several Arabs in the Gaza Strip, the first intifada began and went on until 1993. The second intifada began in September 2000, following Ariel Sharon’s visit to the Temple Mount.

**Islam** Meaning “submit.” The faith practiced by followers of Muhammad. Islam claims more than a billion believers worldwide.

**Jihad** Meaning “struggle.” The definition is a subject of vast debate. There are two definitions generally accepted. The first is a struggle against oppression, whether political or religious. The second is the struggle within oneself, or a spiritual struggle.

**Key resources** As defined in the Homeland Security Act, key resources are publicly or privately controlled resources essential to the minimal operations of the economy and government.

**Knecapping** A malicious wounding by firearm to damage the knee joint; a common punishment used by Northern Ireland’s IRA involves collaborating with the British.

**Koran** The holy book of Islam that is considered by Muslims to contain the revelations of God to Mohammed; also called Qu’ran.

**LD50** The dose of a substance which kills 50 percent of those infected.

**Laboratory Response Network (LRN)** A network of labs developed by the CDC, APHL, and FBI for the express purpose of dealing with bioterrorism threats, including pathogens and some biotoxins.

**Lassa fever** An acute, often fatal, viral disease characterized by high fever, ulcers of the mucous membranes, headaches, and disturbances of the gastrointestinal system.

**Links** The means (road, rail, barge, or pipeline) by which a chemical is transported from one node to another.

**Mindset** According to *American Heritage Dictionary*: “1. A fixed mental attitude or disposition that predetermines a person’s response to an interpretation of situations; 2. and inclination or a habit.” *Merriam Webster’s Collegiate Dictionary* (10th ed.) defines it as (1) A mental attitude or inclination; (2) A fixed state of mind. The term dates from 1926 but apparently is not included in dictionaries of psychology.

**Mitigation** Ongoing and sustained action to reduce the probability of or lessen the impact of an adverse incident.

- Molotov cocktail** A crude incendiary bomb made of a bottle filled with flammable liquid and fitted with a rag wick.
- Monkeypox** The Russian bioweapon program worked with this virus, which is in the same family as smallpox. In June 2003, a spate of human monkeypox cases was reported in the U.S. Midwest. This was the first time that monkeypox was seen in North America, and it was the first time that monkeypox was transferred from animal to human. There was some speculation that it was a bioattack.
- Mullah** A Muslim, usually holding an official post, who is trained in traditional religious doctrine and law and doctrine.
- Muslim** (also Moslem) Followers of the teachings of Mohammed or Islam.
- Mustard gas** Blistering agents which cause severe damage to the eyes, internal organs, and respiratory system. Produced for the first time in 1822, mustard gas was not used until World War I. Victims suffered the effects of mustard gas thirty to forty years after exposure.
- Narcoterrorism** The view of many counterterrorist experts that there exists an alliance between drug traffickers and political terrorists.
- National Pharmaceutical Stockpile** A stock of vaccines and antidotes which are stored at Centers for Disease Control in Atlanta, to be used against biological warfare.
- Nerve agent** The Nazis used the first nerve agents: insecticides developed into chemical weapons. Some of the better known nerve agents include VX, sarin, soman, and tabun. These agents are used because only a small quantity is necessary to inflict a substantial damage. Nerve agents can be inhaled or can absorb through intact skin.
- Network** A group of components that share information or interact with each other in order to perform a function.
- Nodes** A facility at which a chemical is produced, store, or consumed.
- Nuclear blast** An explosion of any nuclear material which is accompanied by a pressure wave, intense light and heat, and widespread radioactive fallout which can contaminate the air, water, and ground surface for miles around.
- Opportunity Contaminant** A contaminant that might be readily available in a particular area, even though they may not be highly toxic or infectious or easily dispersed and stable in treated drinking water.
- Owners/operators** Those entities responsible for day-to-day operation and investment in a particular asset or system.
- Pandemic influenza** Defined by the World Health Organization (WHO) as a global outbreak of influenza, characterized by an emergent strain of the virus, little to no immunity among the general population, rapid and sustained person-to-person transmission, and lack of a vaccine. On June 11, 2009, WHO determined that 2009 H1N1 influenza (also known as “swine flu”) had reached pandemic status.

- Pathogen** Any agent which can cause disease.
- Pathways** The sequence of nodes and links by which a chemical is produced, transported, and transformed from its initial source to its ultimate consumer.
- Physical security** The use of barriers and surveillance to protect resources, personnel, and facilities against crime, damage, or unauthorized access.
- Plague** The pneumonic plague, which is more likely to be used in connection with terrorism, is naturally carried by rodents and fleas but can be aerosolized and sprayed from crop dusters.
- Political terrorism** Terrorist acts directed at governments and their agents and motivated by political goals (i.e., national liberation).
- Possible** In the context of the threat evaluation process, a water contamination threat is characterized as “possible” if the circumstances of the threat warning appear to have provided an opportunity for contamination.
- Potassium iodide** An FDA-approved nonprescription drug for use as a blocking agent to prevent the thyroid gland from absorbing radioactive iodine.
- Preparedness** The activities necessary to build, sustain, and improve readiness capabilities to prevent, protect against, respond to, and recover from natural or man-made incidents. Preparedness is a continuous process involving efforts at all levels of government and between government and the private sector and nongovernmental organizations to identify threats, determine vulnerabilities, and identify required resources to prevent, respond to, and recover from major incidents.
- Presumptive results** Results of chemical and/or biological field testing that need to be confirmed by further lab analysis. Typically used in reference to the analysis of pathogens.
- Prevention** Actions taken and measures put in place for the continual assessment and readiness of necessary actions to reduce the risk of threats and vulnerabilities, to intervention and stop an occurrence, or to mitigate effects.
- Prioritization** In the context of the NIPP, prioritization is the process of using risk assessment results to identify where risk reduction or mitigation efforts are most needed and to subsequently determine which protective actions should be instituted in order to have the greatest effect.
- Protection** Actions or measures taken to cover or shield from exposure, injury, or destruction. In the context of the NIPP, protection includes actions to deter the threat, mitigate the vulnerabilities, or minimize the consequences associated with a terrorist attack or other incident. Protection can include a wide range of activities, such as hardening facilities, building resilience and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing



security systems and redundancy, incorporating hazard resistant into initial facility design, initiating active or passive countermeasures, installing security systems, promoting workforce surety, training and exercises, and implementing cyber security measures, among various others.

**Psychopath** A mentally ill or unstable person, especially one having a psychopathic personality (*q.v.*), according to *Webster's*.

**Psychopathy** A mental disorder, especially an extreme mental disorder marked usually by egocentric and antisocial activity, according to *Webster's*.

**Psychopathology** The study of psychological and behavioral dysfunction occurring in mental disorder or in social disorganization, according to *Webster's*.

**Psychotic** Of, relating to, or affected with psychosis, which is a fundamental mental derangement (as schizophrenia) characterized by defective or lost contact with reality, according to *Webster's*.

**Rapid field testing** Analysis of water during site characterization uses rapid field water testing technology in an attempt to tentatively identify contaminants or unusual water quality.

**Recovery** The development, coordination, and execution of service- and site-restoration plans for affected communities and the reconstitution of government operations and services through individual, private sector, nongovernmental, and public assistance programs that identify needs and define resources; provide housing and promote restoration; address long-term care and treatment of affected persons; implement additional measures for community restoration; incorporate mitigation measures and techniques, as flexible; evaluate the incident to identify lessons learned and develop initiatives to mitigate the effects of future incidents.

**Red teaming** As used in this text, a group exercise to imagine all possible terrorist attack scenarios against the chemical infrastructure and their consequences.

**Redundancy** An energy reliability strategy based on the notion that multiple systems provide needed backup if one system fails or cannot meet demand.

**Resilience/resiliency** The ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions. In the context of energy security, resilience is measured in terms of robustness, resourcefulness, and rapid recovery.

**Response** Activities that address the short-term, direct effects of an incident, including immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans and incident mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include applying intelligence

and other information to lessen the effects or consequences of an incident; increasing security operations; continuing investigations into the nature and source of the threat; ongoing surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.

**Retentate** In ultrafiltration, the retentate is the solution that contains the particles that do not pass through the membrane filter. The retentate is also called the concentrate.

**Ricin** A stable toxin easily made from the mash that remains after processed castor beans. At one time, it was used as an oral laxative, castor oil; castor oil causes diarrhea, nausea, vomiting, abdominal cramps, internal bleeding, liver and kidney failure, and circulatory failure. There is not antidote.

**Risk** The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.

**Salmonella** An infection caused by a gram-negative bacillus, a germ of the *Salmonella* genus. Infection with this bacteria may involve only intestinal tract or may be spread from the intestines to the bloodstream and then to other sites in the body. Symptoms of salmonella enteritis include diarrhea, nausea, abdominal cramps, and fever.

**Sarin** A colorless, odorless gas. With a lethal dose of 0.5 mg (a pinprick-sized droplet), it is twenty-six times more deadly than cyanide gas. Because the vapor is heavier than air, it hovers close to the ground. Sarin degrades quickly in humid weather, but sarin's life expectancy increases as temperature gets higher, regardless of how humid it is.

**Sector** A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society. The NIPP addresses 18 Critical Infrastructures sectors, identified by the criteria set forth in HSPD-7.

**Sentinel Laboratory** An LRN lab that reports unusual results that might indicate a possible outbreak and refers specimens that may contain select biological agents in Reference labs within the LRN.

**Site characterization** The process of collecting information from an investigation site in order to support the evaluation of a drinking water contamination threat. Site characterization activities include the site investigation, field safety screening, rapid field testing of the water, and sample collection.

**Situational awareness** An understanding of the current environment and the ability to accurately anticipate future problems in order to respond effectively.

**Sleeper cell** A small cell which keeps itself undetected until such time as they can “awaken” and cause havoc.

**Smallpox** The first biological weapon, used during the eighteenth century, smallpox killed 300 million people in the nineteenth century. There is no specific treatment for smallpox disease, and the only prevention is vaccination. This currently poses a problem, since the vaccine was discontinued in 1970 and the WHO declared smallpox eradicated. Incubation is seven to seventeen days, during which the carrier is not contagious. Thirty percent of people exposed are infected, and it has a 30 percent mortality rate.

**Smart grid** The electric delivery network, from electrical generation to end-use customer, integrated with the latest advances in digital and IT to improve customer, integrate with the latest advances in digital and IT to improve electric-system reliability, security, and efficiency.

**Sociopath** Basically synonymous with psychopath (q.v.). Sociopathic symptoms in the adult sociopath include an inability to tolerate delay or frustration, a lack of a conscience, a relative lack of anxiety, a lack of compassion for others, a hypersensitivity to personal ills, and a lack of responsibility. Many authors prefer the term sociopath because this type of person had defective socialization and a deficient childhood.

**Sociopathic** Of, relating to, or characterized by asocial or antisocial behavior or a psychopathic (q.v.) personality, according to *Webster’s*.

**Spore** An asexual, usually single-celled reproductive body of plants such as fungi, mosses or ferns; a microorganism, as a bacterium, in a resting or dormant state.

**System** Any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose.

**Terrorism** Premeditated threat or act of violence against noncombatant persons, property, and environmental or economic targets to induce fear, intimidate, coerce, or affect a government, the civilian population, or any segment thereof, in furtherance of political, social, ideological, or religious objectives.

**Terrorist group** A group which practices or has significant elements which are involved in terrorism.

**Threat** An indication that a harmful incident, such as contamination of the drinking water supply, may have occurred. The threat may be direct, such as a verbal or written threat, or circumstantial, such as a security breach or unusual water quality.

**Toxin** A poisonous substance produced by living organisms capable of causing disease when introduced into the body tissues.

**Transponder** A device on an airliner which sends out signal allowing air traffic controllers to track an airplane. Transponders were disabled in some of the 9/11 hijacked planes.

**Transportation Security Administration (TSA)** A new agency created by the Patriot Act of 2001 for the purpose of overseeing technology and security in American airports.

**Tularemia** An infectious disease caused by a hardy bacterium *Francisella tularensis*, found in animals, particularly especially rabbits, hares, and rodents. Symptoms depend upon how the person was exposed to tularemia but can include difficulty breathing, chest pain, bloody sputum, swollen and painful lymph glands, ulcers on the mouth or skin, swollen and painful eyes, and sore throat. Symptoms usually appear from three to five days after exposures but sometimes will take up to two weeks. Tularemia is not spread from person to person, so people who have it need not be isolated.

**Ultrafiltration** A filtration process for water that uses membranes to preferentially separate very small particles that are larger than the membrane's molecular weight cutoff, typically greater than 10,000 daltons. (A dalton is a unit of mass, defined as 1/12 the mass of a carbon-12 nucleus. It's also called the atomic mass unit, abbreviated as either "amu" or "u").

**Value proposition** A statement that outlines the national and homeland security interest in protecting the nation's critical infrastructure and articulates the benefits gain by all critical infrastructure partners through the risk management framework and public-private partnership described in the NIPP.

**Vector** An organism which carries germs from one host to another.

**Vesicle** A blister filled with fluid.

**Vulnerability** A physical feature or operational attribute that renders an entity open to exploitations or susceptible to a given hazard.

**Weapons of mass destruction (WMD)** According to the National Defense Authorization Act: any weapon or device that is intended, or has the capability, to cause death or serious bodily injury to a significant number of people through the release, dissemination, or impact of

- toxic or poisonous chemicals or their precursors
- a disease organism
- radiation or radioactivity

**Webinar** A live online educational presentation during which participating viewers can submit questions and comments.

**Xenophobia** Irrational fear of strangers or those who are different from oneself.

**Zyklon b** A form of hydrogen cyanide. Symptoms of inhalation include increased respiratory rate, restlessness, headache, and giddiness followed later by convulsions, vomiting, respiratory failure, and unconsciousness. Used in the Nazi gas chambers in World War II.



# Index

- aboveground equipment, 144–46
- access control systems, 154
- active infrared sensors, 169–70
- active security barriers, 150–51, 180–81;
  - crash beam barriers, 150;
  - installation of, 149;
  - portable/removable barriers, 153, 153;
  - retractable bollards, 152, 152;
  - types of, 147;
  - wedge barriers, 147–48, 149
- active shooters:
  - armed attacker, 16, 42;
  - CS sector incidents of, 57–60;
  - Las Vegas shootings, 9–10;
  - in terrorism, 55–57;
  - 2000–2017, 57;
  - 2000–2018, 56;
  - 2018, 57;
  - US incidents of, 56, 56–57
- activities priorities, 16–17
- ADA. *See* American with Disabilities Act
- Aguilar, Darion Marcus, 59
- alarm systems, 154, 156–57
- aluminum beams, 148
- American National Standards Institute (ANSI), 175
- American Society for Testing and Materials (ASTM), 174
- American Society of Sanitary Engineers (ASSE), 145
- American with Disabilities Act (ADA), 24
- annunciator, 155
- ANSI. *See* American National Standards Institute
- anti-terrorism technologies, 31
- antivirus programs, 192
- Argonne Nation Laboratory, 37–38
- armed attacker, 16, 42
- arming station, 155
- ASSE. *See* American Society of Sanitary Engineers
- asset considerations, 65, 98;
  - of entertainment and media industry, 24–25;
  - of gaming industry, 25–26;
  - of outdoor events, 27–28;
  - of public assembly, 28;
  - of real estate industry, 29–30;
  - of retail subsector, 30–31;
  - of sports leagues, 31–32
- asset monitoring, 143–44
- ASTM. *See* American Society for Testing and Materials

- audit mode, 88
- Avery, Lanai Daniel, 59
- Awareness Training, 81–82
- Ayala, Erik Salvador, 59
  
- backflow prevention devices, 159–60
- backpressure, 160
- backsiphonage, 160
- ball valve lockouts, 185
- baseline, establishing, 88
- behavioral problems, 84–85
- behaviors, of insider threats, 85
- benchmarking:
  - of CS sector, 14–19;
  - process of, 19;
  - results from, 18–19;
  - targets for, 19
- biometric hand and finger geometry
  - recognition, 161–62
- biometric iris recognition, 162–63
- biometric measures, 163
- biometric security systems, 160–61
- bistatic sensors, 170
- Blake, Alburn Edward, 59
- bollards (vertical barriers), 151, 151–52
- bonding adhesive, 174
- Botnets, 119–20
- Brown, Elijah J., 58
- buffer overflow, 121
- Building Vulnerability Assessment
  - Checklist, 103–4
- buried line fiber-optic cable sensors, 168
- buried line magnetic field sensors, 168
- buried line ported coaxial cable sensors, 168
- buried line sensors, 168
- buried sensors, 166, 167
- Bush, George W., 75
- butterfly valve lockouts, 185
  
- camera systems, 187–88
- cantilever crash beams, 148, 151
- capacitance sensors, 169
- capital crimes, 3
- card reader systems, 163–66, 165
  
- Carlson, L., 39
- casino gaming complexes, 26
- The Castle of Indolence* (Thomson), 8
- CBECS. *See* Commercial Buildings Energy Consumption Survey
- CCD. *See* Charged Coupled Device
- CCP. *See* Crisis Communications Plan
- CCTV. *See* closed-circuit television systems
- celebrities, 25, 27
- central location, 156
- certificate authority compromise, 122
- Chain-of-Command Chart, 130
- Charged Coupled Device (CCD), 162
- chemical concoctions, 4–6
- chemical industry infrastructure, 202
- CIKR. *See* Critical Infrastructure and Key Resources
- circuits, 154–55
- closed-circuit television (CCTV)
  - systems, 154;
  - security cameras, 137;
  - in visual surveillance system, 186
- CMI. *See* Consequences Measurement Index
- CNCI. *See* Comprehensive National Cybersecurity initiative
- Commercial Buildings Energy Consumption Survey (CBECS), 23
- commercial facilities, 22
- Commercial Services (CS):
  - critical interdependency in, 11;
  - diverse assets in, 10–11, 21;
  - operational risks and, 14;
  - sectors linked to, 11–12;
  - subsectors of, 12–13.*See also* CS sector
- communication systems, 156–57;
  - electronic controllers in, 189–90;
  - half-duplex, 190;
  - integration of, 188–91;
  - security related, 205;
  - two-way radios, 188, 190;
  - WAP, 190–91

- community partnerships, 205–6
- competition, of owners and operators, 30
- components:
  - of card reader system, 163–64;
  - of CS sector, 23–32;
  - of doorways, 182;
  - RMI, 47, 48–49
- Comprehensive National Cybersecurity initiative (CNCI), 75
- computers:
  - antivirus programs for, 192;
  - buffer overflow, 121;
  - firewalls for, 193;
  - with malware, 119–20, 192;
  - with ransomware, 81;
  - specialized software for, 161;
  - with spyware, 192;
  - with Trojan horse programs, 81, 119–20.

*See also* software
- concrete enclosure, 1–2
- Consequences Measurement Index (CMI), 37, 40
- contaminant detection, 202
- contaminants, 139
- contingency planning, 127
- control panel, 155, 161
- corrosion resistant, 178–79
- crash barriers, 146–53
- crash beam barriers, 148, 150
- credential management, 71
- credentials based exploit, 121
- criminal activities, 43, 72, 83, 117–18
- Crisis Communications Plan (CCP):
  - EAPs in, 132–33;
  - emergency planning process of, 129;
  - emergency response plan of, 129–32;
  - goals of, 127–28;
  - incident-specific EAPs in, 133–34;
  - template for, 128–35
- critical asset reduction goal, 65
- critical infrastructure, 200;
  - chemical industry, 202;
  - community partnerships and, 205–6;
  - FBI observes threats against, 117–18, 117–19;
  - insider threats against, 82–83, 86;
  - interdependencies of, 100;
  - physical security of, 96–98;
  - RMI of, 38–39, 45–46;
  - sector, 10;
  - security technologies for, 73;
  - threats to, 37
- Critical Infrastructure and Key Resources (CIKR), 14
- Critical Infrastructure Identification, Prioritization, and Protection, 14
- Critical Infrastructure Protection Task Force, 79
- cross contamination, 159;
- cross-site request forgery, 122
- cross-site scripting, 121
- cryptographic weakness, 121
- CS. *See* Commercial Services
- CS sector, 107;
  - active shooter incidents in, 57–60;
  - activities priorities of, 16–17;
  - benchmarking of, 14–19;
  - CCP template for, 128–35;
  - challenges facing, 69–74;
  - components and assets of, 23–32;
  - contingency planning for, 127;
  - critical dependencies of, 20;
  - data protection in, 72–73;
  - facility differences in, 198–99;
  - facility preparation in, 111–13;
  - facility security of, 200–206;
  - goals and priorities of, 15;
  - HSPD-7 importance to, 74–75;
  - identity management in, 71;
  - infrastructure security in, 139–41;
  - insider threat goal of, 71–72;
  - insider threat protection for, 82–83;
  - insider threats to, 81–82;
  - layered security for, 138–43, 140;
  - multi-barrier approach for, 138–43;
  - operating characteristics of, 22;



- practical standards for, 73–74;
- risks in, 40–43;
- security areas in, 141–42;
- security goals for, 65–66;
- security matrix for, 206, 206–7;
- snapshot of, 22–23;
- soft targets in, 64–65;
- software vulnerabilities in, 69–71;
- threat consequences to, 108;
- threat warning signs in, 108–9;
- VA of, 80–81
- customers, of facilities, 112
- cyber-assessment capabilities, 16
- cyberattacks, 13;
  - firewalls against, 193;
  - goals and attributes for, 65;
  - hackers in, 25, 42, 76, 117–18;
  - infrastructure vulnerable to, 20;
  - on IT, 119–20;
  - on national security, 116–19;
  - protection devices against, 192–96;
  - risks of, 16, 41;
  - by Russia, 119–20;
  - SQL Injection, 121;
  - U.S. DHS identifying risks of, 120, 121–22
- cybersecurity, 75, 141
- cyberterrorism, 116
- data protection, 72–73
- Davis, Ronald Dean, 59
- desk/field exercises, 112–13
- detection devices, 154
- digital cameras, 162
- digital relays, 189
- disruptive events, 46
- diversity, facility and activity, 27–28
- Door Impact Test, 183
- doorways:
  - components of, 182;
  - frames for, 183;
  - metal, 182;
  - performance attributes of, 183;
  - security for, 181–83;
  - side-hinged, 181–83
- double-cylinder locks, 179
- drones, 41
- drone technology, for terrorism, 13
- drop-arm crash beams, 148–49
- dual-technology sensors, 170
- due diligence, 110
- Dylan, Bob, 36
- EAPS. *See* Emergency Action Procedures
- ECIP. *See* Enhanced Critical Infrastructure Protection program
- economic fraud, 83
- Edgewater Technology Inc., 57
- education goals, 66
- 80/20 principle (Pareto analysis), 101
- EINSTEIN system, 75
- electric field or capacitance sensors, 169
- electromechanical relays, 189–90
- electronic controllers, 189–90
- electronic identification systems, 163–66
- Emergency Action Procedures (EAPs), 132–34
- emergency planning process, 129–30
- emergency responders, 138–39
- Emergency Response Plan (ERP), 129–32
- emergency services, 11–12, 17, 25, 31
- emergency shelters, 26, 28–29
- employee/employer actions, 86
- employment screening, 141
- encryption, 193
- energy infrastructure, in US, 79
- energy sector, 12
- Enhanced Critical Infrastructure Protection (ECIP) program, 45
- entertainment and media industry, 22–25
- equipment, 131–32, 144–46
- ERP. *See* Emergency Response Plan
- explosives, 42
- exterior intrusion-buried sensors, 166, 167
- exterior intrusion sensors, 167–70
- external notification lists, 131

- external security, 200
- facilities:
  - commercial, 22;
  - construction of, 111;
  - CS sector differences in, 198–99;
  - CS sector preparation of, 111–13;
  - CS sector security of, 200–206;
  - customers of, 112;
  - fences for, 172–73;
  - nuclear, 82;
  - outdoor equipment enclosures, 143–46;
  - personnel of, 111–12;
  - physical security of, 113–14;
  - religious, 29–30;
  - specific measures for, 206;
  - training for, 112–13;
  - VA of, 86–87
- failure mode and effects analysis (FMEA), 101
- Federal Bureau of Investigation (FBI), 41;
  - infrastructure threats observed by, 117–18, 117–19;
  - insider attacks noted by, 84
- Federal Emergency Management Agency (FEMA), 135
- federal enterprise network, 76
- FEMA. *See* Federal Emergency Management Agency
- fence-associated sensors, 169
- fences:
  - for facilities, 172–73;
  - for physical security, 171–73;
  - taut-wire sensor, 169;
  - types of, 171, 172
- films, glass shattering protection, 173–75
- financial services sector, 12, 17, 96, 184
- financial transaction systems, 70–71
- fire detection systems, 154, 156, 158
- fire hydrant locks, 175–76
- firewalls, 193, 194
- Florida’s Water-Wastewater Agency Response Network (FlaWARN), 204
- FMEA. *See* failure mode and effects analysis
- Ford, Cedric Larry, 60
- Ford, Michael Julius, 58
- freestanding sensors, 169–70
- GAAP. *See* Generally Accepted Accounting Principles
- gaming industry, 23, 25–26
- Garcia-Rodriguez, Jose, 59
- gate barricades, 149–51
- gate valve lockouts, 185
- Generally Accepted Accounting Principles (GAAP), 73
- Giuliani, Rudi, 125
- Glass Pad™, 145–46
- glass shattering protection film, 173–75
- guide words, 102, 102–3
- hackers, 25, 42, 76, 117–18
- hacktivism, 41
- half-duplex communications, 190
- hardware devices, security, 142–88
- hardwired systems, 157–59
- Harmon, Arthur Douglas, III, 59
- hatch security, 176–78
- Hazard and Operability (HAZOP), 101;
  - guide words of, 102, 102–3;
  - parameters of, 102;
  - procedures of, 103
- healthcare, 11
- heap-based buffer overflow, 122
- heat detection sensors, 158
- Hendron, Timothy, 59
- high-priority infrastructure, 14
- homegrown terrorism, 36
- homegrown violent extremists (HVEs), 40
- Homeland Security Advisor Council, 29–30
- Homeland Security Presidential Directive 7 (HSPD-7), 14, 74–75

- Homeland Security Presidential Directive 23 (HSPD-23), 75
- Homeland Security Presidential Directives (HSPD), 66, 67–68
- Homeland Security series, 9–10
- Hot Box® enclosures, 145
- hotels/motels, 26–27
- HSPD. *See* Homeland Security Presidential Directives
- HSPD-7. *See* Homeland Security Presidential Directive 7
- HSPD-23. *See* Homeland Security Presidential Directive 23
- Hurricane Katrina, 36
- HVEs. *See* homegrown violent extremists
  
- IBWA. *See* International Bottled Water Association
- ICS-CERT. *See* Industrial Control Systems Cyber Emergency Response Team
- identity management, 71
- IDSs. *See* intrusion detection systems
- IEDs. *See* improvised explosive devices
- IEEE. *See* Institute of Electrical and Electronic Engineers
- IMCC. *See* Incident Management & Command Center
- impact analysis, 100
- improvised explosive devices (IEDs), 42
- Incident Management & Command Center (IMCC), 52
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), 116
- industry security, 199–200
- information, 72, 141, 162, 202–4
- information technology (IT):
  - cyberattacks on, 119–20;
  - penetration testing of, 96;
  - protection of, 202–3;
  - sector, 12
- infrastructure:
  - chemical industry, 202;
  - CS sector security of, 139–41;
  - cyberattack vulnerability of, 20;
  - FBI observing threats to, 117–18, 117–19;
  - high-priority, 14;
  - interconnected, 41;
  - interdependencies, 100;
  - US energy, 79.
  - See also* critical infrastructure
- Infrastructure Survey Tool (IST), 37, 47
- insider threats:
  - behaviors of, 85;
  - characteristics of, 84–85;
  - against critical infrastructure, 82–83, 86;
  - to CS sector, 81–82;
  - CS sector protection against, 82–83;
  - defining, 83;
  - FBI noting, 84;
  - goals, 66, 71–72;
  - malicious, 84–85;
  - organizational factors to, 85;
  - personal factors in, 84–85;
  - scope of, 83;
  - types, 85–86
- Institute of Electrical and Electronic Engineers (IEEE), 145
- integer overflow, 122
- integration, of communication systems, 188–91
- intellectual property theft, 83
- interconnected infrastructure, 41
- interior intrusion sensors, 156, 157
- International Bottled Water Association (IBWA), 138–39
- Intrusion:
  - exterior buried sensors, 166, 167;
  - exterior sensors, 167–70;
  - interior sensors, 156, 157;
  - manhole sensors of, 180;
  - network hardware/software against, 195–96;
  - sensors, 156;
  - techniques, 76, 81–82

- intrusion detection systems (IDSs), 154, 167–70
- iris recognition technology, 162–63
- ISIL. *See* Islamic State of Iraq and the Levant
- Islamic State of Iraq and Syria (ISIS), 36
- Islamic State of Iraq and the Levant (ISIL), 36
- IST. *See* Infrastructure Survey Tool
- IST RMI Dashboard, 38
- IT. *See* information technology
  
- just-in-time buyers, 27
  
- Kerik, Bernard, 125
- key wrenches, 176
- Ki Yung Park, 58
  
- ladder access control system, 178–79
- LAN. *See* local area network
- Large Water System Emergency Response Outline: Guidance to Assist Community Water Systems in Complying with the Public Health and Bioterrorism Preparedness and Response Act of 2002*, 128
- Las Vegas shootings, 9–10
- law enforcement notification, 109
- layered security, for CS sector, 138–43, 140
- life-cycle costs, 73
- lighting systems, 187–88
- local alarm, 155
- local area network (LAN), 191
- Local Emergency Planning Committees, 135
- Lockey, William, 58
- locks, 178–79
- lodging industry, 23, 26–27
  
- macro-level approach, 98
- malicious insiders, 84–85
- malicious software, 81–82
- malware, 119–20, 192
- manhole intrusion sensors, 180
- manhole lock, 180
- Maroochy Shire wastewater system, 115
- mass hysteria, 6–7
- mass protests, 43
- MAUT. *See* multi-attribute utility theory
- McDermott, Michael M., 57
- McVeigh, Timothy, 126
- media outlets, 25, 109, 131
- memoranda of agreement (MOU/MOA), 52
- metal doors, 182
- Meyers, Myles Wesley, 58
- microwave sensors, 170
- mitigation measures, RMI, 49–51, 50
- monitoring, goals for, 66
- monostatic sensors, 170
- MOU/MOA. *See* memoranda of agreement
- movie studios, 25
- multi-attribute utility theory (MAUT), 39
- multi-barrier approach, 138–43
- multiple access points, 30
- multiple-beam infrared sensors, 170
  
- National Cybersecurity Division (NCSD), 75–76
- National Drinking Water Advisor Council (NDWAC), 198
- National Electrical Codes (NEC), 145
- National Fire Protection Association (NFPA), 24, 145, 155
- National Incident Management System (NIMS), 204
- National Infrastructure Advisory Council, 83
- National Infrastructure Council (NIAC), 46
- National Infrastructure Protection Plan (NIPP), 13–14
- national security, 83–84;
  - cyberattacks on, 116–19;

- interests of, 22
- National Security Directive PPD-8, 39
- National Special Security Events (NSSEs), 21
- natural disasters, 36, 42
- natural hazards, 50
- NC. *See* normally closed circuits
- NCSD. *See* National Cybersecurity Division
- NDWAC. *See* National Drinking Water Advisor Council
- NEC. *See* National Electrical Codes
- Nengmy Vang, 60
- network architecture:
  - access to, 194;
  - federal enterprise, 76;
  - intrusion hardware/software, 195–96;
  - local area, 191;
  - process pipe, 184;
  - public, 193;
  - VA of, 94–95;
  - vulnerabilities of, 69–71
- network honeypot, 195
- NFPA. *See* National Fire Protection Association
- NIAC. *See* National Infrastructure Council
- NIMS. *See* National Incident Management System
- 9/11 attacks, 36, 125–27, 138–39
- NIPP. *See* National Infrastructure Protection Plan
- NO. *See* normally open circuits
- normally closed (NC) circuits, 154
- normally open (NO) circuits, 154
- “No Trespassing” signs, 173
- NSSEs. *See* National Special Security Events
- nuclear facility, 82
- Occupational Safety and Health Administration (OSHA), 24
- on-site/off-site capabilities, 51
- operating characteristics, of CS sector, 22
- operating system command injection, 121
- operational risks, 14
- operations security (OPSEC), 99, 199
- organizational security, 199
- OSHA. *See* Occupational Safety and Health Administration
- outdoor equipment enclosures, 143–46
- outdoor events, 17, 23, 27–28
- owners and operators, 23–24;
  - competition of, 30;
  - risk decreased for, 39
- pandemic, 42
- Pareto analysis (80/20 principle), 101
- passive bollards, 152
- passive infrared (PIR) sensors, 170
- passive security barriers, 180–81
- path traversal, 122
- Patterson, Emanuel Burl, 58
- penetration testing, 96
- Performance Requirements for Outdoor Enclosures for Backflow Prevention Assemblies*, 145
- perimeter intrusion sensors, 156, 157
- perpetrator notification, 109
- personal problems, 84–85
- personnel:
  - of facilities, 111–12;
  - safety, 131;
  - security goals, 65
- pest eradication tools, 192
- PFDs. *See* process flow diagrams
- phishing, 121
- physical asset analysis, 98
- physical security, 140–41, 202;
  - of critical infrastructure, 96–98;
  - of facilities, 113–14;
  - fences for, 171–73;
  - goals, 66;
  - locks for, 179;
  - risk reduction of, 203;
  - VA in, 96–98
- pipng and instrumentation drawings (P&IDs), 101, 103

- PIR. *See* passive infrared sensors
- piracy, 25
- PLCs. *See* programmable logic controllers
- point-of-sale cyber systems, 31
- policies and procedures, 99
- population densities, 22
- portable/removable barriers, 153, 153
- PPD-21. *See* Presidential Policy Directive 21
- practical standards, 73–74
- PRD-21, 68
- preparedness:
  - RMI, 48–49, 49;
  - terrorism, 126–27
- pre-removal risk assessment (PRRA), 101
- Presidential Policy Directive 21 (PPD-21), 37, 66
- pressure sensors, 168
- Private Sector Preparedness Program (PSPrep), 39
- process flow diagrams (PFDs), 101
- process pipe network valves, 184
- programmable logic controllers (PLCs), 189
- protection devices, against cyberattacks, 192–96
- protective security advisors (PSAs), 38
- protests, 41
- protocol analysis, 195
- PRRA. *See* pre-removal risk assessment
- PSAs. *See* protective security advisors
- PSPrep. *See* Private Sector Preparedness Program
- public access, 22
- public assembly, 23, 28
- public network, 193
- Queensland, Australia, 115
- Rack Load Test, 183
- radicalized terrorists, 1–8
- radios, two-way wireless, 188, 190
- ransomware, 81
- real estate industry, 23, 28–30
- Real Estate Information Sharing and Analysis Center (RE-ISAC), 24
- recovery mechanisms, RMI, 52, 52–53
- Reference Manual to Mitigate Potential Terrorist Attacks against Buildings*, 104
- RE-ISAC. *See* Real Estate Information Sharing and Analysis Center
- religious facilities, 29–30
- remote telemetry units (RTUs), 191
- residential property, 29
- resilience, 44;
  - disruptive events and, 46;
  - measures toward, 68
- Resilience Index (RI), 46
- Resilience Measurement Index (RMI), 16–17, 37;
  - component levels of, 48–49;
  - of critical infrastructure, 38–39, 45–46;
  - cyber risks and, 41;
  - IST RMI Dashboard and, 38;
  - level 1 components of, 47, 48;
  - methodology of, 46–47;
  - mitigation measures, 49–51, 50;
  - organization of, 47;
  - preparedness, 48–49, 49;
  - recovery mechanisms, 52, 52–53;
  - relationships in, 47;
  - response capabilities, 51, 51–52;
  - RI revision creating, 46;
  - weakest link found with, 38–39
- “Resilience: Theory and Applications” (report), 46
- response capabilities, RMI, 51, 51–52
- Response Protocol Tool Boxes (RPTBs), 110
- retail subsector, 12–13, 23, 30–31
- retractable bollards, 152, 152
- return-on-investment (ROI), 73
- RI. *See* Resilience Index
- risk:
  - assessment, 74;
  - characterizations of, 100–101;

- in CS sector, 40–43;
  - of cyberattacks, 16, 41;
  - elements of, 40;
  - operational, 14;
  - owners and operators decreasing, 39;
  - physical security reduction of, 203;
  - U.S. DHS identifying cyber, 120, 121–22
- risk management, 80, 88;
  - bowtie diagram of, 45, 46;
  - defining, 44–45;
  - in threat environment, 95
- RMI. *See* Resilience Measurement Index
- ROE. *See* rules of engagement
- ROI. *See* return-on-investment
- RPTBs. *See* Response Protocol Tool Boxes
- RTUs. *See* remote telemetry units
- rules of engagement (ROE), 96
- Russia, cyberattacks by, 119–20
  
- SAFETY Act. *See* Support Anti-terrorism by Fostering Effective Technologies Act
- Schneier, B., 142
- seasonality, 27–28
- Secret Service National Threat Assessment Center, 84
- Sector Coordinating Council, 17
- security:
  - of aboveground equipment, 144–46;
  - active barriers to, 180–81;
  - awareness, 87–88, 200;
  - biometric systems for, 160–61;
  - breach, 108–9;
  - CCTV cameras for, 137;
  - communications related to, 205;
  - critical infrastructure technologies for, 73;
  - CS sector areas of, 141–42;
  - CS sector goals for, 65–66;
  - CS sector infrastructure, 139–41;
  - CS sector layered, 138–43, 140;
  - cybersecurity, 75, 141;
  - for doorways, 181–83;
  - expectations and responsibilities for, 202;
  - external, 200;
  - facility-specific measures on, 200–206;
  - hatch, 176–78;
  - industry, 199–200;
  - information management, 72;
  - matrix, 206, 206–7;
  - operational, 99, 199;
  - organizational, 199;
  - passive barriers to, 180–81;
  - personnel goals of, 65;
  - priorities, 201;
  - skills, 88–89;
  - terrorism and preparedness for, 126–27;
  - threat-level information concerning, 204;
  - VA efforts of, 89;
  - for vents, 185–86
- security hardware:
  - active barriers, 146–53;
  - alarms, 154–59;
  - backflow prevention devices, 159–60;
  - biometric geometry recognition, 161–62;
  - biometric iris recognition, 162–63;
  - biometric systems, 160–63;
  - camera systems, 187–88;
  - card identification systems, 163–66;
  - devices, 142–88;
  - doorway, 181–83;
  - exterior sensors, 166–70;
  - fences, 171–73;
  - fire hydrant locks, 175–76;
  - glass shatter protection, 173–75;
  - hatch, 176–78;
  - ladder access control, 178–79;
  - locks, 179;
  - manhole locks, 180;
  - passive barriers, 180–81;
  - physical monitoring, 143–46;

- valve lockout devices, 183–85;
- vent, 185–86;
- visual surveillance, 186;
- seismic sensors, 168
- sensors, 154–55;
  - active infrared, 169–70;
  - in alarm systems, 156–57;
  - biometric security systems, 160–61;
  - bistatic, 170;
  - buried, 166, 167;
  - buried line, 168;
  - buried line fiber-optic cable, 168;
  - buried line magnetic field, 168;
  - buried line ported coaxial cable, 168;
  - capacitance, 169;
  - dual-technology, 170;
  - electric field, 169;
  - exterior intrusion, 167–70;
  - exterior intrusion-buried, 166, 167;
  - fence-associated, 169;
  - freestanding, 169–70;
  - heat detection, 158;
  - interior intrusion, 156, 157;
  - manhole intrusion, 180;
  - microwave, 170;
  - monostatic, 170;
  - perimeter intrusion, 156, 157;
  - PIR, 170;
  - pressure, 168;
  - seismic, 168;
  - single-beam infrared, 170;
  - taut-wire fence, 169;
  - VMD, 169–70
- Service-Level Agreements, 52
- shopping center subsector, 13
- side-hinged doors, 181–83
- single-beam infrared sensors, 170
- single-cylinder locks, 179
- social media, 41
- soft targets, 10, 22, 64–65
- software:
  - encryption, 193;
  - malicious, 81–82;
  - piracy, 25;
  - specialized, 161;
  - vulnerabilities, 69–71
- Software Engineering Institute, 84
- sports leagues, 23, 31–32
- spyware, 192
- SQL. *See* Structured Query Language
- Injection
- “Standard Test Method for glazing and Glazing Systems Subject to Air Blast Loadings” (ASTM), 174
- standoff distance, 50
- stinky chemicals, 4–7
- streaming video on demand (SVOD), 24
- Structured Query Language (SQL) Injection, 121
- subcontractors, illegal, 29
- suicide bombers, 126
- Superstorm Sandy, 36
- “supervised” systems, 154
- supply chain, 30, 43
- Support Anti-terrorism by Fostering Effective Technologies Act (SAFETY Act), 31–32
- surface-mounted wedges, 147
- surveillance curriculum, 16, 26
- SVOD. *See* streaming video on demand
- switches, 154–55
- Talovie, Sulejman, 58
- targets, 139, 140
- taut-wire sensor fences, 169
- technology, 71;
  - anti-terrorism, 31;
  - card reader system, 164, 165;
  - dual sensors, 170;
  - iris recognition, 162–63;
  - terrorists using drone, 13.
- See also* information technology
- television, 24
- terrorism:
  - active shooters in, 55–57;
  - cyberterrorism, 116;



- defining, 9–10, 55;
- domestic and international threats of, 40–41;
- drone technology for, 13;
- homegrown, 36;
- preferred targets in, 29;
- radicalized, 1–8;
- security preparedness against, 126–27;
- suicide bombers, 126;
- technologies against, 31;
- threat management process for, 110–11
- terror premium, 108
- theft-related crimes, 43
- thioacetone, 5
- Thomson, James, 8
- threat environment:
  - due diligence in, 110;
  - FBI observations of, 117–18;
  - law enforcement notification, 109;
  - management process for, 110–11;
  - perpetrator notification, 109;
  - responses in, 109–11;
  - risk management in, 95;
  - security breaches, 108–9;
  - witness accounts, 108–9
- threat-level information, 204
- threats, 40, 43–44
- threat warning signs, in CS sector, 108–9
- three-dimensional information, 162
- throughput attributes, 65
- timers, 189
- traffic anomaly detection, 195
- traffic lights, 83
- training:
  - awareness, 81–82;
  - for facilities, 112–13;
  - goals, 66
- transportation system, 11
- transportation systems sector, 12
- tree-spiker, 9–10
- Trojan horse programs, 81, 119–20
- trusted third parties, 121
- two-way radios, 190
- two-way wireless radios, 188
- UAS. *See* unmanned aircraft systems
- UL. *See* Underwriters Laboratory
- uncontrolled format string, 122
- Underwriters Laboratory (UL), 156
- unintentional user errors, 121
- United States (US):
  - active shooter incidents in, 56, 56–57;
  - energy infrastructure in, 79
- unmanned aircraft systems (UAS), 43
- unrestricted upload, of files, 122
- US. *See* United States
- U.S. Computer Emergency Response Team (U.S.-CERT), 75
- U.S. Department of Homeland Security (U.S. DHS), 11;
  - coordination improvement of, 16;
  - cyber risks identified by, 120, 121–22;
  - ECIP program of, 45;
  - EINSTEIN system for, 75;
  - NSSEs of, 21
- valve lockout devices, 183–85
- valves, process pipe network, 184
- valve types, 185
- VAs. *See* Veterans Affairs vulnerabilities assessment
- vents, security for, 185–86
- vertical barriers (bollards), 151, 151–52
- Veterans Affairs (VA), 104
- video, 163
- video motion detection (VMD) sensors, 169–70
- violence, 3
- visual surveillance system, 186
- VMD. *See* video motion detection sensors
- volumetric attributes, 65

- vulnerabilities, 40, 44;
  - of financial transaction systems, 70–71;
  - software and network, 69–71
- vulnerabilities assessment (VA), 14, 201;
  - action promoted through, 88–89;
  - Awareness Training in, 81–82;
  - baseline established in, 88;
  - benefits of, 87–89;
  - checklist for, 103–4;
  - of CS sector, 80–81;
  - cyber assets in, 94;
  - elements of, 90–93;
  - of facilities, 86–87;
  - impact analysis in, 100;
  - methodology of, 94–101;
  - of network architecture, 94–95;
  - physical assets in, 94;
  - of physical security, 96–98;
  - policies and procedures in, 99;
  - procedures for, 101–3;
  - process of, 89–94;
  - responses developed from, 88;
  - risk characterizations in, 100–101;
  - security efforts from, 89;
  - what-if analysis in, 101–2
- vulnerability ratings, 164–66
- WAP. *See* Wireless Access Point
- water distribution system, 175
- watering hole, 121
- Water Security Working Group (WSWG), 197
- weather, extremes in, 42
- wedge barriers, 147–48, 149
- Wel Merc, 4, 5, 7
- what-if analysis, 101–2
- Windows and Doors Manufacturers Association, 183
- Wireless Access Point (WAP), 190–91
- Wireless Network Interface Card, 190–91
- wireless radios, 188
- witness accounts, 109
- World Trade Center, 36
- WSWG. *See* Water Security Working Group

