Workplace Violence and Active Assailant—Prevention, Intervention, and Response

ANSI/ASIS WVPI AA-2020 (revision and redesignation of 2011)
Approved May 7, 2020
ASIS International

Abstract

This *Standard* provides an overview of policies, processes, and protocols that organizations can adopt to help identify, assess, respond to, and mitigate threatening or intimidating behavior and violence affecting the workplace. It describes the implementation of a workplace violence prevention and intervention (WVPI) program and personnel within organizations who typically become involved in prevention and intervention efforts. In addition, this Standard now includes an annex which provides actionable information and guidance relative to prevention, intervention, and response to incidents involving an active assailant/active shooter.

ISBN: 978-1-951997-03-8

FOREWORD

The information contained in this Foreword is not part of this American National Standard (ANS) and has not been processed in accordance with ANSI's requirements for an ANS. As such, this Foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the *Standard*.

ANSI guidelines specify two categories of requirements: mandatory and recommendation. The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages.

About ASIS

Founded in 1955, ASIS International is the world's largest membership organization for security professionals. With hundreds of chapters across the globe, ASIS is recognized as the premier source for learning, networking, standards, and research. Through its board certifications, award-winning *Security Management* magazine, and the Global Security Exchange—the most influential event in the profession—ASIS ensures that its members and the security community have access to the intelligence and resources necessary to protect their people, property, and information assets. Learn more about the work we do at **asisonline.org**.

The work of preparing standards and guidelines is carried out through the ASIS International Standards and Guidelines Committees and governed by the ASIS Professional Standards Board. An ANSI-accredited Standards Development Organization (SDO), ASIS actively participates in the International Organization for Standardization (ISO). The mission of the ASIS Professional Standards Board i*s to advance the practice of security management through the development of standards and guidelines within a voluntary, nonproprietary, and consensus-based process, utilizing to the fullest extent possible the knowledge, experience, and expertise of ASIS membership, security professionals, and the global security industry*.

Suggestions for improvement of this document are welcome. They should be sent to ASIS International, 1625 Prince Street, Alexandria, VA 22314-2818, USA.

ASIS Professional Standards Board
Chair: Werner Cooreman, CPP, PSP, Solvay
Vice-Chair: Lisa DuBrock, CPP, Radian Compliance
Charles Baley, Farmers Group, Inc.
Bruce Braes, CPP, PSP, Jacobs UK Ltd.
Robert Carotenuto, CPP, PCI, PSP, The Shed
Michael Crane, CPP, Securisks
David Dodge, CPP, PCI, David Dodge & Associates
David Feeney, CPP, Deloitte and Touche LLP
Linda Florence, CPP, The Florence Group
Tommy Hansen, CPP, Hansen Security Risk Management
Ronald Lander, CPP, Ultrasafe Security Solutions
Bryan Leadbetter, CPP, GM Financial
Ronald Martin, CPP, Open Security Exchange
Juan Muñoz, CPP, Associated Projects International
Angela Osborne, PCI, PSP, Guidepost Solutions
Werner Preining, CPP, Interpool Security
Jeffrey Slotnick, CPP, PSP, Setracon Enterprise Security Risk Management Services
J. Kelly Stewart, Newcastle Consulting, LLC
Timothy Sutton, CPP, Guidepost Solutions
John Villines, CPP, PCI, PSP, John C. Villines LLC
Roger Warwick, CPP, Pyramid Temi Group
Allan Wick, CPP, PCI, PSP, Tri-State Generation & Transmission

The revision of this standard was undertaken with the support and contribution of individuals from both the private and public sectors. The technical committee and working group included experts representing the areas of security, human resources, law enforcement, government, emergency management, fire and life safety, healthcare, behavioral science, psychology, legal, and academia.

At the time it approved this document, WVPI AA Committee, which is responsible for the development of this *Standard*, had the following members:
Committee Members
Committee Chair: Michael Crane, CPP, Securisks
Standards and Guidelines Program Office: Aivelis Opicka, Director, ASIS International
Standards and Guidelines Program Office: Patricia Fusaro, AStd., Manager, ASIS International
Charles Adkins, CPP
Deborah Aebi, McPherson Organization Consultants
Michael Allen, CPP, PCI, PSP, Manulife
George Anderson, Port Authority of NY & NJ
Matthew Anderson, Briggs & Stratton
Richard Axtell, APEMS Solutions LLC
Robert Baggett, CPP, PCI, PSP, USDA Office of Inspector General
Michael Balentine, CPP, ABB Incorporated
Holly Bartecki, Jasculca Terman Strategic Communications

Jay Beighley, CPP, Nationwide Mutual Insurance Company
Peter Bernritter, CPP, Dassault Systems Americas Corp.
William Besse, Avalon Knights LLC
David Bixler, The Boeing Company
Dennis Blass, CPP, PSP, Children of Alabama (Retired)
Steve Brack, CPP, Noble Energy
Chan Browne, Airbus Americas
Robert Buhrmeister, Prudential
Ross Bulla, CPP, PSP, The Treadstone Group, Inc.
Herbert Calderon, CPP, PCI, PSP, CCM2L
John Caldwell, CPP, The Walt Disney Company - Lucasfilm Ltd.
James Cameron, CPP, Security Concepts Group
Edward Carney, CPP, Contra Costa Community College District
Robert Carotenuto, CPP, PCI, PSP, The Shed
James Cawood, CPP, PCI, PSP, Factor One
David Cheuvront, PCI, John Hopkins University Applied Physics Laboratory
Adam Clarke, Fiat Chrysler Automobiles
Ryan Clements, Easterwood Airport Management
Sheldon Cooke, PSP, Canadian Parliament
Patrick Cooper, PCI, Lockheed Martin
William Cousins, CPP, WJ Cousins & Associates
Rhedonda Cox, C-Bond Systems
Kevin Craig, Porzio Compliance Services
Matthew Cresta, Lockheed Martin
David Crevillén, GrupoDC Solutions S.L.U.
Andrew Cuomo, PSP, Chicago Police Department
Luther Cutts, CPP, Wolverine Security Risk Management
Lori Dahm, CPP, Wells Fargo Bank
Eric Davoine, CPP, Axa Partners
Steven Dawson, University of Michigan
Philip Deming, CPP, Philip S Deming & Associates
Kort Dickson, Perdue Farms
Matthew Dimmick, CPP, PSP, STV Inc.
Daniel Donohue, CPP, DGI Security Solutions
Kevin Doss, CPP, PSP, Level 4 Security
Jack Dowling, CPP, PSP, J D Security Consultants
Eric Drewry, CPP, Detroit Institute of Arts
James Dutkowski, PSP, The Stalwart Group
Timothy Easton, Castle Defense 360 Security Consulting and Protection Services LLC
Thomas Frank, CPP, AbbVie
Tracy Frazzano, Montclair Police Department
Lauris Freidenfelds, Telgian Engineering & Consulting
Don Gemeinhardt, University of Phoenix
Craig Gundry, PSP, Critical Intervention Services
Beatriz Gutiérrez López, APP, GrupoDC Solutions
Thomas Hale, CPP, Intuit

Kathryn Hartrick, Hartrick Employment Law, Ltd
Joseph Hendry, PSP, ALICE Training Institute
Laurence Hess, QTS Data Centers
Christina Holbrook, The Boeing Company
Jennifer Holcomb, CPP, PSP, Markon Solutions
Christian Huenke, PCI, Amazon Studios
David Hunt, CPP, Homeland Security Consulting, LLC
Gregory Jarpey, PSP, Northrop Grumman
Celia Jarvis, QMSG Ltd
Donald Jordan, Inter-Sec Group
Edmund Kardauskas, CPP, PCI, PSP, Excaliber Security Services LLC
Anthony Kather, CPP, Redstone Federal Credit Union
Jonathan Kremser, CPP, Kutztown University of Pennsylvania
Bryan Leadbetter, CPP, GM Financial
Derek Lemire, Citizens Financial Group
Mark Lies, Seyfarth Shaw LLP
Gary Lopez, Arthur J. Gallagher Risk Management Service
Melissa Mack, CPP, Willis Towers Watson
Michael Mann, CPP, PSP, Smile Direct Club
Ronald Martin, CPP, Open Security Exchange
Caliph Mathis, S&P Global
Patrick McCarthy, CPP, Western Digital Corporation
Scott McClellan, Schools First Federal Credit Union
Allan McDougall, CPP, PSP, Irving Shipbuilding Industries
James McGinty, Allied Universal Security Service
John McGrath, CPP, Raytheon Missile Systems
James McGuffey, CPP, PCI, PSP, A.C.E. Security Consultants
Norman Merritt, Fortress Consulting
Stanley Mezewski, University of Maryland Baltimore Washington Medical Center
Theodore Miles, CPP
Mark Nagel, City of Orinda
Jonathan Napier, City of Calgary
Christopher Nowlin, S3 Integration, LLC
Larson Parker, Department of Homeland Security CISA
Brian Peters, CPP, Target Corporation
John Petruzzi, CPP, G4S Americas
William Phillips, New Source Security
Jeremy Prout, CPP, International SOS
Joseph Rector, CPP, PCI, PSP, 11th Security Forces Group
Michael Rehfeld, Intrusion Technologies Inc.
Shawn Reilly, CPP, PSP, Tech Systems
Jonathan Rose, CPP, PCI, PSP, National Forensic Consultants
Scott Ruddick, Mennonite Economic Development Associates
Eugene Rugala, Eugene A Rugala & Assocs LLC
James Sanford, SMP Engineering
Jeffrey Sarnacki, CPP, Skylight Global LLC

Jack Schnur, The Gardens Mall
Josh Schubring, CPP, Schubring Global Solutions
William Scott, CPP, ABS Group
Jeffrey Slotnick, CPP, PSP, Setracon Enterprise Security Risk Management Services
Lori Dahm, CPP, Wells Fargo Bank
Eric Davoine, CPP, Axa Partners
Steven Dawson, University of Michigan
Philip Deming, CPP, Philip S Deming & Associates
Kort Dickson, Perdue Farms
Matthew Dimmick, CPP, PSP, STV Inc.
Daniel Donohue, CPP, DGI Security Solutions
Kevin Doss, CPP, PSP, Level 4 Security
Jack Dowling, CPP, PSP, J D Security Consultants
Eric Drewry, CPP, Detroit Institute of Arts
James Dutkowski, PSP, The Stalwart Group
Timothy Easton, Castle Defense 360 Security Consulting and Protection Services LLC
Thomas Frank, CPP, AbbVie
Tracy Frazzano, Montclair Police Department
Lauris Freidenfelds, Telgian Engineering & Consulting
Don Gemeinhardt, University of Phoenix
Craig Gundry, PSP, Critical Intervention Services
Beatriz Gutiérrez López, APP, GrupoDC Solutions
Thomas Hale, CPP, Intuit
Kathryn Hartrick, Hartrick Employment Law, Ltd
Joseph Hendry, PSP, ALICE Training Institute
Laurence Hess, QTS Data Centers
Christina Holbrook, The Boeing Company
Jennifer Holcomb, CPP, PSP, Markon Solutions
Christian Huenke, PCI, Amazon Studios
David Hunt, CPP, Homeland Security Consulting, LLC
Gregory Jarpey, PSP, Northrop Grumman
Celia Jarvis, QMSG Ltd
Donald Jordan, Inter-Sec Group
Edmund Kardauskas, CPP, PCI, PSP, Excaliber Security Services LLC
Anthony Kather, CPP, Redstone Federal Credit Union
Jonathan Kremser, CPP, Kutztown University of Pennsylvania
Bryan Leadbetter, CPP, GM Financial
Derek Lemire, Citizens Financial Group
Mark Lies, Seyfarth Shaw LLP
Gary Lopez, Arthur J. Gallagher Risk Management Service
Melissa Mack, CPP, Willis Towers Watson
Michael Mann, CPP, PSP, Smile Direct Club
Ronald Martin, CPP, Open Security Exchange
Walter Sparks, Southern Security Consultants
J Kelly Stewart, Newcastle Consulting, LLC
Sallie Stone, Hart International Australia

Jordan Strauss, Kroll Inc.
John Strawn, Blue Cross Blue Shield of Nebraska
Bryan Strawser, CPP, Bryghtpath
Timothy Sutton, CPP, Guidepost Solutions
Scott Taylor, CPP, Southern Cross Group
Jesse Taylor, CPP, VTI Security
James Terman, Jasculca Terman Strategic Communications
Mark Theisen, CPP, Thrivent Financial
Jeffrey Torain, CPP, 20th Judicial Circuit of FL
Jeff Trinidad, CPP, L3 Harris Technologies
Kirk Turner, Tarleton State University
Herbert Ubbens, CPP, PSP, Paratus Consultants Group, LLC
JoAnn Ugolini, CPP, Control Risks
Brian Uridge, CPP, University of Michigan
Anthony Valicenti, Department of Homeland Security
Ray Van Hook, CPP, AbbVie
Shawn VanSlyke, Control Risks
Sean Varney, CPP, PSP, Swedish Medical Center
G. Michael Verden, The Lake Forest Group
Joshua Villines, CPP, PCI, PSP, Human Intelligence Group
Erika Voss, Salesforce
Ted Wade, All Hazards Security, LLC.
John Ward, Stroud Area Regional Police Department
James Whitaker, CPP, PCI, Cincinnati Children's Hospital Medical Center
John Whitney IV, Scottsdale Fire Department
Allan Wick, CPP, PCI, PSP, Tri State Generation & Transmission
William Wills, CPP, Briggs and Stratton
Kevin Wilson, Asurion
Nancy Zarse, The Chicago School of Professional Psychology

Working Group Members
Working Group Chair: Michael Crane, CPP, Securisks
Melissa Mack, CPP, Willis Towers Watson
Michael Allen, CPP, PCI, PSP, Manulife
Herbert Calderon, CPP, PCI, PSP, CCM2L
Robert Carotenuto, CPP, PCI, PSP, The Shed
James Cawood, CPP, PCI, PSP, Factor One
Patrick Cooper, PCI, Lockheed Martin
Rhedonda Cox, C-Bond Systems
Eric Davoine, CPP, Axa Partners
Kort Dickson, Perdue Farms
Kevin Doss, CPP, PSP, Level 4 Security
Thomas Frank, CPP, AbbVie
Craig Gundry, PSP, Critical Intervention Services
Beatriz Gutiérrez López, APP, GrupoDC Solutions
Thomas Hale, CPP, Intuit

Celia Jarvis, QMSG Ltd
Bryan Leadbetter, CPP, GM Financial
Allan McDougall, CPP, PSP, Irving Shipbuilding Industries
Eugene Rugala, Eugene A Rugala & Assocs LLC
Jack Schnur, The Gardens Mall
Timothy Sutton, CPP, Guidepost Solutions
James Terman, Jasculca Terman Strategic Communications
JoAnn Ugolini, CPP, Control Risks
Shawn VanSlyke, Control Risks
John Whitney IV, Scottsdale Fire Department

ASIS International acknowledges the contributions of the following volunteers in preparing the initial draft that served as the starting point for Annex A - Active Assailant:
Chair: Michael Crane, CPP, Securisks
Holly Bartecki, Jasculca Terman Strategic Communications
David Bixler, The Boeing Company
James Cawood, CPP, PCI, PSP, Factor One
Kevin Doss, CPP, PSP, Level 4 Security
Thomas Frank, CPP, AbbVie
Tracy Frazzano, Montclair Police Department
Christina Holbrook, The Boeing Company
Mark Lies, Seyfarth Shaw LLP
Eugene Rugala, Eugene A Rugala & Assocs LLC
James Terman, Jasculca Terman Strategic Communications
JoAnn Ugolini, CPP, Control Risks
Ray Van Hook, CPP, AbbVie
Shawn VanSlyke, Control Risks
G. Michael Verden, The Lake Forest Group
John Whitney IV, Scottsdale Fire Department
Nancy Zarse, The Chicago School of Professional Psychology

Executive Summary

All organizations have a responsibility to protect employees and others by taking measures to detect threats of violence, intervene through incident management, and mitigate consequences should violence erupt. Organizations that cannot manage and prevent workplace violence may experience disrupted productivity, low morale, and a public image that communicates a disregard for employee safety.

The *Standard* defines workplace violence as "A spectrum of behaviors, including overt acts of violence, threats, and other conduct that generates a reasonable concern for safety from violence, where a nexus exists between the behavior and the physical safety of employees from any internal or external relationship."

A workplace violence prevention and intervention (WVPI) program should state the employer's commitment to providing a safe workplace. It should also define unacceptable behavior; regulate weapons; facilitate prompt reporting; assure that reports will be treated with discretion and investigated; include a commitment to nonretaliation; and impose disciplinary actions.

A WVPI program should include a multidisciplinary team that is trained to evaluate and respond to violent incidents or reports of concerning behavior. This team, commonly known as a Threat Management Team, will assess, investigate, manage, and resolve reports made under the organization's WVPI policy. The team will also be prepared to work with law enforcement and emergency responders if violence occurs.

Response to a violent action must also be considered in the WVPI plan. The organization must be prepared to notify individuals about the danger, prepare employees to evacuate or shelter in place, coordinate with law enforcement and first responders, help contain the violence within a perimeter, establish reunification zones and provide first aid, and communicate with the public and the media, among other things. Once the incident is over, the plan should be evaluated and improved.

1. Scope

This *Standard* provides an overview of policies, processes, and protocols that organizations can adopt to help identify, assess, respond to, and mitigate threatening or intimidating behavior and violence affecting the workplace. It describes the implementation of a workplace violence prevention and intervention (WVPI) program and personnel within organizations who typically become involved in prevention and intervention efforts. In addition, the Standard now includes an annex which provides actionable information and guidance relative to prevention, intervention and response to incidents involving an active assailant/active shooter.

This *Standard* is meant to serve as a tool and resource that organizations of any size can use to evaluate, develop, and implement policies, structures, and practices related to workplace violence. This Standard remains at a generic level, adapted to the multidisciplinary roles of the stakeholders involved in the incident management process, while integrating specificity and detail as appropriate to the organization consistent with applicable legal and regulatory requirements.

The *Standard* reflects a consensus among professionals from several disciplines including security, human resources, mental health, law enforcement, and legal arenas regarding best practices viewed as effective, recommended, and in some cases essential through work in this field. In many ways, this Standard will help organizations to discharge important legal responsibilities related to their need to maintain a safe workplace; it is not intended, though, to set or define new legal obligations.

This Standard is applicable to any organization that chooses to establish, implement, maintain, and improve upon its:

- WVPI program;
- Threat assessment and management protocols; and
- Practices that can assist the organization in effectively managing post-incident issues.

2. Normative References

This document does not contain normative references.

3. Definitions

For the purposes of this *Standard,* the following terms and definitions apply

3.1 active assailant A person or group of people actively engaged in the killing or attempted killing of individuals in an area that is populated or defined by an activity.
3.2 business continuity Ability of an organization to operate at predefined levels following a disruptive event.
3.3 crisis management Holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience, with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities—as well as effectively restoring operational capabilities.

NOTE: Crisis management also involves the management of preparedness, mitigation, response, continuity, or recovery in the event of an incident—as well as management of the overall program through training, rehearsals, and reviews to ensure that preparedness, response, and continuity plans stay current and up to date.

3.4 emergency Serious, unexpected, and precarious situation requiring immediate action.

3.5 emergency operations center Central command and control facility responsible for carrying out the principles of emergency preparedness and emergency management, or disaster management functions at a strategic level during an emergency, and ensuring the continuity of operation of an organization, political subdivision or other organization.

3.6 emergency responder Individual(s) first on the scene at a disruptive incident.

NOTE: Includes employees or other individuals trained to respond to an incident.

3.7 employee assistance program An employee benefit involving mental health counseling offered by some employers.

3.8 first responder A member of an emergency service who is first on the scene at a disruptive incident.

NOTE: Emergency services include any public or private service that deals with disruptions, such as the initial responding law enforcement officers, other public safety officials, emergency medical personnel, rescuers and/or other emergency response service providers.

3.9 fitness for duty examination A process at times imposed by an employer when an employee exhibits behavior that does not generate a concern for safety from violence but that impedes job functioning and could be related to a physical, mental, or emotional disorder.

3.10 incident An event with consequences that has the capacity to cause gains or losses/harm to objectives and/or assets.

3.11 incident commander (IC) Person on the scene with overall incident management responsibility.

3.12 incident management Processes, strategies, methods, and tactics used to manage an incident.

3.13 intimate partner violence Abusive behavior(s) in an intimate relationship, including marriage, cohabitation, dating, family, or friendship.

NOTE: Intimate partner violence can consist of physical aggression, threats, stalking, sexual abuse, psychological abuse, neglect, economic deprivation, and any form of threatening, injurious, and violent acts.

3.14 lock down A state of isolation or restricted access instituted as a security measure.

3.15 policy Overall intentions and direction of an organization, as formally expressed by top management.

3.16 procedure An established or specified way to conduct an activity or a process.

3.17 resources Any asset (human, physical, information, or intangible), facilities, equipment, materials, products, or waste that has potential value and can be used.

3.18 response plans Documented collection of procedures and information that is developed, compiled, and maintained in readiness for use in an incident.

3.19 risk assessment Overall and systematic process of evaluating the effects of uncertainty on achieving objectives.

NOTE: Risk assessment includes risk identification, risk analysis, and risk evaluation.

3.20 risk management Strategic business discipline that supports the achievement of an organization's objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as an interrelated risk portfolio.

3.21 safety Freedom from danger, risk, or injury.
3.22 secure area A location that is free from danger or attack.
3.23 security The condition of being protected against hazards, threats, risks, or loss.
NOTE 1: In the general sense, security is a concept similar to safety. The distinction between the two is an added emphasis on being protected from dangers that originate from outside.
NOTE 2: The term security means that something not only is secure, but that it has been secured. [ANSI/ASIS SPC.1-2009]
3.24 shelter in place The act of finding a safe location or refuge in a building one is occupying.
3.25 stakeholder Person or organization with an interest or concern.
NOTE: A stakeholder can affect and may be affected by the organization and its achievement of its objectives (real or perceived).
3.26 tabletop exercise Pre-scripted scenario using a test method that presents a limited simulation of an emergency or crisis scenario in a narrative format in which participants review and discuss, but not perform, the policy, methods, procedures, coordination, and resource assignments associated with plan activation.
3.27 threat Any verbal or physical conduct that conveys an intent or is reasonably perceived to convey an intent to cause physical harm or to place someone in fear of physical harm.
3.28 threat assessment A process that attempts to predict the likelihood that an individual will commit a violent act.
3.29 top management Directors, managers, and *officers* of an organization that can ensure effective management systems -- including financial monitoring and control systems -- have been put in place to protect assets, earning capacity, and the reputation of the organization.
3.30 vulnerability State of being susceptible to harm or injury.
NOTE: Susceptibility to negative outcomes of a risk.
3.31 workplace violence A spectrum of behaviors, including overt acts of violence, threats, and other conduct that generates a reasonable concern for safety from violence, where a nexus exists between the behavior and the physical safety of employees from any internal or external relationship.
3.32 workplace violence prevention policy A written policy adopted by an organization that strictly prohibits violence and threats affecting the workplace, as well as other behavior deemed inappropriate by the organization from a violence-prevention standpoint.
3.33 workplace violence prevention and intervention program A coordinated collection of policies, procedures, and practices adopted by an organization to help prevent workplace violence and to assist the organization in effectively responding to reports of problematic behavior made under the organization's workplace violence prevention policy.

4. Defining the Reach of Prevention and Intervention Efforts

4.1 General

No organization, large or small, public or private, for-profit or in the nonprofit sector, can assume that it will be immune to the wide range of disturbing, threatening, and violent conduct that falls within the broad definition of "workplace violence." All organizations ultimately carry a responsibility, both for humanitarian and legal reasons, to protect employees and others who interact with the workplace to the fullest practical extent by taking measures to detect threats at

the earliest possible moment, engage in effective intervention through careful incident management, and mitigate consequences should violence erupt.

Education and awareness about workplace violence—its nature and scope, an employer's obligation to address this complex problem, and the practical steps that can be taken to ensure adequate prevention and management–lie at the heart of successful workplace violence prevention and response efforts. An integrated, multidisciplinary approach is vital to a successful workplace violence program. No one sector of an organization can successfully act alone to prevent violence, and no one profession or discipline possesses the skills and capabilities needed to design, implement, and administer a successful workplace violence prevention and intervention (WVPI) program.

A successful workplace violence prevention program begins at the top, with a firm commitment from executive management for a safe and respectful workplace. Responsibility for a WVPI program then falls on an array of professionals within an organization who can bring their skills to bear on this complex problem. Together, different stakeholders within an organization (assisted by outside experts as necessary) can work to develop and implement a prevention and intervention program that brings structure, predictability, and consistency to the handling of the wide range of behaviors and circumstances that can jeopardize workplace safety.

The benefits of adopting a proactive and reasoned approach to workplace violence are many. Disturbing, threatening, and violent behavior affects more than just the person or persons directly threatened or harmed. Beyond questions of legal liability and other tangible financial costs (which can be staggering), organizations that lack effective means of detecting, managing, and preventing workplace violence will meet up with more fundamental costs in the form of disrupted productivity, low employee morale, and a public image that potentially communicates a disregard for employee safety. Alternatively, an organization that properly manages workplace violence risk not only can avoid costly incidents, but will also benefit from feelings of confidence, security, and safety that characterize a successful organization
.
Ultimately, workplace violence—in its many forms—presents one of the most challenging problems that an organization can face. It is the intent of this Standard to provide information and practical steps that will enable an organization to develop an effective and informed approach to this important workplace issue.

4.2 A Working Definition of "Workplace Violence"

An organization that chooses to develop and implement a WVPI program should begin by considering the scope of the program. An organization should engage in efforts designed to prevent and/or mitigate all forms of violence (e.g., assault, battery, deadly force, etc.). Organizations more often will find themselves needing to manage an array of behaviors that falls short of homicide or even simple assault. The spectrum of behaviors that may lead to workplace violence is broad. It includes not only threats, but harassing and intimidating behaviors that are disruptive and potentially dangerous.

The context in which problematic behavior can occur is diverse. The perpetrators themselves also add a complicating dimension given that violence and threats can occur at the hands of a:

- Current or former employee;
- Independent contractor or temporary worker;
- Past, current, or prospective client or customer;
- Family member or partner of an employee;
- Vendor or someone providing professional services to an organization; Shareholder; or
- Person with no apparent connection to the organization.

Given those complexities, a working definition of workplace violence for purposes of establishing the scope of an organization's prevention and intervention efforts should capture a spectrum of behaviors implicating workplace safety while also avoiding overreaching. A working definition should encompass all conduct that could be associated with a potential escalation to violence that an organization will be called on to intervene in. Namely:

- All forms of violence (irrespective of perceived harm or severity) such as aggressive or intimidating behaviors (including bullying and harassment); physical violence, self-harm, or harm toward a person or organization, as well as threats of violence, whether direct or indirect; and
- Behavior that has generated a concern for safety from violence due to its nature and severity. This category includes a variety of conduct that may act as potential "warning signs" or precursors to possible violence. It includes behavior that (from the perspective of a reasonable person) has generated a concern indicating someone may act out violently. Some examples include:
    - Stalking;
    - Erratic and bizarre behavior;
    - Physical intimidation and aggression;
    - Infatuation with violence; and
    - Suicidal statements.

The definition should include these behaviors for several important reasons:

- The behavior is disruptive in and of itself, whether or not it progresses to actual violence;
- The behavior offers a chance at intervention before it can progress to violence; and
- The conduct can be seen as putting an organization "on notice" of possible violence, triggering important legal obligations for the organization to act.

As an important aspect, the definition should limit itself to behavior relevant to workplace safety; it must have a nexus to the workplace, even if it does not occur strictly at the workplace. Tracking the reach of an organization's legal liability, the definition should consider any behavior that has a foreseeable impact on safety at the workplace or during work-related activities. Along those same lines, the definition should consider that the victim or target can be anyone, so long as, again, a nexus exists to the workplace. So, for instance, the victim or target can be an employee or a visitor to the workplace or to an organization-sponsored event (such as a vendor, client, and so forth).

Synthesizing the above broad principles, an organization, in determining the scope of its prevention and intervention efforts, should view workplace violence as:

A spectrum of behaviors, including overt acts of violence, threats, and other conduct that generates a reasonable concern for safety from violence, where a nexus exists between the behavior and the physical safety of employees from any internal or external relationship.

4.3 Legal, Regulatory, and Contractual Requirements

An organization that chooses to adopt workplace violence prevention, assessment, and intervention efforts shall identify and address applicable legal, regulatory, and contractual obligations that affect the scope of those efforts and the manner in which they can be implemented. For example, the organization shall consider:

- Applicable requirements and guidelines promulgated by various governmental occupational safety and health organizations both at the country level, as well as the state, province, canton, county, city level, etc.;
- Common principles and local laws and ordinances that define required prevention, assessment, and intervention efforts, such as:
    - Duty of care;
    - Reporting requirements;
    - Premises security and liability;
    - Respondeant superior;
    - Negligence theories; and
    - Discrimination and harassment laws and regulations.
- Any obligations under an applicable collective bargaining agreement, for example any requirements related to reporting of safety concerns or conduct of investigations.

The organization shall consider all of these elements and review them periodically to address evolving laws, regulations, and contractual requirements.

5. Establishing Multidisciplinary Involvement

Due to the complex and multidimensional nature of workplace violence, effective prevention, assessment, and intervention along with response strategies require a multidisciplinary approach involving the participation of multiple stakeholders within an organization. Workplace violence is not exclusively a security, human resources, employment law, management, employee health, safety, or behavioral problem, but rather it involves all of these disciplines.

An organization should develop and implement prevention and intervention strategies and assign roles and responsibilities for:

- Developing and implementing the WVPI program;
- Conducting ongoing threat management; and
- Periodically assessing the effectiveness of the program.

The organization shall consider the involvement of personnel listed in the subsections below.

5.1 Top Management

Effective WVPI efforts require a clear top-down commitment to ensure that the right resources are allocated to develop a WVPI program; to effectively carry out incident management; and to secure training, outside consulting, security measures, and other needs essential to successful prevention and intervention efforts.

An organization that chooses to implement prevention and intervention strategies should obtain the participation of top management in:

- Establishing the WVPI program as an organizational priority amongst senior leadership;
- Reviewing and approving a WVPI policy;
- Designating appropriate personnel to develop, implement, and monitor the WVPI program;
- Providing resources and authorizations to establish, implement, operate, monitor, and maintain the program through employee training and education; and
- Providing resources and authorizations as required during incident management.

5.2 Key Stakeholders

An organization should strive to engage all employees in the process of creating a safe and secure work environment. However, depending on the size, resources, preferences, and internal workings of an organization, the major responsibility for establishing a WVPI program–and conducting incident management—will largely fall on the key stakeholders of human resources, security, and legal.

5.2.1 Human Resources

Human resources (HR) personnel commonly play a central role in establishing and implementing an organization's violence prevention and intervention strategies, typically as part of broader responsibilities in the area of employee relations management. In many organizations, HR may occupy a leadership role in:

- Developing the WVPI program and supporting policies, procedures, and practices;
- Organizing and/or conducting training;
- Enforcing workplace violence prevention policies and procedures; and
- Managing employee assistance programs and employee resources.

Employees often will direct their concerns or complaints about threatening behaviors, threats, or acts of violence to HR. After receiving a report, HR often will contribute key skills to incident management, including—but not limited to—coordinating with appropriate WVPI team members and other personnel, conducting or assisting with the investigations process, communicating with affected or involved employees, and providing input as the organization attempts to resolve a report, as well as implementing corrective actions where needed.

In workplaces where employees are represented by a union, HR also may become involved in negotiating with labor representatives regarding policies and procedures established under the organization's WVPI program, including disciplinary measures to be taken following policy violations.

5.2.2 Security

Workplace violence prevention typically will find core support and involvement among security personnel already oriented around questions of workplace safety.

Depending on their training and experience, security personnel can contribute practical expertise on a range of topics related to prevention, assessment, and intervention—such as on-site physical security, employee background screening and other investigations, threat assessment, and incident management, as well as coordination with law enforcement.

In addition, like HR, security personnel often will be the first contacted about a threat or violent incident and will assist in providing an appropriate initial response. During an incident, security personnel may become involved in controlling and securing the worksite and assisting law enforcement and other public safety responders.

5.2.3 Legal Counsel

Legal counsel is tasked with helping an organization to understand and comply with legal obligations related to WVPI. Accordingly, legal counsel should have the appropriate training, education, and experience in a variety of disciplines (e.g., employment law, civil litigation, premises liability, etc.) to provide analysis and recommendations. Legal counsel—whether from an organization's own legal department or from an outside law firm—should involve itself in ensuring that the organization has met legal requirements related to violence prevention and that it properly navigates the numerous legal issues that arise during all phases of incident management. In addition, legal may have insight into ongoing litigation, filed complaints, and other actions that can trigger situations of concern. These matters should be brought to the team's attention and discussed when applicable.

Before an incident, counsel can serve a crucial role in helping management to develop appropriate and legally compliant policies, procedures, and practices related to threat and violence assessment, prevention, and intervention. This may include contractually required suppliers and vendors to provide information concerning known behavior. During an incident, counsel should work in close coordination with HR, security, and other involved management to advise the organization regarding such matters as:

- Legal issues that commonly arise during incident assessment and management, including—but not limited to—rights to privacy, compliance with the organization's established policies and procedures, legal obligations, relevant statutes, evidence preservation, due process, and disciplinary protocols as applicable;
- Comprehensive investigations or fact-finding techniques;
  Appropriate employee disciplinary or other remedial steps;

- Potential legal risks and liabilities raised by courses of action the organization might have under consideration, and weighing legal exposure against any countervailing security, confidentiality, or other threat mitigation actions or concerns; and
- In appropriate circumstances, legal counsel may also lead efforts to obtain corporate restraining orders or engage in other legal processes.

5.2.4 Occupational Safety and Health Personnel

Ideally, workplace violence prevention, intervention, and response should be viewed as an integral part of an organizations' s comprehensive occupational injury and illness prevention program. As such, the participation of safety and health personnel in the organization's emergency plans, primarily as emergency responders, play a vital role in employee safety post an incident. In addition, these personnel may be the first to be notified of an incident, a victim, or unsafe condition that warrants their expertise as well as the involvement of the workplace violence and intervention team.

5.2.5 Union Leaders

In organizations that have collective bargaining agreements, unions are legally empowered to represent the workforce and bargain with employers regarding the terms and conditions of employment, including disciplinary policies and procedures and employee rights that apply during efforts to prevent violence or manage an incident. In industries such as healthcare, education, and social services, collective bargaining entities may be involved in developing and implementing successful workplace violence prevention, intervention, and response programs. Establishing labor involvement in the development of workplace violence policies and procedures can help promote an informed workforce and a collaborative relationship with respect to safety issues that impact everyone.

5.2.6 Employee Assistance Programs

Employee assistance program personnel may become involved in prevention and intervention efforts in several ways:

- As part of efforts to resolve an incident, an employee who has been found to have engaged in concerning behavior may be referred to employee assistance program for counseling as part of a remedial or corrective plan;
- An employee assistance program may be engaged to provide psychological counseling to employees or work groups affected by a threat or violent incident; and
- While normally bound by obligations of confidentiality, employee assistance program personnel involved in counseling an employee may receive information that triggers an obligation to warn the employer of a threat posed by the employee.

Depending on the employee assistance program relationship with and role within the organization, employee assistance program personnel who have received specialized training in violence assessment may be called upon to conduct an initial violence risk screening, unless prohibited from doing so by obligations of confidentiality or other legal or ethical restrictions.

5.2.7 Crisis Management Personnel

Crisis management personnel can play a vital role in ensuring that the organization's WVPI program includes means to address and recover from emergency situations caused by a violent incident or threat. Crisis management personnel can contribute their expertise in developing a crisis management process that includes a consideration of possible violent incidents or threats and that is fully integrated into the organization's broader crisis management and recovery plans.

5.2.8 Risk Management Personnel

Risk management personnel help to ensure that workers' compensation and other liability insurance policies are maintained at appropriate levels of coverage, so that the organization is adequately insured against any losses from a violent workplace incident. Such personnel, in their risk management role, can also support efforts by the organization to implement a WVPI program as part of the organization's overall risk management practices.

5.2.9 Business Continuity Personnel

Business continuity personnel develop practices and systems that aid in the management of operations from the onset of a disruption through the recovery period.

Therefore, these personnel can play a key role in helping to develop measures to assist in the identification of the essential functions and operations that would be essential to address during workplace violence events, how to move or continue these functions and operations during violent events, and how to reestablish normal operations after the event is safely resolved.

5.2.10 Public Relations/Corporate Communications

Specialists in the area of public relations and corporate communications can help the organization manage the media and other outside parties. In addition, corporate communications may play a role in helping to develop internal communications that inform employees of the organization's WVPI program, related policies and procedures, and incident-related communications.

6. Planning The Workplace Violence Prevention and Intervention Program

6.1 Conducting a Needs Assessment

In developing a WVPI program, organizations should conduct a needs assessment designed to identify, evaluate, and prioritize the presence of risks of violence affecting the workplace (whether from internal or external sources), and the organization's readiness to respond to concerning behaviors, threats, and violent incidents. This assessment will help the organization understand its safety and security needs and effectively focuses its workplace violence initiatives.

6.1.1 General Approach

As a general approach, prior to designing a WVPI program, an organization should evaluate factors related to possible violent events; their impact on employee welfare and the organization itself; and the organization's policies, practices, and structures as they relate to the organization's current ability to prevent violence and properly intervene when threats and violent incidents occur. For additional guidance, refer to the ANSI/ASIS R*isk Assessment Standard and ASIS Enterprise Security Risk Management Guideline*.

6.1.2 Assessing the Organization's Vulnerability to Violence

An organization should begin by examining its vulnerability to violence from external and internal sources based on the nature of the organization, including the type of industry to which it belongs and other factors. In addition, careful consideration should be given to understanding all the different relationships and potential sources of conflict that could lead to violence on an organization's premises or in relation to organizational activities. Types of relationships include but are not limited to:

- Current and former employees;
- Customers;
- Vendors;
- Contractors and other individuals working with or on behalf of the organization;
- Friends, family members, intimate partners;
- Visitors and guests; and
- Individuals in opposition of the organization's mission, goals, objectives, etc.

In addition to considering the types of relationships, an organization should consider other factors that can affect exposure to possible violence.

Additional considerations include but are not limited to:

- Do employees work during hours of darkness?
- Do employees work alone and/or remotely?
- Is the workplace located in an area at high risk of crime?
- Do employees handle cash or other valuable/desirable goods?
- Is your organization/location open to the public?
- Are alcohol or other intoxicants served or sold?
- Are there disgruntled or unhappy employees who have exhibited concerning behavior at the location?
- Do employees interact with individuals experiencing medical or psychological issues?
- Do employees work in high-risk healthcare environments?
- Are there any current or pending organizational events or conditions which may contribute to unusual tension and/or stress, or conflicts affecting employees?

6.1.3 Evaluating Current Prevention and Intervention Practices

In performing a needs assessment, the organization should also conduct a detailed evaluation of its current violence prevention and intervention practices. In doing so, the organization shall evaluate how current policies, procedures, and practices compare to those required or recommended in this *Standard* and (by doing so) identify gaps.
In that evaluative process, the organization can ask, among others, a variety of questions:

- Does the organization have any violence prevention policies or programs in place, either as stand-alone policies or procedures, or integrated in other broader policies or procedures?
- Is management supportive of violence prevention efforts? Is there a top-down commitment to violence prevention?
- Does the organization enforce standards of professionalism and respect through appropriate discipline and identify clear lines of appropriate workplace behavior?
- Does the workplace, as a cultural matter, care about safety and encourage employees to report circumstances of concern?
- Does the organization periodically conduct violence prevention training?
- Are employees aware of the organization's policies or programs related to workplace violence and procedures for reporting incidents?
- Does the organization have an established practice for managing reports of behavior that raise safety and/or security concerns, and a centralized way to record and track reports over time? If so, how effective are those practices?
- Does the organization have processes in place to manage incidents in remote locations?
- Has the organization established trusted relationships with threat assessment professionals and legal counsel who can assist during the process of assessment and incident management?
- Does the organization conduct employee background screening and implement safety and security procedures for terminating employment and/or business relationships?
- Does the organization have protocols in place for managing workplace emergencies?
- Are employees trained to recognize the warning signs of concerning behaviors?
- Are employees trained in methods of de-escalating concerning behaviors?
- Does the organization have a documented process for ongoing review of the efficacy of the WVPI program?

6.1.4 Evaluating Physical Security

As part of its needs assessment, the organization should also examine elements affecting physical security, including but not limited to such factors as:

- Are entrances and exits clearly marked and controlled to prevent unauthorized entry?
- Are there security personnel on site?
- Are visitors signed in and accompanied by employees while on site?
- Is lighting adequate?
- Are current floor plans posted to show all possible escape routes in case of emergency?

- Are there potential safe shelters that employees can go to if evacuation is not possible?
- Is parking on site? If so, is it secure?
- Are emergency buttons or other alarm procedures in place and assessed for effectiveness?
- Are there cameras at various locations around the property that are either monitored or recorded?
- Are entrances and parking lots readily visible?
- Is office furniture positioned for effective evacuation?
- Can doors and windows be secured?
- Are there sitewide communication and/or mass alert and notification systems?

6.2 Elements of a Workplace Violence Prevention and Intervention Program

Establishing a program that outlines policies, procedures, and practices for WVPI will help ensure that an organization will be adequately prepared to recognize and effectively respond to behavior and circumstances that pose a threat of violence.

Organizations retain wide latitude in developing a program of violence prevention and intervention, depending on the organization's size, resources, and needs. Whatever the specifics of the workplace violence program the organization implements, it should include the following general components as detailed in the subsections below.

6.2.1 Workplace Violence Prevention and Intervention Policy

A WVPI program shall include a policy that is clearly communicated to employees at the time of hire and throughout the course of employment. The policy shall state the employer's commitment to providing a safe workplace and should set forth a code of conduct that prohibits all violence, threats, and behavior that reasonably could be interpreted as an intent to cause harm, either on-site or off-site during work-related activities. The policy should:

- Clearly define unacceptable behavior prohibited by the policy, consistent with the definition provided in Section 4 above;
- Regulate or prohibit weapons on site, on organization-controlled property, and during work-related activities, to the extent permitted by applicable laws;
- Mandate prompt reporting of any behaviors or circumstances that raise a concern for safety from violence or any potential violations of the policy;
- Provide multiple avenues for reporting—including human resources, security personnel, anonymous reporting systems, and members of the organization's Threat Management Team;
- Assure employees that reports made under the policy will be treated with the highest degree of discretion, will promptly be investigated by the employer, and notifications made to appropriate parties;
- Include a commitment to nonretaliation toward employees who make a good faith report under the policy;

- Mandate employees to inform security or other designated personnel of any protective or restraining order that is being sought, has been applied for, or has been issued for their protection;
- Impose appropriate disciplinary action up to and including termination for violations of the WVPI policy, including false or misleading reporting; and
- Avoid the use of the term "Zero Tolerance" because the term diminishes reporting and decreases safety.

The WVPI policy should be bolstered and supported by additional policies that, together with the WVPI policy, set clear expectations for appropriate workplace behavior and facilitate incident management. These policies may include:

- Anti-harassment and discrimination;
- Substance abuse;
- Code of business conduct/ethics;
- Electronic communications/computer use; and
- Inspections policy that establishes the employer's right to access an employee's workplace computer, desk, locker, and other items and premises as may be necessary and appropriate during an investigation.

6.2.2 Multidisciplinary Threat Management Team

A WVPI program further should include a multidisciplinary team created and periodically trained to evaluate and respond to violent incidents or reports of concerning behavior made under the WVPI policy. Depending on preference, organizations commonly refer to these teams as a "Threat Management Team," "Threat Assessment Team," "Incident Management Team," or "Case Management Team." For clarity and consistency, this Standard will employ the term "Threat Management Team."

Creating and training a Threat Management Team helps to ensure that lines of authority and communication and a general incident management process are established before a threat or violent incident occurs, and that personnel will know how to respond to reports concerning workplace violence. Typically, a Threat Management Team will include human resources, security, and legal personnel; in addition, other personnel may be included (as described in Section 5).

An organization should select personnel for the Threat Management Team who possess the requisite experience, training, judgment, authority, and temperament to effectively and collaboratively carry out the difficult duties involved in incident management.

The designation of a Threat Management Team should be accompanied by the identification of qualified external resources that the team can call upon as needed to assist with incident management, where the organization lacks the expertise in-house.

6.2.2.1 The Team Environment and the Use of External Experts

Effective prevention and management of workplace violence requires a team approach. Ideally, an organization at the early stages of its program development will conduct an assessment of its internal resources to support violence prevention and management efforts.

Often, an organization will supplement its internal expertise with outside experts, particularly in the areas of threat assessment, law, and security. Organizations that engage the help of external experts will—in the program development stages—identify, evaluate, and select professionals with documented expertise and experience specific to workplace violence prevention and management. Those qualified professionals can lend significant help in both the planning and implementation stages of a prevention program, as well as during incident management.

6.2.3 Incident Management Protocols

A WVPI program should include a predetermined general protocol by which the Threat Management Team will assess, investigate, manage, and resolve reports made under the organization's WVPI policy. The protocols may address:

- The personnel who will receive reports made under the WVPI policy and to whom those reports will be escalated;
- The personnel who will conduct an initial data gathering;
- Circumstances in which reports will be escalated and handled exclusively by the Threat Management Team, as opposed to the organization's human resources or employee relations organization under non-workplace violence protocols;
- The initial actions that the Threat Management Team will consider taking upon receiving a report;
- Coordinating reports made under the WVPI policy with related policies or processes within the organization (such as complaints coming through an anonymous ethics or tip line);
- Circumstances in which additional investigatory steps will be taken, the investigatory steps that will be considered, and the specifically trained investigators who will conduct the investigation;
- The circumstances and thresholds under which the Threat Management Team will engage outside experts, including legal counsel and threat assessment experts, to assist with incident assessment and management;
- The circumstances in which the Threat Management Team will engage outside law enforcement;
- The intervention and mitigation strategies the Threat Management Team will generally consider in addressing and resolving an incident made under the WVPI policy;
- The steps the Threat Management Team will take to adequately document a report or incident and its resolution;
- Lessons learned by the Threat Management Team following an incident to identify appropriate actions taken and areas of potential improvement; and
- The steps the Threat Management Team will take to continuously monitor, evaluate and improve the effectiveness of its intervention and mitigation strategies.

The specifics of the incident management protocols will vary from organization to organization, and at times from incident to incident. Accordingly, organizations should refine their incident management process during training exercises and over time as they identify areas for improvement through day-to-day case management.

The outline of an Incident Management Process is discussed in Section 8.

6.2.4 Protocols to Address Emergencies and Incidents That Generate Heightened Concern

The WVPI program should also include protocols for addressing incidents and reports that generate an immediate emergency or a heightened concern for impending violence. These critical or emergency measures and protocols are addressed in Section 8.9 below.

6.2.5 Training

A WVPI program shall include initial and periodic training for the Threat Management Team, top management, supervisors/managers, employees, and persons working on behalf of the organization. While the content and level of training varies depending on an individual's role in the organization, all employee training should include the following foundational topics:

- The basic facts about workplace violence, including a general overview of the behavioral or psychological aspects of workplace violence;
- The specific terms of the organization's WVPI policy, related policies, and the rights, duties, and obligations under those policies, such as reporting responsibilities and venues;
- Identification of concerning behavior that should be reported; and
- Responding to reports of concerning behavior and related emergency situations.

In addition, the organization should conduct advanced or specialized training for specific audiences:

- Training for members of the Threat Management Team, human resources personnel, legal advisers, and security personnel should cover the broad range of workplace violence issues discussed in this Standard. Members of the Threat Management Team should receive the most detailed and comprehensive training regarding the behavioral or psychological aspects of workplace violence, violence risk screening, investigatory and intervention techniques, incident resolution, and multidisciplinary case management strategies. Commonly, this training will be conducted or assisted by outside specialists with proven expertise in WVPI.
- Training for all levels of management and supervisors should emphasize their duties and roles in identifying and reporting concerning behaviors, and aiding the Threat Management Team in the implementation of mitigation strategies.
- Employee training should include information on the organization's WVPI program, organization's commitment to providing a safe workplace, employee's obligation to adhere to the organization's program and related policies, and reporting procedures and response options. Training could also include after-incident care training, informing employees of workplace violence related stressors, mechanisms to manage

stressors, and available resources. The organization should maintain effective documentation of its training programs and its attendees to ensure that all employees have obtained the appropriate training.

The organization should consider integrating a variety of methods for training for the various audiences. Those methods should serve the basic goal of effectively communicating the organization's WVPI policy, the employees' rights and obligations under the policy, and other information (such as the behavioral aspects of workplace violence) needed to enable employees to effectively participate in violence prevention practices consistent with the employees' roles and responsibilities within the organization.

6.2.6 High-Risk Workplaces

In developing and implementing their workplace violence program, organizations in industries that face a high incidence of workplace violence should consider policies and training to address the particular risk and response of violence faced by their employees (e.g., healthcare, taxi service, and all-night enterprises).

6.2.7 Record Keeping

The WVPI program should include a system of organization-wide record keeping specific to threats or concerning behaviors, making sure that all reports made under the WVPI policy are recorded and tracked for the purpose of identifying, monitoring, and guiding ongoing response. A system of centralized record keeping becomes especially important in large organizations, where offenders can at times move to various positions within the organization. In some cases, this system may include a connection with reporting mechanisms available to the organization.

All information in such reports should be handled with the highest degree of confidentiality and shared on a strictly compartmentalized need-to-know basis for the purposes of incident management and follow-up monitoring by current and future management. This information, if contained in physical files, should be kept secured; likewise, strict security measures should be applied to all data stored electronically. In addition, an organization should consider document retention practices to ensure that records of reports made under its workplace violence policy are kept for a sufficient period of time to allow for appropriate ongoing monitoring and follow-up.

6.2.8 Additional Prevention and Intervention Strategies and Protocols

As part of its WVPI program implementation, an organization should broadly evaluate the benefit of adopting additional security, employment, or management practices that can advance the goal of violence prevention. These practices may include but are not limited to:

- Effective employment screening techniques, including rigorous interviewing and the use of background investigations, for both employees and contractors where appropriate to the position in question. Background investigations may include, as legal and appropriate, criminal and civil history, drug testing, credit check, and social media research;

- Physical security measures, such as access control and visitor management, intrusion detection and alarm monitoring, video and other surveillance systems (as permitted by law), and protective design and hardening of workspaces;
- Policies and practices that help establish a work culture that expects professionalism and respect among employees; between employees and managers; and between employees and customers, clients, vendors, and others who interact within the workplace. In particular, the organization should consider implementing management and disciplinary practices that enforce behavioral standards at all levels of the organization and that encourage early intervention with all behaviors of concern. These include efforts to curb harassment of all kinds, bullying, and other similar conduct;
- A conflict resolution or mediation process to assist an organization in addressing normal, work-related interpersonal tensions and conflicts that might arise among coworkers; and
- A broad program to inform employees involved in workplace violence cases about assistance available through the organization's employee assistance program and outside agencies.

7. Implementing the Program

An organization should carefully consider how it can successfully implement a collaborative violence prevention and intervention program that involves all stakeholders. The nature and sequence of steps an organization takes to design and implement a workplace violence program will depend on a variety of factors, including the size, characteristics, culture, and resources of the organization. Implementation can best be thought of as a series of steps taken over time that help ensure full commitment to and an understanding of violence prevention practices.
The implementation of a WVPI program typically will include the following steps, some of which can be taken simultaneously.

7.1 Designate a Group to Design and Implement the Program

The organization should designate a small group who will hold primary responsibility for developing and implementing the WVPI program. Typically, this group will include human resources and security personnel, legal counsel, and other key stakeholders. Often, some members of this planning and implementation group will be assigned to the organization's Threat Management Team.

Because a successful program requires a top-down commitment, this planning and implementation group may become engaged in efforts to educate executive or senior management regarding the need for a workplace violence program and solicit their commitment to the program. Ultimately, it is important to ensure that the planning and implementation group has the full support of executive or senior management for the time and resources that will be required to develop and implement the program.

7.2 Design the Program and Establish a Plan for Its Implementation

The organization's planning and implementation group should draft an outline of a prevention and intervention program that fits the organization's resources, needs, and culture. Further, the group should set realistic deadlines for the systematic development and implementation of the program.

In designing the workplace violence program, the group should consider:

- The requirements and recommendations contained in this *Standard*;
- Legal, regulatory, and contractual requirements; and
- Relevant information available from government agencies, professional and trade groups, and other sources.

In addition, the group can benefit from:

- Guidance received from similarly situated companies that have successfully implemented a workplace violence program (e.g., benchmarking);
- Advice from outside experts in the areas of security, human resources, law, and psychology who possess substantial expertise regarding topics addressed in this *Standard*; and
- Legal counsel regarding aspects of the program that warrant legal review.

7.3 Establish Elements Essential to Incident Management

The organization should establish key elements essential to incident management:

- Designate a Threat Management Team to be responsible for receiving, investigating, and resolving reports made under the WVPI policy (see section 6.2.2);
- Develop an incident management protocol (see section 6.2.3);
- Conduct comprehensive training for members of the Threat Management Team (see section 6.2.5); and
- Establish relationships with local first responders.

7.4 Develop and Disseminate the Workplace Violence Prevention and Intervention Policy

With the Threat Management Team and incident management protocol in place, the organization can implement its WVPI policy.

The organization should obtain approval of the WVPI policy from senior management and legal counsel. The policy should include the definition of workplace violence. In addition, it should consider various means to effectively disseminate the policy to employees and persons working on behalf of the organization:

- Through workplace postings, mailings, or e-mail communications announcing the policy;
- As part of employee orientation and training;
- During company, department, or work group meetings; and
- As part of the process used by the organization to contract for temporary workers and independent contractors.

7.5 Monitor, Evaluate, and Improve Prevention and Intervention Strategies and Protocols

Once the organization has fully implemented its WVPI program, it should periodically assess the effectiveness of the program and revise policies, procedures, training, strategies, and protocols, as necessary. In evaluating the workplace violence program, the organization should examine:

- The effectiveness of the Threat Management Team, its composition, training, and participation;
- Any failures, successes, or other challenges encountered in addressing or resolving individual reports or incidents made under the WVPI policy, which might identify changes needed in incident management protocols;
- The number and nature of reports along with metric data made under the WVPI policy to assist the organization in directing resources to areas of needed attention;
- Any evolving legal, regulatory, or contractual requirements that might demand a revision of the WVPI program or specific incident management practices;
- Any failures, successes, lessons learned, or challenges encountered in integrating WVPI strategies into the organization's overall training and organizational culture; and
- Any additional training or prevention practices that the organization is now able to undertake.

8. Threat Response and Incident Management

8.1 Warning Signs and Their Significance to Incident Management

Inappropriate behaviors and/or communications by a person of concern often precede a violent incident. In addition, some behaviors emerge as warning signs of potential violence, offering a key opportunity for the organization to prevent a progression to more serious misconduct and violence.

While certain behaviors raise flags and serve as a warning, no profile exists to identify likely perpetrators of workplace violence. No single act or behavior can predict whether someone will commit violence. Instead, the discipline of violence risk assessment involves examining a full range of factors and circumstances, including the individual's personal history, grievances, motives, justifications, intentions, and actions. Organizations faced with obvious problematic behavior should conduct an assessment (internal and/or external) to determine the risk of violence posed by a person and identify and implement strategies that could avert or mitigate that risk. Accordingly, all personnel should be trained to identify concerning behavior and warning signs that should prompt reporting and possible intervention under the organization's WVPI policy.

In particular, organizations should remain alert to:

- A history of threats or violent acts, including threats or violence occurring during employment and a criminal history suggestive of a propensity to use violence to project power and to control others, or as a response to stress or conflict;
- Threats, bullying, or other concerning behavior, aggressive outbursts or comments, or excessive displays of anger;

- Abuse or harassment by any means or medium;
- Harboring grudges, an inability to handle criticism, habitually making excuses, and blaming others;
- Chronic, unsubstantiated complaints about persecution or injustice; a victim mind-set;
- Obsessive intrusion upon others or persistent unwanted romantic pursuit;
- Erratic, impulsive, or bizarre behavior that has generated fear among coworkers;
- Expression of homicidal, suicidal, or self-harm intentions;
- A high degree of emotional distress;
- A disturbing or threatening fascination with weapons;
- A preoccupation with violent themes of revenge, and/or an unusual interest in publicized violent events, if communicated in a manner that creates discomfort for coworkers; and
- Any behavior or collection of behaviors that instills fear and/or generates a concern that a person might act out violently.

Problematic behavior may emerge as particularly concerning if it is newly acquired or is accompanied by sudden personal or behavioral changes, such as decreased productivity, increased absenteeism, or an abrupt withdrawal from normal social circles at work. The context in which problematic behavior occurs likewise can heighten a concern for violence. Namely, the potential for violence may increase when the person in question suffers from an emotional, financial, or other significant stressor, such as the possible or actual loss of employment, financial hardship, divorce, a death in the family, legal challenges, and substance abuse.

The organization should remain mindful that a person can exhibit one or more warning signs and never resort to violence. However, the existence of concerning behavior and warning signs creates a need for prompt and thorough examination (and at times intervention) to help prevent escalation.

8.1.1 Identifying Potential Violence Stemming from An Abusive Relationship

Unlike with most other types of violence, victims of intimate partner violence commonly will try to conceal their abuse, presenting special challenges to an organization that endeavors to prevent workplace violence. Organizations do not have an unlimited right to pry into an employee's private life, but they do carry an overriding responsibility to respond to signs of intimate partner violence when that violence threatens workplace safety. For that reason, an organization shall remain aware of signals that an employee is involved in a violent relationship.

Warning signs of intimate partner violence, which can occur singly or in combination, include but are not limited to:

- Injuries (especially repeated injuries) such as bruises, black eyes, and broken bones—especially if the employee tries to conceal the injuries or offers unconvincing explanations for how they occurred;
- Absenteeism or lateness, poor concentration, and work-related errors or inconsistent work quality that is uncharacteristic of the employee;
- Requests for time off to attend court appearances;

- Signs of emotional distress, such as unusual quietness and increased isolation from coworkers, and unusual or repeated emotional upset during and following a phone call or contact with the employee's partner;
- Suggestions or statements by the employee that a former or current partner is engaging in unwanted contact;
- An unusual number of phone calls or emails, text messages, voicemails, or faxes from a current or former partner, and reluctance by the employee to converse with the partner or to respond to messages;
- Abrupt changes of address by the employee or a reluctance to divulge where the employee resides; and
- Unwelcome visits by the employee's partner to the workplace, particularly if the visit elicits a strong negative reaction by the employee.

8.2 Reporting of Concerning Behavior

History is replete with instances in which ample concerning behavior—including clear warning signs—had preceded an incident, but information about that conduct was never channeled to persons with the expertise, ability, or authority to intervene. As an essential prevention and intervention tool, an organization should adopt practices designed to maximize the reporting of conduct or circumstances that raise a concern for possible violence, so that the organization can take appropriate action. These practices can include:

- Implementing a WVPI policy and other complementary policies (such as an anti-harassment policy) that require and encourage employees to report concerning behavior and assist in the investigation process without fear of retaliation (see Section 6.2.1);
- Establishing a variety of methods for reporting concerning behavior, such as to members of the Threat Management Team, supervisors in the subject employee's chain of command, and other designated personnel, such as human resources and security. In addition, designated personnel should receive training regarding how to handle a report they receive and required escalation protocols;
- Training employees to recognize concerning behavior and to report the behavior to members of the Threat Management Team and other designated personnel;
- Establishing means by which employees can anonymously report concerning behavior, such as through a hotline, a tip-line, or other electronic means. Careful consideration should be given to how anonymous reports will be received to ensure that adequate information is reported to enable a meaningful response by the organization;
- Fostering a work culture and environment that supports the good faith reporting of concerning behavior; and
- Review of internal incident reports by qualified personnel to identify potential indicators of threat or future violence.

In contemplating the above strategies, the organization should remain mindful that it seeks information that is accurate, complete, timely, and reported in good faith. The more quickly and accurately a threat or concern with possible violence is reported, the greater the opportunity for successful intervention. The best opportunity for prevention is early intervention.

8.3 Overview of the Incident Management Process

Although circumstances, fact patterns, and other factors will drive the specific actions an organization takes in response to a report made under its WVPI policy, the organization should establish an incident management process.

When a reported situation involves an immediate threat to physical safety, local law enforcement and emergency response personnel should be notified, and the organization's emergency response implemented (see Section 8.9).

Upon receiving a report that is determined not to be an immediate threat made under the organization's WVPI policy, the Threat Management Team should gather readily available information and conduct a preliminary threat assessment to analyze the threat posed by the behavior or circumstances in question.

8.3.1 Objectives of the Threat Assessment

A threat assessment conducted by the Threat Management Team determines the general urgency of a situation and appropriate initial actions to take. The team will engage in fact gathering to determine, to the extent possible with readily available information, the "who, what, where, when, and why" of a report.

The team should focus on the persons of concern and the most readily available information, which should be gathered discreetly. Potential sources of initial information can include:

- Individuals who have reported the problematic conduct in question or who have emerged as the target of the behavior;
- Current and former supervisors or managers of the employee;
- Relevant human resources representative;
- Personnel files;
- Computers and communications devices and their applications (e.g., email, intranet history, and messenger, etc.);
- Network files;
- Background check, including court and other public records (where applicable and appropriate);
- Publicly available information (e.g., the internet, websites, blogs, social media, chat rooms, and other postings; and
- Video surveillance and access control records.

8.3.2 Information Relevant to the Threat Assessment

An organization conducting a threat assessment should obtain as much information as possible relevant to the situation reported.

Questions pertinent to the threat assessment fall into two general categories:

- Information regarding factors that establish a risk of violence; and

- Information regarding factors that lower or mitigate the risk of violence.

Key questions aimed at identifying a risk of violence include:

- What is motivating the individual to make the statements or take the actions that led to concerns about the safety of the workplace and its employees?
- What has the individual communicated concerning his or her intentions, whether by words or other disclosures or actions?
- What interest has the individual shown in violence or its justification, violent perpetrators, weapons, or extremist groups?
- Has the individual engaged in planning and preparation for violence, such as approaching a target or site; breaching security; or monitoring, harassing, or stalking a target?
- Does the individual have a known or suspected current or past history of a mental disorder or substance abuse? Has the individual exhibited symptoms of paranoia, delusional ideas, hallucinations, extreme agitation, despondency, or suicidal tendencies (especially with any violent content)? Has the individual ever acted on such beliefs?
- What evidence exists of serious oppositional or counterproductive attitudes or behavior in the workplace? For example, does the individual blame others or exhibit a strong sense of entitlement, defensiveness, self-centeredness, or intolerance of others' rights?
- How does the individual manifest anger and how focused is this anger on other individuals in the workplace?
  Has the individual experienced (or likely to experience in the near future) any serious personal or financial stressors, such as divorce, custody disputes, job or status losses, or deaths in the family? Does the individual show poor coping skills in reaction to such events?
- What is the individual's known history of serious interpersonal conflict, violence, or other criminal conduct (in domestic or other settings)?
- Is there evidence of any organizational, supervisor, or work group problems that have contributed to, provoked, or exacerbated the situation, and how do those problems influence the individual's perception of his or her circumstances?

Key questions aimed at disclosing factors that may lower or mitigate the risk of violence include the following:

- Does the individual have valued family or other positive personal attachments (i.e., critical emotional anchors)?
- Has the individual expressed genuine remorse for making threats or engaging in the behavior that has generated a concern for safety?
- Has the individual responded positively to defusing or limit-setting efforts by others?
- Has the individual engaged in appropriate problem solving or sought professional treatment or legal recourse as a way to manage the situation or problems at issue?
- What services have been offered to the individual and which have been accessed?

Of course, answers to many of these questions may not initially be available and in a given case may be particularly difficult to ascertain. The Threat Management Team should exercise caution

and good judgment and seek legal counsel (as necessary) in order to pursue information in a manner that does not complicate the incident management process, properly balances the need for thoroughness with the need for promptness, and complies with applicable laws. The Threat Management Team should further exercise care in conducting data gathering in a way that does not unwittingly increase the risk of violence.

8.3.3 Evaluating Information from the Threat Assessment

The team should consider all information it has gathered consistent with Sections 8.3.1 and 8.3.2 to assess:

- If the concern for violence is unwarranted, so that the incident can be handled (when involving an employee offender) within normal human resources, disciplinary, or employee relations protocols, as opposed to by the Threat Management Team?
- If the concern for violence is warranted but not imminent or urgent, should the organization consider other early incident management steps (see Section 8.4)?
- If the concern for violence is imminent, is emergency or urgent action needed? Does the concern require engagement of security or law enforcement?

8.4 Actions by the Threat Management Team

When the threat assessment indicates that a concern for violence is unwarranted, the Threat Management Team (when the incident involves an employee offender) may direct the incident to be handled by human resources or other management within normal human resources, disciplinary, or employee relations protocols, consistent with the WVPI policy.

When the threat assessment indicates a concern for violence that is not urgent, the Threat Management Team may proceed with early incident management steps, including, but not limited to:

- Continuing or expanding its information collection efforts;
- Consulting with external threat assessment professional(s) to obtain a more comprehensive assessment of the risk for violence, and steps that can be taken to mitigate the risk. Immediate or early consultation with a qualified external professional is particularly advised when the team feels uncertain in its ability to accurately evaluate risk, even in a general manner;
- Consulting with other resources, such as executive protection specialists and legal counsel;
- Assessing the need for additional security;
- Initiating, where necessary, coordination with local law enforcement; and
- Conducting ongoing monitoring, as appropriate.

When the concern for violence is imminent such that emergency or urgent action is needed, contact law enforcement and security immediately.

8.5 Threat Response Actions by the Threat Management Team

As the Threat Management Team continues its work, it should implement and coordinate measures to monitor the potential for violence, to manage and mitigate that risk, and to successfully resolve an incident.

8.5.1 Actions Directly Involving the Person of Concern

The Threat Management Team should consider the following actions directly involving the person who has generated the concern for workplace violence, whether an employee or other insider threat or a third party or other external threat, including but not limited to:

- Conducting a deeper investigation, potentially including searches of workplace computers or networks, public records, databases, social media, and other sources (including, most importantly, interviews with coworkers) legitimately available to the organization, for information pertinent to expressed hostilities, violent ideation, and a history of harassment, aggression, or violence;
- Engaging a qualified internal and/or external threat assessment professional to conduct a violence assessment and to counsel the organization on steps it can take to address and mitigate the behavior of concern, including (if needed) specific defusing and treatment interventions;
- When the person of concern is an employee, considering appropriate and safely conducted employment actions, including discipline, suspension, or termination. Appropriate actions may further include a referral to employee assistance program, transfer, administrative leave, and other possible actions;
- When the person of concern who exhibits behavior that might be associated with behavioral/mental health issues, consult legal counsel to determine the employer's applicable legal and regulatory obligations;
- When the person of concern is a company contractor or related third-party, the organization should consult legal counsel and the person's employer;
- When the person of concern's information and activities are less accessible, the organization may consider additional investigation efforts; and
- Considering necessary or appropriate law enforcement or legal action.

8.5.1.1 Managing an Employee with an Intimate Partner Violence Issue

When a threat assessment reveals that an employee's partner poses or may pose a danger to the employee and/or the organization, the organization should consider specific safety and security measures. Some of these measures may require the participation of the abused employee and others in the workplace. These security measures may include:

- Taking steps to limit the abuser's (or suspected abuser's) access to the workplace, such as distributing the abuser's photograph to security personnel and, if appropriate, members of relevant management or a specific work group;
- Encouraging and/or requiring the abused employee to inform members of the Threat Management Team or other designated personnel about behaviors of significance in line with those listed in Section 10, such as any new threats or contacts received from the abusive partner;

- Providing a parking space for the employee close to building entrances, providing a security escort to the employee's car, offering flexible or variable work hours, removing the employee's name from office telephone directories, changing the employee's workplace email address, changing the employee's office or work location, and screening phone calls;
- Requiring the employee to inform members of the Threat Management Team or other designated personnel if the employee obtains or receives a restraining or protective order, or other judicial order, as a result of a criminal or civil proceeding. When a restraining order names the workplace, security personnel should be informed of orders restricting the abused partner's presence on the work site;
- Where permitted, employers obtain restraining orders covering the workplace. The organization should evaluate the feasibility and desirability of obtaining such an order when it learns of threats from an employee's abusive partner affecting the workplace; and
- Referring the abused employee to outside resources, such as community organizations focused on intimate partner violence, to obtain assistance in creating a personal safety plan.

8.5.1.2 Managing an Employee with a Known or Suspected Behavioral/Mental Disorder

On occasion, an employer will possess information that, as a legal and practical matter, places it "on notice" that an employee of concern suffers or exhibits symptoms of a behavioral/mental disorder. At times, the employee has engaged in behavior so bizarre, inappropriate, and inexplicable that the employer may reasonably conclude that a problem exists. Sometimes, an employee may even self-disclose a mental disorder. In all cases, the organization should consult with legal counsel to determine employer obligations under related governmental regulations, which may offer employment protections to employees who suffer from certain defined disabilities.

As a rule, the existence of a behavioral/mental disorder does not excuse breaches of company policy or offer immunity when an employee engages in threats, violence, and other inappropriate workplace behavior. Often laws and governmental regulations do not offer protections to employees with a declared behavioral/mental disorder when they present a threat of violence to the organization. However, the existence of a known or suspected behavioral/mental disorder typically will affect incident management, causing the employer to consider actions, such as:

- Securing the advice of a qualified threat assessment professional in the early stages of incident management;
- Encouraging the employee to seek medical attention, including the placement of the employee on medical leave;
- Securing the help of family members or close friends in encouraging or enabling the employee to seek medical help if not in breach of the employee's right to privacy;
- Engaging law enforcement and/or mental health professionals to facilitate admission to a medical/psychiatric facility for evaluation, consistent with applicable laws; and
- Having the employee undergo a fitness for duty examination, when required by the organization's policy.

8.5.1.3 Ensuring a Safe Separation of Employment or Business Relationship

When an organization chooses to separate an employment or business relationship with an individual of concern, it should engage key stakeholders in designing and implementing strategies to ensure a thoughtful, respectful, and safe separation from employment. The organizations should recognize that terminating employment or a business relationship may not eliminate the potential risk of harm to the organization. Strategies may include:

- Obtaining the advice of a qualified threat assessment professional in designing a separation plan, including how the interaction should be conducted;
- Offering an outcome for the individual of concern (which may include a separation package) that is intended to promote safety and that is fair and respectful to those involved;
- Conducting the separation consistent with the organization's established practices, policies, and procedures addressing the concern for violence, and obtaining legal advice as necessary to ensure compliance with applicable laws;
- Implementing short- and long-term security measures, when appropriate;
- Considering the nature and form of information that will be provided in the future in response to queries about the former party by other entities; and
- Monitoring for behaviors that may have an impact on the safety of the organization and its employees.

8.5.2 Actions Involving the Potential Victim or Target

Within the context of a comprehensive multidisciplinary evaluation and understanding of an incident, the Threat Management Team should also consider actions involving the victim or target of the threatening behavior, including but not limited to:

- Offering to answer questions the employee may have regarding personal safety and security considerations;
- Referring the employee to professionals who can provide emotional counseling and safety and security training, such as employee assistance program and community-based resources like public safety agencies, advocacy groups, shelters, or other private services;
- Identifying local domestic/intimate partner violence organizations that serve appropriate cultural or religious groups the employee may belong to;
- Discussing with the employee nonpunitive employment actions, such as a relocation or transfer within the organization, administrative leave, or other reasonable accommodation;
- Instructing the employee about steps he or she should take to inform the Threat Management Team of any future contacts by the person of concern and how to respond to communications or contacts made by that person;
- Keeping the employee appropriately informed of actions the Threat Management Team is taking to address the incident or behavior in question. Of course, the employee should not be provided detailed information, but enough information to elicit confidence that the employer is responding appropriately; and
- Contacting a parent or guardian (as appropriate) if the victim is a minor.

8.5.2.1 Maintaining Proper Limits to Organizational Involvement

An organization will involve itself in managing threats to the workplace stemming from a variety of sources, including intimate partner violence. However, the organization is discouraged from undertaking a "counseling" role with suspected or identified victims of any of these types of violence. The Threat Management Team, while maintaining a compassionate stance, should limit its involvement to steps necessary to safeguard workplace safety and productivity. The Threat Management Team should encourage employees who need broader support and assistance (whether emotional, financial, or legal) to contact appropriate outside resources, such as an employee assistance program, local domestic violence victim advocates and service providers, law enforcement agencies, district attorneys' offices, and judicial victim services providers.

As part of its workplace violence program, an organization should maintain a list of these resources, which it can provide to its employees when necessary.

8.5.3 Additional Actions

The Threat Management Team may consider additional actions, including but not limited to:

- Reporting criminal activity to law enforcement. This may also include consulting with law enforcement agencies or otherwise engaging law enforcement resources and assistance in addressing an incident and cooperating with any ensuing criminal investigation;
- Adopting security measures covering the workplace generally or the specific targets. These measures can include steps to alter access to workspaces, networks, and equipment;
- Developing strategies and communications to address fear and disruption affecting employees and work groups;
- Coaching relevant managers and supervisors (when the organization permits the person of concern to continue in his or her employment or relationship with the organization following an incident) to:
    - Enforce standards of appropriate workplace behavior;
    - Closely monitor the workplace conduct of the individual of concern; and
    - Immediately report any future concerns to the Threat Management Team.
- Revising WVPI policies and procedures as needed.

8.6 Engaging an External Threat Assessment Professional

Many organizations' Threat Management Teams, through training and accumulated experience, will be adept at assessing potential risk and at developing risk mitigation strategies. However, when the Threat Management Team lacks the proper knowledge, training, or experience to fully assess a situation; or when the Threat Management Team seeks a third-party perspective, the organization may consult with an external threat assessment professional.

Outsourcing a violence risk assessment to a qualified threat assessment professional can enhance the quality of incident management; in addition, it can help to mitigate the organization's liability by ensuring that the organization has allowed a qualified person to assess violence risk.

In selecting an external threat assessment professional, the organization should consider factors such as the person's training, education, and experience in conducting violence assessments (especially in the workplace context), and knowledge of applicable laws and regulations pertaining to workplace violence.

8.7 The Importance of Legal Oversight

As referenced elsewhere in this Standard, workplace violence prevention and intervention is a multidisciplinary endeavor. Legal counsel, whether in house or from an outside law firm, with expertise in employment law and relevant experience in managing workplace violence incidents, should be consulted for guidance during the incident management process. This guidance may include:

- Compliance with the organization's established policies and procedures, privacy, legal obligations regarding disabilities and other applicable anti-discrimination laws, due process requirements, obligations under data protection and privacy laws, and additional laws and regulations, including evidence preservation, and requirements under any applicable collective bargaining agreement;
- Effective and legal investigatory or fact-finding processes;
- Process for engaging in the threat and/or violence assessment of an employee, including guiding the organization;
- Appropriate employee disciplinary or other remedial steps, including termination;
- The composition and conditions of a separation package and related releases;
- The nature and form of information that will be provided in the future in response to queries about the terminated employee by prospective employers;
- Potential legal risks and liabilities raised by courses of action the organization might have under consideration;
- In appropriate circumstances, legal counsel may also lead efforts to obtain corporate restraining orders, criminal trespass warnings, or engage in other legal processes;
- Notification and involvement of law enforcement; and
- Obligations to warn potential targets of possible violence, and to provide security protection.

8.8 After an Incident Has Been Resolved

After the Threat Management Team has concluded the investigation of an incident or report (by implementing remedial steps and resolving safety and security concerns), it typically will engage in the following additional actions:

- The team should ensure appropriate recordkeeping of the incident, including all actions taken by the team;
- When the organization permits the person of concern to continue in his or her employment or relationship with the organization following an incident, it should instruct relevant managers and supervisors to:
    - Enforce standards of appropriate workplace behavior;
    - Closely monitor the workplace conduct of the individual in question; and

    - Immediately report any future concerns to the Threat Management Team. Relevant management should remain alert to any new information indicating a need for additional action, either with respect to the specific situation at issue or the workplace in general.
- The team should undertake a careful review of the incident in question, examining both the precipitating event and the organization's and the team's response to it. The purpose of the review is to determine any needed or desired changes in workplace conditions, policies, procedures, or training that could help avoid similar incidents in the future or help the organization to manage them more effectively if they occur.

8.9 Responding to an Act of Violence

Despite the best prevention and deterrence efforts, workplace violence can still occur, resulting in injuries and death. For that reason, an organization's threat management protocols should consider the organization's response to acts of violence.

8.9.1 General Considerations in Pre-Planning

Pre-planning, training, and simulation exercises are critical to helping an organization establish an effective response to a violent incident. Response plans should consider:

- The core types of incidents that the organization can face, including aggressive posturing without physical contact; injurious aggression, such as slapping, pushing, shoving, punching, kicking, and wrestling; the use of various weapons, conventional or improvised, and of incendiaries or explosives; and active assailant scenarios;
- The possibility of single or multiple offenders;
- Expectations regarding employee involvement in responding to violence;
- Policies that establish how the organization intends to mitigate or stabilize an immediate threat to personnel who are in direct contact with an active assailant to prevent casualties;
- Pre-planning involving first and emergency responders, such as ensuring that they have access to floor plans, access to the site, and can set up command posts as appropriate;
- Training to all employees, contractor employees, and regular site visitors regarding how to maintain physical safety during an incident; and
- Other strategies and policies (see Sections 8.9.2).

8.9.2 Immediate Response Critical Considerations

Studies show that once violence begins, actions with the greatest impact on the outcome will be taken by persons already at the scene. For that reason, the organization's trained emergency responders should be considered part of the violence response plan.

In a potentially life-threatening situation, immediate response procedures for individuals present on site should address the following:

- Avoid the danger zone by moving to a safer location in the facility or away from the facility itself, as indicated by the situation;

- Alert others of the incident;
- Notify first responders and local security/safety resources, as soon as possible;
- Provide first responders with necessary building floor plans and access. Use available technology (e.g., video surveillance systems) to monitor unresolved situations and communicate real-time updates to affected personnel and first responders to help them make appropriate decisions;
- Deny an attacker access to additional victims by notifying those within the potential danger zone to either escape or seek shelter in place. Whenever possible, take action to prevent an attacker's movement into other areas, or effectively barricade portals to areas where personnel have taken temporary refuge;
- Defend against the attacker to stop the attack if escape is not possible, or if victims who cannot protect themselves are in immediate danger and intervention can be accomplished without unreasonable risk to the defender's own safety;
- Provide first aid to injured persons when and where this can be done without placing either victims or rescuers in further danger;
- Close off access to any areas affected by the incident as soon as possible to prevent contamination of evidence;
- Comply with the instructions of first responders during their response to an incident, and avoid any action that could be viewed as disruptive; and
- Account for all personnel and determine their status and location in order to identify those who are missing and may still need help and to be able to respond accurately to concerned parties.

The organization should identify appropriate personnel to receive specialized training on each of the specific considerations according to their roles and assignments. For additional information on the topics relevant to business continuity and preparedness, see Section 11.

9. The Role of Law Enforcement

While not every workplace incident will reach the level of criminal conduct, cases that involve physical assault, significant destruction of property, or serious threats (especially with a weapon) generally require intervention by law enforcement and possibly other public safety agencies as well.

Law enforcement's role as an emergency responder is widely recognized. If a situation arises in a workplace that puts life, personal safety, or property in immediate danger, any business owner or manager will know that an emergency response call will quickly bring law enforcement and possibly other emergency personnel to the scene. Once there, law enforcement officers have the responsibility for controlling the situation and ending the threat and, in many cases, for arresting the offender and gathering evidence for criminal prosecution.

However, emergency response is not the law enforcement community's only role in workplace violence. Employers should be aware that establishing contact and exchanging information with local law enforcement before a violent act occurs is vital in developing and administering an organization's workplace violence program. An existing relationship and communication channel

between an organization and local law enforcement may also make the response more effective if an emergency arises.

Law enforcement agencies in different jurisdictions have different laws, policies, budgets, manpower, and competencies, and may have different priorities and different attitudes on cooperating with employers in workplace violence prevention and response efforts. In developing workplace violence plans, employers should contact law enforcement for their geographic area and meet to discuss law enforcement response and investigation procedures to ensure an effective collaboration to respond to crimes in progress and other emergency calls.

Employers should find out how law enforcement would answer questions such as:

- What is your standard response to a report of a suspicious person on our property or in our building? How will you respond to a report of an unauthorized person on the property or in the building with a firearm?
- Do you have a policy of investigating threats before any injury occurs? What is your position on responding to conduct that creates fear, such as threatening, bullying, and intimidation, but that may not be characterized as criminal?
- What is the procedure following a report of a duress alarm or crime in progress at our facility?
- How long do you estimate it will take to reach the scene after an emergency call?
- Do you have a dedicated domestic violence officer or unit that provides preventive services to victims?

In establishing a channel of communication with a law enforcement agency, it is preferable for an organization to designate one person and an alternate as its permanent liaison officer with the agency. It is even better if the agency also provides a single point of contact to the organization.

Once the communication channel has been established, the organization's representative can use it to:

- Make sure the appropriate law enforcement entities have correct information about the organization in their record systems (often a computerized database). Data such as address, telephone number(s), and the physical layout of the site—including main power and water locations—should be on file, along with 24-hour contact information for the appropriate contact person(s);
- Ask what additional information might be put on file to help law enforcement respond more effectively in an emergency (for example, fire and evacuation plans to include where employees will meet after an evacuation, or locations of hazardous materials or high-value goods). Consider providing local law enforcement detailed and current floor plans of the facilities and key cards to access secured areas. These will facilitate local emergency services responses, especially in cases of barricaded suspects or hostage situations;
- Find out if the department offers any crime prevention outreach programs that could be useful to company executives or employees;
- Ascertain the law enforcement agency’s policy on responding to noncriminal yet threatening behavior and determine what information the organization will share with law enforcement in such incidents;

- Get advice on planning and possible assistance or support from law enforcement when a situation or event may create a heightened risk of violence. Possible examples include announcements of layoffs, an adversarial termination, or knowledge that an employee is in an abusive personal relationship; and
- Build a relationship with local law enforcement in order to better prepare for the possibility of a serious violent event in the workplace. In addition, the organization may wish to consider partnering with law enforcement for on-site training, drills, and exercises. Joint exercises familiarize law enforcement and other first responders with the premises, reveal areas of friction in response procedures, and deepen the relationship between the organization and the agencies involved.

While it is imperative for an organization to reach out to its law enforcement partners to determine exactly what they will or will not do in a given situation, it is just as important for law enforcement to understand how the organization will respond to a given situation. This mutual exchange of information permits a seamless plan for intervention and assistance. A partnership based upon the knowledge of each other's capabilities and enhanced communication will strengthen an organization's overall violence prevention efforts.

9.1 Law Enforcement Intervention

While actual criminal violations should be reported to the appropriate law enforcement agency, the Threat Management Team should carefully consider the potential risks and benefits of requesting law enforcement intervention in a situation that may not rise to the level of a criminal act. The Threat Management Team, in advance of any particular incident, would benefit from developing an understanding regarding the willingness and ability of its local law enforcement agency to appropriately intervene during incident management, and the nature and limits of its prospective role during incident management. Of course, as emphasized throughout this Standard, the question of law enforcement intervention should be considered within the context of a Threat Management Team's overall incident management strategies.

10. Integrating the Issue of Intimate Partner Violence into Workplace Violence Prevention and Intervention Strategies

While traditionally seen solely as a private problem, intimate partner violence can significantly impact workplace safety and productivity. When an employee is in an abusive relationship, it is not uncommon for the abuser to seek out the abused employee at work, where he or she can readily be found. When these threats from private or intimate violence intrude on the workplace, they endanger not only the abused partner but coworkers as well. In addition, the abuser will at times use his or her own resources at work (such as work time, computers, telephones) to harass or threaten the abused partner.

Due to its significant potential impact on workplace safety, an organization's WVPI program and its overall prevention and intervention strategies should address intimate partner violence. When incorporating intimate partner violence issues into a WVPI program, an employer should consider the following strategies.

10.1 Include Intimate Partner Violence in the Policy Statement

An employer's WVPI policy should recognize intimate partner violence as a workplace violence symptom and should address it in several ways:

- The policy should require or strongly encourage employees to report to designated personnel any restraining or protective orders sought or obtained covering the workplace. The policy should encourage employees to report safety concerns related to intimate partner violence without fear of retaliation or negative job consequences;
- The policy should reflect a commitment to support victims of intimate partner violence by providing referrals to appropriate community or employee assistance program resources and providing time off for reasons related to intimate partner violence as required by law or company policy;
- The policy should address abusive partners by making it a violation to stalk, threaten, or harass anyone (in the same workplace or elsewhere) while on the job or with the use of the organization's resources, including computers, telephones, fax machines, or vehicles; and
- The policy should communicate that the organization treats threats coming from an abusive personal relationship as it does all other forms of violence.

10.2 Implement Prevention Strategies Specific to Intimate Partner Violence

An organization should incorporate prevention strategies specific to intimate partner violence.

These can include:

- Specialized training (in addition to that outlined in Sections 6.2.5 and 7.5) to address:
    - Warning signs that an employee may be involved in a violent relationship;
    - Circumstances in which behavior seemingly tied to an abusive relationship should be reported to the Threat Management Team;
    - How members of the Threat Management Team, supervisors, and other relevant personnel can approach an employee in an appropriate, effective, and compassionate manner to ask about a suspected abusive relationship; and
    - Community, employee assistance program, and other outside resources that the organization can refer employees to for assistance in addressing intimate partner violence.
- As with other workplace violence training, members of the Threat Management Team should receive detailed training regarding intimate partner violence, methods of responding to reports of workplace threats stemming from an abusive relationship, and special privacy issues that arise during incident management. To maximize the chances that employees will report threats stemming from an abusive relationship, the organization should create a supportive environment and encourage or require employees to inform designated personnel of safety concerns stemming from intimate partner violence without fear of retaliation or negative job consequences; and
- As part of efforts to create a supportive environment, the organization should provide information to employees (during training or otherwise) regarding community

resources available to them in addressing an abusive relationship, including legal, psychological, and financial resources.

10.3 Legal Issues Specific to Intimate Partner Violence

In addition to the legal issues that arise during incident management as a general matter, organizations faced with workplace safety issues tied to intimate partner violence should consider additional specific legal requirements during incident management. An organization managing safety questions tied to an abusive relationship should seek legal counsel to ensure compliance with applicable laws and regulations, which may include the following:

- Providing paid or unpaid leave in a variety of circumstances, including for an employee's serious health condition or a family member's serious medical condition. Those provisions may apply when an employee seeks time off to attend to his or her own or a family member's injuries stemming from an abusive relationship;
- Prohibiting an employer from discriminating against employees involved in an abusive relationship by terminating them or imposing other negative job consequences Some jurisdictions specifically require employers to grant abused employees time off for reasons related to intimate partner violence, such as receiving medical attention, attending court proceedings, or receiving counseling;
- Providing reasonable accommodations to employees involved in an abusive relationship; and
- Mandating or recommending that employers provide employee training regarding intimate partner violence.

10.4 When Employees Are Abusers

Organizations that are committed to mitigating threats to the workplace shall address the issue of employees who perpetrate or threaten violence against their partners, whether at the same workplace or elsewhere.

As part of its WVPI program:

- The organization should make clear in its WVPI policy that it prohibits employees from using workplace time and resources to harass, threaten, or harm a partner, whether or not the partner is an employee;
- An organization that learns of possible policy violations by an abusive partner (or suspected abusive partner) should follow its incident management protocols to investigate the reported misconduct (while also determining if the employee has engaged in any concerning behaviors directed towards other organizational members), and impose appropriate disciplinary and other remedial measures; and
- Upon confirming misconduct by an abusive employee, the organization may refer the employee, if appropriate and as part of (but not a substitute for) broader disciplinary and remedial measures, to an employee assistance program to secure counseling through an accredited and standardized batterers' intervention program.

In cases where concerning conduct is reported that took place outside the organization, appropriate steps should be taken (consistent with legal considerations) to alert management and

conduct an appropriate assessment concerning whether conduct exists that could affect the safety of the worksite.

10.5 Documentation Specific to Intimate Partner Violence

In circumstances involving intimate partner violence, the organization shall maintain thorough documentation as it would with any incident, as discussed in Section 6.2.7. Documentation should include all information gathered during incident management and during ongoing monitoring, as well as all restraining, protective, or judicial orders relevant to the specific incident or report.

11. Post-Incident Management

While this *Standard* focuses on prevention and intervention, an organization should also consider a business continuity plan for incidents of workplace violence, particularly significant incidents resulting in injury and death. For the purposes of this section, it is assumed that:

- The immediate incident is stabilized;
- Some form of resolution has been achieved;
- A determination has been made to resume operations; and
- potential for renewed escalation or a new threat exists.

In addition, an organization should consider the strategies in developing a continuity plan (immediate, short-term, and long-term) specific to workplace violence incidents detailed in the following subsections.

11.1 General Elements of a Post-Incident Recovery Plan

The following elements should be considered when establishing a post-incident recovery plan for acts of workplace violence:

- Protocols for priority responses. Immediate priorities will include:
    - Life safety, with consideration given to the immediate needs of those directly impacted by the violent event (e.g., medical attention to injured personnel; addressing the needs and concerns of impacted stakeholders);
    - Evidence preservation for impending investigation; and
    - Asset preservation, with a view towards protecting any threatened core assets.
- Crisis containment. Crisis containment may include efforts to:
    - Gather facts regarding the incident as quickly and completely as possible;
    - Securing and containing affected physical areas to preserve information and the integrity of an ensuing investigation;
    - Separating witnesses; and
    - Anticipating and addressing other steps needed to preserve safety.
- Continued assessment of threats. Following a violent incident, the organization should address the likelihood of a continuing threat, including any reignition of conflict; the possibility of a copycat incident; or a preplanned multiple attack.

Personnel should evaluate whether security or other gaps enabled the initial violent act and determine measures to promptly mitigate or eliminate those gaps.

- Coordination with the Threat Management Team. The organization's Threat Management Team and any existing crisis management team should:
    - Coordinate efforts to evaluate ongoing threats;
    - Protect core assets;
    - Fully resolve the violent incident; and
    - Achieve business resumption.
- Notifications. Typically, a violent incident will give rise to a need for multiple notifications, including to:
    - Managers. While on-site management will likely be aware of the violent incident, those in other locations may not. A preexisting plan should be implemented to notify relevant management of the violent incident as soon as reasonable;
    - Employees at large. Employees need accurate and timely information during the lifecycle of an event. Those responsible for internal communications must be made aware of the event and level of details that can be disseminated, so that they can assist recovery efforts;
    - Next of kin/intimate partner. In the event of serious injury, death, or other circumstances, management may have a responsibility to ensure proper notification (in consultation with law enforcement) of an employee's next of kin or partner;
    - Regulatory authorities. Notification to regulatory agencies should be made promptly. Agencies may include federal, state, and local agencies. A list of all required agency notifications, with phone numbers, should be maintained as part of the post-incident management process; and
    - News media. Notifications to the media (coordinated with the incident management team) will be necessary during the lifecycle of an event. Ongoing interaction with news media, as appropriate, will help ensure dissemination of accurate and timely information. Those responsible for external communications (e.g., public information officer) must be made aware of the event and the level of details that can be disseminated, particularly if and when names of victims can be released. In post-incident management, communications with the news media can help to inform interested and impacted stakeholders (e.g., victims, workers, customers, contractors, competitors). These statements will contribute to a sense of personal and public safety. Proper and honest communications with business partners and the public will assist in managing and recovering from the event.
    - Ongoing communications. Communication with all impacted stakeholders is the foundation for effective crisis management. Potential stakeholders may include customers, clients, employees, contractors, business partners, families, visitors, institutional investors, shareholders, insurance representatives, suppliers, distributors, unions, community members, politicians, and Internet users, depending on the organization.

- Mobilization of resources. The organization should mobilize needed resources to assist in post-incident recovery. Applicable principles are discussed in the ASIS Security and Resilience in Organizations and their Supply Chains standard. Additional resources could include extra security, risk management (insurance) services, and qualified and temporary work staff.
- Mental health response. Mental health services should be offered to those affected by the violent event.
- Law enforcement involvement. If there is actual or suspected criminal activity, law enforcement will conduct investigations and take appropriate actions to help restore a sense of safety and security. A liaison should be established to assure proper cooperation and communication between the company and law enforcement.
- Legal oversight. As a critical part of crisis management, the legal team will need to promptly evaluate and address potential legal claims and minimize exposure. Legal counsel will assist in providing direction and advice in many areas of post-incident operations. Advising on actions early in the post-incident period can greatly reduce downstream lawsuit and litigation activity.
- Family representative program. Consideration should be given to the establishment of a family representative program to address ongoing questions and concerns of the families of those affected. Trained family representatives should include a multidisciplinary representation of the company.
- Protection of core assets. The organization should address strategic issues related to the protection of core assets (e.g., reputation, brand, trust, operations, and property) following the violent incident.
- Business operations. It should be recognized that a traumatic incident can have a significant impact on a business's ability to resume operations. Pre-planning is essential. Advanced thought should be given to the orderly shutdown of operations; business sustainability, continuation, or cessation; recall of products; and employee management.

Annex A

(informative)

A.1 Introduction to Active Assailant

Active assailants are a global problem and all nations must work towards the identification, prevention, response, and recovery from these violent acts.

Mass casualty attacks involving active assailants are a persistent, ongoing, and active threat throughout the world. Reported incidents involving firearms in the United States can give the misleading impression that countries with increased civilian firearm ownership are the only ones facing the threat of active assailants. To the contrary, while statistics on workplace violence outside the United States are not comprehensive, one 2010 study of the European Union noted that one in 20 workers (5 percent) experienced an incident of physical violence in any one-year period. The prevalence of this level of violent behavior exists because active assailants are not limited to the use of firearms; they often resort to vehicles, edged weapons, blunt weapons, chemical or biological devices, improvised devices, and/or other instruments or means. Active assailants differ from terrorists in that they are usually not politically motivated. Often, an active assailant is linked to issues such as bullying, troubled interpersonal relationships, employment-related issues, and mental health-related issues. An active assailant also differs from gang-related violence and other criminal homicide offenses that are often based on crime-for-profit or in retribution to rivals or informants.

What is evident is that active assailants throughout the world are choosing target locations across the spectrum of organizational types, including educational institutions, healthcare settings, houses of worship, public agencies, military properties, or private business settings (to include sporting events, malls, and other settings with large gatherings of people). Although places involving commerce (i.e., corporations, other types of businesses, etc.) and schools seem to have the highest percentage of active assailants, there is no safe haven. While historical data is not a predictor of future violence, statistics indicate that the active assailant threat is growing and will continue to grow in the future. It would be remiss to ignore such facts and not make every effort to develop and implement pre-incident response planning, incident response, and post incident recovery for such acts of violence.

Annex A is meant to serve as a tool and resource that organizations of any size can use to evaluate, develop, and implement measures, resources, and protocols related to an active assailant incident. The information and recommendations provided in this Annex A are generic and can be developed as a stand-alone program and/or incorporated into an organization’s existing WVPI program.

Annex A reflects a multidisciplinary perspective from a variety of professions to include security, human resources, mental health, law enforcement, crisis communications/public relations, and legal regarding practices viewed as effective, recommended, and—in some cases—essential through work in this field.

Accordingly, effective prevention, identification, intervention, response and recovery efforts will draw on the knowledge, skills, and participation of many stakeholders—including outside sources such as first responders, counselors, threat assessment professionals, and all levels of governmental agency support.

A.2 Pre-Incident Planning

This annex was developed to guide and assist individuals who have the responsibility for developing and implementing an active assailant program. This program is no substitute for a comprehensive workplace violence prevention program; however, this should constitute an element of an organization's program. Included in this annex are recommendations and actions that should be taken during pre-incident planning, incident response, and post-incident recovery in an active assailant incident.
It is further recommended that organizations with existing response plans use Annex A to consider further enhancements to their plan and/or validate what is currently in place.

A.2.1 General Considerations

Active assailant response plans should be developed and implemented based on the organization's:

- Size;
- Scope;
- Complexity;
- Presence or absence of security personnel;
- Resources and operation of the location; and
- Site risk assessments and gap analysis.

Plans should be documented, reviewed annually, and updated accordingly. Plans should also comply with local, state, federal, international laws, legal and regulatory requirements.
NOTE: Distribution of the plan should be limited to authorized personnel.

A.2.2 Active Assailant Response Plan

In developing its active assailant (AA) response plan, the organization should:

- Identify internal and external key personnel (to include alternates) and resources needed to support and respond to an active assailant situation such as:
    - Chief security officer (CSO) or head of human resources;
    - Threat Management Team;
    - Security personnel;
    - Incident commander (IC) and IC structure;
    - Crisis communications/public relations officer and/or external consultant;
    - Global security operations center (GSOC)/dispatch center;
    - Safety liaison; and
    - Multitenant representatives (if applicable).
- Identify responsibilities and authorities of key personnel (see section A.2.3);
- Establish emergency management liaisons (see Section A.2.4);

- Create emergency response kits/bags (see Section A.2.5);
- Establish notification and communications strategies (see Section A.2.6);
- Follow guidelines for selecting staging and operations areas (see Section A.2.7);
- Test and validate the plan (see Section A.2.8);
- Train the response teams (see Section A.2.9);
- Provide employee awareness training (see Section A.2.10);
- Consider psychological aspects (see Section A.2.11); and
- Consider legal aspects (see Section A.2.12).

A.2.3 Identify Responsibilities and Authorities of Key Personnel

The organization should establish a formal planning team consisting of key personnel as identified in A.2.2 to develop, execute, maintain, and improve the organization's active assailant response plan. Each member of the planning team should understand his or her role, as well as other members' roles in the pre-planning, incident response, and post-incident recovery phases.

The following activities are key in each of the phases and should be assigned to appropriate members:

- Pre-incident planning:
    - Identify protection focused objectives and mitigation strategies consistent with corporate strategic and business continuity planning for preventing, mitigating, and responding to AA situations;
    - Conduct an annual risk assessment/gap analysis to identify any vulnerabilities, risks, and/or gaps. Institute changes or develop plans to mitigate any vulnerabilities, risks or and/or gaps;
    - Evaluate physical protection programs (e.g., access control and video surveillance systems) and security measures (e.g., emergency communications and workplace violence prevention programs) for the purpose of preventing, mitigating, and responding to incidents;
    - Collaborate with qualified external experts as appropriate for independent site security reviews and incident/scenario-based violence assessments;
    - Establish and maintaining relationships with local, state, and federal law enforcement and other related government agencies;
    - Work with key stakeholders to allocate resources (e.g., financial, personnel, equipment, training, etc.), and take a proactive approach (rather than reactive) —for example, to increase allocation of budgets for personnel and training time and add a safety matrix for employment evaluations—towards preparing for incidents of AA;
    - Identify the organization's on-site leader and establish protocols for transfer of command to first responders as appropriate;
    - Identify primary and alternate locations for emergency operations center (EOC), incident command center, media area, and equipment considerations for coordinating incident management response activities;
    - Identify appropriate logistics and employee support needs (e.g., family notification/reunification center), critical employee support resources (crisis counselors, childcare, evacuation, transportation, etc.); and basic

necessities (water, restrooms, etc.) that will need to be available in the event of an incident) and establish relationships with supplier/providers where necessary.
    - Adopting and training on a standardized system for managing an incident;
    - Review and update applicable procedures based on the evaluation and assessment of the program; and
    - Pre-plan with multitenant facilities to understand each other's procedures and processes in responding to and mitigating active assailant situations. This will also provide organizations with the opportunity to establish a relationship and open communication with tenants should the need arise to discuss other potential threat management concerns in the facility.
- Incident Response:
    - The onsite leader implements response protocols and oversees crisis management processes including but not limited to:
        - Directing all response activities and tactical execution of continuity plans;
        - Establishing real-time communications between site personnel and executive management;
        - Acting as the liaison between on-site crisis team and executive management, vendors, service providers, etc.; and
        - Monitoring and reporting out information related to response/recovery actions and resource requirements.
    - Other considerations include:
        - Directing, monitoring, and reporting on-site security posture and activities;
        - Establishing perimeters to ensure security of assets and response personnel;
        - Establishing secure communications among all parties involved in the management and resolution of the crisis;
        - Ensuring that employees and others on site are accounted for and evacuated to a safe and secure area away from the incident;
        - Implementing plans for notifying and communicating with families of individuals impacted by the incident;
        - Identifying and monitoring media and social media coverage of the incident, both in the home country and globally;
        - Controlling the content, timing, and method of issue of all statements to the media; and
        - Implementing emergency IT plans and capabilities.
- Post-incident Recovery:
    - Identifying the three phases of the recovery process (see Section A.4.1):
        - Immediate recovery;
        - Short-term recovery; and
        - Long-term recovery.

A.2.4 Emergency Management Liaisons

Pre-planning with law enforcement, fire personnel, and other key stakeholders is a critical element in the overall effort to quickly respond to and mitigate an active assailant event. It provides the organization and emergency management partners with clear expectations and limitations should a situation occur.

The organization should establish relationships with law enforcement at every level (e.g., federal, state, local, tribal and territorial), where possible, because those agencies can be an invaluable resource in every phase of an organization's violence prevention, response planning, and incident management. Accordingly, it is prudent to integrate them into your training, familiarize them with your facility, and establish (if needed) a mutual aid agreement (e.g., memorandum of understanding [MOU] or memorandum of agreement [MOA]), with appropriate response agencies. Organizations that have multiple sites should identify which agencies have jurisdiction for specific sites, and establish the appropriate points of contact and communications protocols for on-site personnel to reach those agencies.

It is equally important that the organization develop strong partnerships with other first responders such as fire and emergency medical services (EMS) personnel. Ensuring that these partners are familiar with the incident response team, the facility layout, any facility-specific hazards, as well as access to utility controls, medical supplies and other relevant systems, allows them to move through the facility more fluidly during an emergency.

Once the partnership has been established, the organizations should:

- Identify and maintain a current law enforcement, fire personnel, and other key stakeholders' point of contact list;
- Conduct annual tabletop exercises with external emergency management agencies; and
- Host annual meetings with law enforcement and selected key stakeholders, and offer site familiarization tours for law enforcement and other first responders.

Organizations should be aware that emergency management agencies can vary based on multiple jurisdictions.

A.2.5 Emergency Response Kits/Bags

Pre-planning with law enforcement, fire personnel, and other key stakeholders is a critical element in the overall effort to quickly respond to and mitigate an active assailant eventPhysical and technical security measures may prevent or slow first responders' access to a facility unless emergency response kits/bags are deliberately developed and strategically placed to help bypass security measures. The organization should create, maintain, and properly secure emergency response kits/bags to be used in the event a situation occurs.

The organization should include the following in its emergency response kits/bags:

- Tools to access the facility, such as access control badges or grand master keys;

- Laptop/tablet with portable wireless devices with connectivity to the organization's network to access digital copies of floor plans, contact list, and connection to on-site video camera feeds (if possible);
- Property maps and floor plans in hard copy format, including aerial photos with areas identified;
- Contact list of all organization emergency management personnel including incident command system (ICS) positions;
- Radios for interoperable communications between first responders and organization personnel including, but not limited to: security, facilities, engineering, and safety;
- Doorstops, flashlights, permanent ink pen/marker, and paper; and
- Hemorrhage control kit for trained employees. Kits should include tourniquets, rapid blood clotting bandages, gauze, and/or trauma dressings.

A.2.6 Notification and Communication Strategies (Pre-Incident Planning)

Initial communications during an active assailant incident prior to the arrival of law enforcement and other first responders are of critical importance to convey the present danger and location (if known) to internal or external audiences. In this regard, the purpose is to manage crisis communications in a professional, timely, and clear manner so that people know to protect their health and safety during a chaotic situation.

In the pre-planning stage, it is essential to identify a redundant mass notification system (primary and backup) and ensure that procedures and protocols for systems are outlined in the event individuals must hide and are unable to use landlines or desktop computers.

The organization should consider using all available mass communications options that can be accessed using:

- Handheld and/or mobile devices;
- Emergency alert systems;
- Website banners;
- Email and text messages;
- Audio broadcast announcements; and
- Automated calls with recorded messages (e.g., reverse 911 systems).

As part of its protocols, the organization should include alternate forms of communications for persons with visual or auditory impairments. In addition, the organization (where appropriate) should investigate the need to develop notification capabilities in alternate languages.
Many systems also incorporate interactive response technology and real-time reporting/analytics that can allow for tracking to ensure that messages have been received/acknowledged.

When an emergency suddenly strikes an organization, its website is ordinarily the first place the outside world turns to for information. There is rarely enough time to construct a new crisis site from scratch. Accordingly, organizations should consider establishing a prebuilt website, webpage, or microsite that can be quickly enabled or "turned on" as needed during a crisis.

The organization should ensure authorized individuals have received proper training on all the systems and that the systems are tested on a frequent basis (e.g., monthly, quarterly) and are working properly.

A.2.7 Guidelines for Selecting Staging and Operations Areas

The organization should pre-establish primary and alternate staging and operations locations in the event of an active assailant situation. The organization should consider various factors when selecting primary locations and alternates. Events will require the consideration of adjusting command structures to scale, and logistical considerations such as computers, phones, workspace, break-out rooms, restroom facilities, food, water, rest areas, etc.

Considerations for critical locations include:

- Emergency operations center (EOC) is typically responsible for carrying out emergency responses, business continuity operations, and crisis communications during an event (e.g., active assailant, fires, widespread power loss, floods, earthquakes, etc.). EOCs are typically managed by established emergency response personnel;
- Incident command center (ICC) location and alternates will serve as a secure location for command and control of an incident. Considerations for an ICC should include relative security and proximity to the incident, as well as size of location to accommodate adequate personnel and equipment. The location of the ICC is communicated to all responding entities including different departments, agencies, and disciplines/functional areas;
- Media staging area is set aside for interaction with the media to provide incident updates and answer media questions as appropriate. The media staging area should be placed away from ongoing operations with no view of incident management actions to protect affected individuals, responders, and scene integrity. However, the location needs to be convenient to command personnel that would be responsible for media interaction so that quick updates can be provided without impacting critical operations; and
- Family notification/reunification center is a centralized safe and secure location for individuals evacuated from and coming to the incident area (e.g., family members, significant others, individuals waiting for victims). It also provides incident updates and controls misinformation. The family notification/reunification center should be placed away from the media staging area and ongoing operations with no view of incident management actions. It is imperative that an organizational representative be at this location. This representative should identify and create a list of the individuals present and update the list with individuals being transported to the location from the incident. This list should include family members and other individuals that arrive throughout the incident.

In addition, is it important to recognize and be aware that victims may choose to transport themselves to the nearest hospital which may cause the closest hospital to be overwhelmed faster. Therefore, organizations should identify available hospitals capable of handling mass

trauma incidents. Having contact information for all local hospitals will significantly assist in reunification and information sharing.

A.2.8 Test and Validate the Plan

The active assailant draft plan should align with best practices and contain planning assumptions that should be tested and validated before finalizing the plan. Once developed, organizations should initially facilitate an internal plan validation workshop which includes a tabletop exercise. The tabletop exercise will enable the team to work through the complexities of dealing with an incident and its recovery, challenges (particular planning assumptions), and refining the process.

The training program should cover the following objectives:

- Review the following elements of plan with team members, including but not limited to:
    - Team roles and responsibilities;
    - Training requirements;
    - Testing notification and communication systems;
    - Effective crisis communications; and
    - Other relevant topics, such as staging and operations areas, legal considerations, business continuity.

Organizations should distribute the plan to team members prior to the training workshop.

- Validate plan assumptions through a simulated tabletop exercise. This type of exercise is designed to facilitate the response and analysis of an emergency event to relevant stakeholders in an informal, stress-free environment. The tabletop exercise should:
    - Help team members understand how to approach the emergency event;
    - Identify how team members should communicate with each other (e.g., personnel, systems, etc.);
    - Identify which team members need to coordinate with law enforcement, fire, emergency medical services (EMS), top management, etc.;
    - Include actions team members can take to protect lives and assets;
    - Demonstrate strengths and areas for enhancement of the plan; and
    - Facilitate discussion for a mutual interaction and understanding among various departments and working groups.
- Once the plan is internally validated, include local external response personnel (e.g., law enforcement agencies, fire departments, and emergency medical services, etc.) in a subsequent tabletop exercise so they understand the organization's plan. It is critical to incorporate their response protocols into the tabletop exercise to ensure rapid access to the facility and an understanding of how the organization and the responding agencies work together; and
- Identify and incorporate lessons learned and areas for improvement for the plan throughout the process.

In a tabletop exercise environment, the scenario can incorporate crisis communications to the media and other stakeholders, counseling, and follow-up care for the affected workforce, and other business continuity considerations.

A.2.9 Training for Response Teams

The organization may choose to conduct full-scale drills. A full-scale drill is coordinated with first responders and is designed to simulate a real event as closely as possible. A full-scale drill should only be exercised once the active assailant plan has been validated and tabletop exercises with external response personnel have been conducted. To be effective, a full-scale drill should be realistic and encapsulate all components of the response effort, including the command structure, use of any equipment needed for the response, and effective and timely communications. Members of the organization's incident response team should be well versed in their roles and responsibilities prior to the full-scale drill in order to perform successfully under pressured circumstances. This should include awareness by security personnel of their responsibilities and actions to be taken, depending on the circumstances, as an active assailant event is unfolding. This will help team members understand how to approach the situation, how they should communicate, who they need to coordinate with, and what steps they can take to protect the lives and assets prior to the arrival of first responders.

A full-scale drill is designed to ensure that external responders are prepared for your specific business setting by allowing them to train at your facility. The organization should seek to interact, coordinate, and align key business resources with the same agencies that will be responding to an actual crisis event. Advanced full-scale drill scenarios may include role players following prewritten scripts and portraying an active assailant or casualties. Participating first responders should include appropriately dressed and equipped tactical teams simulating the search of preselected areas until the assailant is under control and victims are located and treated. In preparation for a full-scale drill, the organization should ensure that its plans include procedures for supporting individuals who may require assistance (e.g., children, elderly, persons with disabilities or mobility issues, etc.). The organizations should also carefully consider the timeframe for conducting full-scale drills and ensure that employees, volunteers, neighbors, the community, as well as other stakeholders, are notified well in advance.

Where relevant, notice should be given to concealed-carry permit holders in your organization to ensure that their firearms are not present during the full-scale drill. During the event, communications must be confined to drill participants, and signage should be posted to ensure that no one who is unaware of the full-scale drill walks in on it.

Activation of mass notification process should be tested at the initiation of the simulated incident. The organization should also simulate its primary and alternate staging and operations locations.

The organization's primary focus, after law enforcement takes control of the incident, will be accounting and caring for employees and others who may have been on site at the time of the incident. The exercise could be expanded to include first responders and/or other government

entities beyond the incident site which may include emergency transportation, hospitals, or other related functions.

A secondary focus will be considering business continuity plans to restart normal operations after the incident occurs. Various departments or disciplines may consult on their respective business continuity plans in order to identify critical processes.

After completion, the participants should assemble for an immediate after-action review of the exercise to solicit feedback and identify areas for improvement.

Legal issues can arise in conducting active assailant training exercises. Accordingly, the organization should coordinate and communicate in advance with the workforce that the drill being conducted is a training exercise.

A.2.10 Employee Awareness Training

An organization should provide active assailant awareness training to its employees/workforce to promote an environment of shared responsibility when it comes to safety and security in compliance with applicable laws and regulations. Awareness training should emphasize the employee's reporting responsibility, response options, and available organizational resources. The training should familiarize the workforce with alert systems, evacuation routes, safe havens, and other general concepts the organization has established to better prepare for and react to an active assailant situation (e.g., run, hide, fight, defend, etc.). The organization should also take into consideration in its training program the response options for individuals with disabilities.

A.2.10.1 Checklists/Tools Guidelines

The organization should identify and provide materials containing critical information on response components in an active assailant incident to support its training efforts and build awareness. Informational materials should be made available to all employees and posted in high-traffic areas such as break rooms, hallways, workspaces, offices, conference rooms, the organization's intranet site, and other suitable areas. Examples of informational materials include, but are not limited to:

- How to report an active assailant incident;
- Checklist of options for employees when dealing with an active assailant incident;
- Organization's policy on active assailant incidents; and
- Review of evacuation procedures.

A.2.11 Psychology Aspect

A.2.11.1 Psychological Preparation for an Incident

An incident involving an active assailant will cause a variety of psychological effects that will have consequences to the behavior and performance of individuals during the time of the incident and long after. Given this reality, organizations should take important preparation steps to provide pre-incident information to its workforce regarding the effects of traumatic events on

individuals. This pre-incident education has been shown to reduce some of the effects of trauma during the event itself, as well as aid in the post-incident processing and reduction of post-traumatic incident effects.

In addition to this pre-incident training, it is also important that the organization identify trained mental health providers in the community that can provide mental first aid and trauma counseling services in the aftermath of an incident. The sooner individuals that need assistance are identified and connected with, the more likely they can be provided, and be willing to accept, the support they may need to begin processing their emotional reactions to the incident.

In general, considerations for pre-incident psychological preparation include:

- Training in mental first aid for emergency responders and individuals in positions of organizational responsibility (e.g., managers, supervisors, teachers, administrators, peer counselors, etc.).
- Training on the effects of trauma, including:
    - Altered perceptions and/or disorientation;
    - Shock;
    - Fear; and
    - Slowed response times.
- Training on how to overcome the effects of trauma, including:
    - Monitoring for signs of negative emotional and psychological effects;
    - Guiding individuals to areas away from high-traffic activity;
    - Helping individuals focus on breathing exercises, while limiting visual distractions;
    - Providing hydration such as water, juice, sport drinks; and
    - Providing individuals with the means to stay warm.

This psychoeducation should be provided both verbally and in writing. It is deeply reassuring, in the aftermath of an active assailant incident, to realize that many reactions from individuals are a normal response to an abnormal event.

A.2.11.2 Psychological Issues for Consideration and Management During an Incident

The organization should consider the following during an active assailant incident:

- The role of first responders and appropriately trained organizational individuals, and the need to actively triage individuals for shock and trauma, when it is safe to do so. If the incident has been contained to a specific area, then, ideally, a space should be located out of the active incident area at a distance that limits the auditory and visual stimulus from the incident, so that individuals placed in that area will have an opportunity to be provided hydration, warm coverings, and a calmer environment, where they feel safe to begin the process of re-engaging with their environment; and
- Monitoring all critical incident responders to note behaviors that would suggest individuals need to disengage, even briefly, from immediate activity to allow them to refresh their mental and emotional resources. Individuals under high stress may experience diminished cognitive capacity and decreases in appropriate judgment, thereby affecting the quality of their response to the demands they are facing.

A.2.11.3 Psychological Issues for Consideration and Management After an Incident

After an active assailant incident, victims represent the first group of those impacted; however the organization should also recognize others who may be affected such as witnesses, emergency responders, first responders, and the community at large.

It is important to note that not all individuals involved in active assailant incidents will require professional services. The support of their loved ones and the community, as well as religious/spiritual support, is often sufficient. Care must be taken to determine those who develop more intense psychological reactions or those for whom a pre-existing condition is aggravated by the recent violence. It is critical to note that some symptoms might take up to six months to surface, so planning should include availability of follow-up for at least six months.

For some, it is only with the passage of time that one realizes that existing coping strategies are not productive or sufficient, so professional services are warranted. Keep in mind that victims might be more receptive to services than emergency responders or first responders, so policies should remove the need for individuals to self-identify and seek help. The culture must be one of support and non-judgment.

In the immediate aftermath of an active assailant incident, we want to activate a network of community resources. As noted above, having a network of services in place facilitates the speed with which professionals can respond.

A.2.12 Legal Considerations

As organizations grapple with the means to address the topic and associated risks of an active assailant, legal principles are of critical importance. As described in this Standard, legal considerations include an understanding of the various national, state, and local laws and statutes pertaining to the pre-planning, response, and recovery of an active assailant event.

The organization should consult its legal counsel to ensure that its active assailant plan complies with applicable laws and regulations. Legal counsel should have the appropriate training, education and experience in a variety of disciplines (e.g., employment law, civil litigation, premise liability, etc.) to provide analysis and recommendations.

With an active assailant event, there will likely be personal injuries and possibly deaths. For that reason, it is of paramount importance that the organization undertake efforts to develop and maintain a program that aims at helping its employees understand the complexities associated with an active assailant event and measures they can take to protect themselves and each other. Immediately after an active assailant event and during the recovery phase, the organization should seek legal counsel and engage with appropriate governmental agencies and departments, as well as law enforcement, in gathering information to conduct an after-action evaluation of the organization’s response, adherence to its established active assailant plan or program, and potential legal liabilities.

A.3 Incident Response

A.3.1 Execute Plan

When an incident occurs organizations should activate their site active assailant plan. This should include activation of:

- Crisis communications;
- Perimeter containment;
- Incident command center;
- Media staging area; and
- Family notification/reunification center.

A.3.1.1 Activate Crisis Communications

The organization should consider on-site communication needs for notification of imminent threat, emergency action procedures, and potential variations from the plan. Off-site crisis communications could include outside agencies, policymakers, media, and families.

Additionally, consideration should be made in advance to plan on what information will and will not be shared in the event of a crisis, as well as a timeline for information sharing. A central location of decision makers should be established (i.e., emergency operations center) to help control the sharing of misinformation.

During an incident, depending on its length, there may be a need to apprise the media of relevant facts to avoid misinformation. During the post-incident timeframe, media will have inquiries regarding the cause of the incident, how it could have been avoided, impact on victims, the company and its employees. Crisis communications responses should be coordinated both internally and externally with entities such as:

- The public information officer;
- Public relations/crisis communication representative;
- Legal counsel;
- Law enforcement; and
- Appropriate government agencies.

The organization should establish a crisis communication approval chain for releasing information to the public and other stakeholders (i.e., release authority). The organization should identify the appropriate senior-level organizational leader with knowledge of the events to serve as the spokesperson for both media briefings and for attribution in written statements.
All communications should be factual, timely, and reflect the appropriate tone of compassion with respect for the privacy of victims and their families. The organization should develop key messages that address the facts of what is known about the incident and the organization's response, as well as an incident chronology and/or fact sheet that can be updated as needed to ensure that all parties have access to accurate, up-to-date information. The organization may wish to prepare a question-and-answer document to help prepare the organizational spokesperson with messaging to address important questions, including those that cannot be answered due to

legal/privacy concerns or lack of information. The organization may wish to post the document on its website as a resource for additional information. All public-facing materials should be periodically reviewed and updated.

Initial media materials should anticipate and try to proactively address public concerns using facts that have been gathered, confirmed, and authorized by law enforcement. Key components of an initial media statement for all media outlets and platforms (which could be prepared and distributed in written format), include but are not limited to:

- People impacted by this situation are the number one priority;
- What is known about the incident;
- Organization is cooperating with law enforcement in their investigation(s);
- What the organization has done so far, and what next steps it is taking; and
- Point of contact for additional information.

Periodic media updates should be scheduled and announced in advance with a goal of balancing the public's interest with appropriate safety, security, and privacy considerations. It may be advisable to require credentials at media briefings to develop an understanding of who is covering the incident and to maintain some control over who attends these sessions. In certain situations, it may be necessary to engage security or local authorities to assist in dealing with confrontations or disruptions. It is appropriate to establish a clear timeframe and topics to be addressed at the beginning of the briefing, followed by prepared statements and Q&A session.

It will be important to establish both mainstream and social media monitoring to allow communicators to identify and address significant inaccuracies in future media updates and organizational communications. If needed, legal counsel can be engaged to assist in efforts to have offensive, violent or confidential content removed.

There are additional audiences, including off-site employees, customers, vendors, local elected officials, community partners and others with which the organization should establish and maintain communication regarding the incident, its impact on business continuity, and supportive services available to victims and their families. Specific organizational leaders should be provided with communications materials (e.g., talking points, draft emails) and assigned responsibility for reaching out to and remaining in communication with specific audiences in the aftermath of an incident.

A.3.1.2 Activate Perimeter Containment

Depending on the location, mobility, and overall dynamics of the threat, perimeter containment should be initiated when reasonable and appropriate. In the beginning stages, an inner perimeter should be established and as more resources arrive, a second outer perimeter can be created. Active assailant incidents are dynamic. While not always possible to contain, initial steps should be taken to prevent potential victims from unknowingly entering an area under active or potential threat.

A.3.1.3 Activate Incident Command Center

Activation of an incident command center is most effective early in an incident. First responders will implement their incident command processes upon arrival. That foundation provides for adaptability should the incident grow in size or complexity.

A.3.1.3.1 Liaise with First Responders

The first group of law enforcement arriving on the scene will focus on clearing and neutralizing the threat. Subsequent first responders arriving on the scene will focus on conducting triage, evacuating those injured, and responding to other critical needs.

It is vital to remain available to liaise with first responders when appropriate. Individuals liaising with responders should be trained and prepared to work in an ICS.

First responders will seek out the organization's facility representative to obtain information and gain access keys or codes for areas in the building that may be secured. Law enforcement and public safety personnel should have free movement on the site and provisions made for providing the contents of the emergency response kits/bags. Limiting the number of people interacting with first responders may be beneficial in the very early stages of an event because vetting information is critical.

A.3.1.4 Activate Media Staging Area

Media staging areas need to be established within a reasonable timeframe to manage the delivery of information. The media can be a resource in information sharing, especially regarding family reunification center information. Consideration needs to be given regarding potential locations and whether or not to have multiple staging areas. In the initial phases and throughout the event, media will typically attempt to get as close to the scene as possible. As the incident continues, they will still want a location for photos and video but may function better in a more formal place for press conferences and information sharing. For long-term events, a typical setup would look like a media staging area on-scene where cameras can be set up. Separate from that location, and typically within relative proximity of the incident command center or emergency operations center, an additional media area may be established for press conferences and information sharing.

A.3.1.5 Activate Family Notification/Reunification Center

Family notification/reunification center preparedness should be considered early in an event because activation and preparation may take longer than expected. The announcement of the center's location will typically coincide with notification to involved parties. It is essential to be able to provide as much information as possible to those notified, especially regarding where to go, because their natural inclination will be to go to the incident area. Relaying the location of a center will significantly assist in minimizing the number of people reporting directly to the scene.

A.4 Post-incident Recovery

A.4.1 Phases of Recovery

Below are the three phases of the recovery process that may overlap and can run concurrently:

- Immediate recovery phase includes but is not limited to:
    - Coordinating medical assistance and life safety activities;
    - Identifying and accounting for all individuals who were on site during the incident (employees, visitors, customers, vendors, etc.); and
    - Ongoing communications to employees, families, the public, and the media.
- Short-term recovery phase includes but is not limited to:
    - Activating an emergency operations center, if needed, to coordinate incident management response and support business continuity activities;
    - Preserving the crime scene. Once authorized by law enforcement, scene clean-up and stabilization process can begin. Clean-up should be done by trained professionals to lessen the psychological impact;
    - Monitoring response personnel for signs of psychological trauma and, where practical, establishing quiet areas, with access to hydration, and allowing for further evaluation and stress relief;
    - Identifying and activating the family notification/reunification center and ensuring adequate resources (e.g., employee assistance program). This will include information about survivors relocated to hospitals;
    - Helping relocate evacuees and witnesses to the family notification/reunification center to enable them to contact family/friends and assist law enforcement as needed;
    - Providing information about stress reactions and coping strategies, and access to resources (e.g., crisis lines and employee assistance program) to individuals who are impacted by the incident; and
    - As soon as feasible following the active assailant incident, organizations should also review and consider necessary revisions to planned communications tools and events, both to share information and to demonstrate sensitivity and compassion. This could include:
        - A new website landing page or banner that acknowledges the incident and provides necessary emergency contact or business continuity information, as well as information about any donation or public support opportunities;
        - Telephone hotline with recorded message;
        - Electronic message boards or signage;
        - Prescheduled communications, including advertising, newsletters, email, or social media content; and
        - Special or celebratory events.
- Long-term recovery phase includes but is not limited to:
    - Conducting a formal post-incident debrief with internal and external emergency management and key stakeholders, as appropriate;

- Providing information about and access to group and individual counseling services. Anniversary dates can be of concern, the organization should consider a pre-plan to have services available;
- Supporting the business continuity plan(s), which should include performing damage assessments and restoring operations for a sustainable recovery;
- Replenishment of emergency supplies and kits; and
- Communications at anniversaries and in the aftermath of a similar local or national incident.

Annex B

(informative)

B.1 References

ASIS ESRM-2019, Enterprise Security Risk Management Guideline, ASIS International, 2019. Available at < **http://www.asisonline.org** >.

ANSI/ASIS/RIMS RA.1-2015, Risk Assessment Standard, ASIS International, 2015. Available at < **http://www.asisonline.org** >.

ISO 31000, Risk Management - Guidelines. Available at < **http://www.iso.org** >.