



Security Plan

Information Adopted Material

Violence in the Federal Workplace:
A Guide for Prevention and Response

Cyber Bullying

Assault
Warning
Signs of
Violence

Employee
Assistance
Programs
Considerations

Behavioral Risks Assessment

Psychological
First Aid

Written Policy

Active Shooter/
Active Threat
Evacuation Plan

Risk Assessment

Insider Threat

Risk Assessment
Computer Security

Workplace Security

Workplace Violence Response

Facility Security & Protection

Bullying

Incident Response
Team
Active Shooter/
Active Threat

**Insider
Threat**

Threat Assessment

Security
Measures

Planning &
Prevention

Stalking

**Workplace
Violence
Prevention**

Organization
Recovery
Post-Incident

Violence in the Federal Workplace:

A Guide for Prevention and Response

2019



Interagency
Security
Committee

Change History

Rev. #	Date	Changes	Approver
1.0	1998	Initial issue	Office of Personnel Management
2.0	2010	Complete document revision	Interagency Security Committee
3.0	2013	Complete document edit and structural revision; separation of appendices into standalone documents	Interagency Security Committee
4.0	2019	Completed document edits and structural revision; Appendices A, B, and C were created as separate standalone documents	Interagency Security Committee

NOTE: This version of *Violence in the Federal Workplace: A Guide for Prevention and Response* replaces all previous editions of the Office of Personnel Management’s handbook, *Dealing with Workplace Violence: A Guide for Agency Planners*.

Message from the Chair

No workplace is immune to violence, as shown by recent events in the public and private sectors. Even our Federal facilities can serve as the setting for an incident. One of the Department of Homeland Security's (DHS) top national priorities is the protection of Federal employees, contractors, and visitors to U.S. government-owned or leased facilities. The Interagency Security Committee (ISC), chaired by DHS, consists of 60 Federal Departments and Agencies committed to enhancing the quality and effectiveness of security and protection in those facilities. The ISC's mission is to develop security standards and best practices for non-military Federal facilities in the United States.



As Chair of the ISC, I am pleased to present this update to the ISC's *Violence in the Federal Workplace: A Guide for Prevention and Response* (2019). This guide updates the ISC publication *Violence in the Federal Workplace: A Guide for Prevention and Response* (2013). It provides comprehensive information to assist in the creation of an effective workplace violence prevention and response program. The document also addresses facility security issues relevant to workplace violence and provides a variety of examples based on real-world events for planners to study and take into consideration.

Consistent with Executive Order (EO) 12977, this guide will assist those responsible for the security and protection of all buildings and facilities in the United States occupied by Federal employees for non-military activities. These include existing owned, to be purchased, or leased facilities; stand-alone facilities; Federal campuses; individual facilities on Federal campuses; and special-use facilities. Additionally, this guide applies to all off-installation leased space managed by the Department of Defense (DoD) and all DoD-occupied space in buildings owned or operated by the General Services Administration (GSA).

As with all ISC documents, *Violence in the Federal Workplace: A Guide for Prevention and Response* (2019) is a collaborative effort across multiple Federal agencies within the ISC. In particular, I would like to thank the ISC Workplace Violence Working Group for their hard work and dedication to this important publication.

A handwritten signature in black ink, appearing to read 'Brian Harrell', written in a cursive style.

Brian Harrell
Interagency Security Committee Chair
Department of Homeland Security

Executive Summary

The overwhelming majority of instances of Federal workplace violence were a result of acts conducted by employees and customers—individuals who were permitted to be at the Federal site.¹ One example of this type of incident occurred on September 16, 2013 at the Navy Yard in Washington, D.C. The Navy Yard shooting is an extreme example of how an office setting can be affected by workplace violence.

Fortunately, tragic events such as these are still the exception. Most acts of Federal workplace violence occur as some form of verbal or non-verbal threat, bullying, harassment, intimidation, or non-fatal physical assault. However, it is important to remember that acts of physical violence might start with behavioral risk indicators. Agencies must take all reported safety concerns seriously and respond appropriately. It is also important to note that most threats will not lead to a violent act in the majority of cases. The threat itself, however, affects the workplace and must be addressed.

An act of workplace violence generally can be categorized as one of four types:²

- Criminal intent;
- Customer/client;
- Employee on employee; or
- Personal relationship.

According to the Occupational Safety and Health Administration (OSHA), workers are at greater risk of becoming victims of workplace violence if they:

- Exchange money with the public;
- Deliver passengers, goods, or services;
- Work alone or in small groups during late night or early morning hours;
- Work in high-crime areas; or
- Work in community settings and homes experiencing extensive contact with the public.³

In addition to these standard descriptions of incidents and the classification categories in use since at least 2000, newer classification systems focus on triggers and intent, often distinguishing

¹ U.S. Merit Systems Protection Board's *Employee Perceptions of Federal Workplace Violence Report*: <https://www.mspb.gov/mspbsearch/viewdocs.aspx?docnumber=759001&version=761840&application=ACROBAT>, accessed May 1, 2018.

² McPhaul, K., Lipscomb, J., (September 30, 2004). "Workplace Violence in Health Care: Recognized but not Regulated". *Online Journal of Issues in Nursing*. Vol. 9 No. 3, Manuscript 6. Available at: <http://ojin.nursingworld.org/MainMenuCategories/ANAMarketplace/ANAPeriodicals/OJIN/TableofContents/Vol9me92004/No3Sept04/ViolenceinHealthCare.aspx>

³ Department of Labor, 2002

predatory from affective violence. Identifying triggers and intent can support risk assessment and prediction of recurrence, as well as the required prevention strategies.⁴

The remainder of this document provides guidance on planning, prevention, and response, as well as administrative inquiries and the assessment process. The document is accompanied by three appendices:

- *Appendix A: Awareness* addresses a process for evaluating threats to Federal facilities.
- *Appendix B: Resources* provides a list of resources, such as free courses and online materials.
- *Appendix C: Case Studies* provides extensive case studies.

The information provided in this guide is based on the collective expertise and experience of Federal Government law enforcement officers, security specialists, criminal investigators, attorneys, employee relations specialists, employee assistance program counselors, forensic psychologists, and union officials. It consists primarily of lessons learned from many years of experience with actual cases involving potentially violent employees. The guidance covers not only the macro issues of facility security, but also incidents of physical violence such as shootings and assaults and the far more prevalent incidents of nonphysical violence, intimidation, bullying, and other inappropriate behaviors prone to create an environment that can exacerbate the potential for violence.

⁴ Meloy, JR. Empirical basis and forensic application of affective and predatory violence. *Aust N Z J Psychiatry*. 2006 Jun- Jul;40(6 - 7):539-47.

Table of Contents

- Change History..... 1**
- Message from the Chair 2**
- Executive Summary 3**
- Table of Contents 5**
- 1.0 Introduction 9**
- 2.0 Purpose 11**
- 3.0 Contributors..... 13**
- 4.0 Planning, Prevention, and Response 14**
 - 4.1 Program Development..... 14**
 - 4.1.1 Forming an Agency Planning Group 15**
 - 4.1.1.1 Fill the Skill Gaps..... 16**
 - 4.1.1.2 Law Enforcement and Security Assistance 17**
 - 4.1.1.3 GSA Designated Officials 18**
 - 4.1.1.4 Working with Your Union 18**
 - 4.1.1.5 Working with Your Insider Threat Program 19**
 - 4.1.2 Assessment and Analysis 20**
 - 4.1.2.1 Analyze Your Agency’s Current Ability to Handle Potentially Violent Situations... 20**
 - 4.1.2.2 Review Existing OEPs 21**
 - 4.1.2.3 Physical Security Assessment 21**
 - 4.1.2.4 Physical Security Measures..... 22**
 - 4.1.3 Develop a Procedure for Employees to Report Incidents 23**
 - 4.1.3.1 Reporting..... 24**
 - 4.1.3.2 Field Worker Concerns 24**
 - 4.1.4 Develop Plans to Respond to Workplace Violence Incidents..... 25**
 - 4.1.4.1 Workplace Violence Incident Response..... 26**
 - 4.1.4.2 Communication 26**

4.1.4.3	Supportive Resources and Care.....	27
4.1.4.4	Facility Response	27
4.2	Prevention.....	28
4.2.1	Warning Signs of Violence	28
4.2.2	Pre-Employment Screening	30
4.2.2.1	Hiring Process	30
4.2.2.2	Challenges to the Hiring Process	31
4.2.2.3	Resources and Support.....	32
4.2.3	Training.....	32
4.2.3.1	Employee Training.....	34
4.2.3.2	Supervisor Training.....	35
4.2.3.3	Incident Response Team Training.....	36
4.2.4	Using Alternative Dispute Resolution as a Preventive Strategy.....	37
4.2.4.1	Ombudsmen	37
4.2.4.2	Facilitation.....	37
4.2.4.3	Mediation	37
4.2.4.4	Interest-Based Problem Solving.....	38
4.2.4.5	Peer Review	38
4.2.4.6	Termination of Employment	38
4.2.5	Computer Security	39
4.2.5.1	Revocation of Access after Termination.....	39
4.3	Conclusion to Planning, Prevention, and Response	40
5.0	Administrative Inquiries and the Assessment Process	41
5.1	Fact Finding.....	41
5.1.1	Incident Intake and Inquiry	41
5.1.2	Understanding the Situation.....	42
5.1.3	Consider Immediate Security Needs.....	42
5.2	Types of Investigations and Inquiries	43
5.2.1	Administrative Inquiries	43
5.2.1.1	Use a Trained and Appointed Fact Finder	43

5.2.1.2	Ensure Criminal Prosecutions are Not Compromised.....	44
5.2.1.3	Guidance for Information Gathering and Interviewing.....	44
5.2.1.4	Reviewing Available Information.....	45
5.2.1.5	Selecting an Interview Site.....	45
5.2.1.6	Scheduling the Interview.....	45
5.2.1.7	Allowing the Presence of Additional Persons.....	45
5.2.1.8	Adhering to the Law Regarding Bargaining Unit Employees	45
5.2.1.9	Taking Notes	46
5.2.1.10	Maintaining Control of the Interview	46
5.2.1.11	Developing Rapport.....	46
5.2.1.12	Handling Hostility.....	47
5.2.2	Other Considerations for the Agency Planning Group.....	47
5.2.2.1	Agency Policy	47
5.2.2.2	Administrative Details	48
5.2.2.3	Factors in Credibility Determinations by MSPB	48
5.2.2.4	Contents of the Final Inquiry Report.....	48
5.2.3	The Behavioral Risk Assessment Process	49
5.2.3.1	Framework and Methodology	49
5.2.3.2	Resources	49
5.2.3.3	Considerations and Fundamental Principles	49
5.2.3.4	Threat Assessment Program Process and Framework	51
5.3	EAP Considerations	56
5.3.1	Overview of the Employee Assistance Program.....	57
5.3.2	EAP’s Role in Dealing with Workplace Violence.....	57
5.3.2.1	Role in Early Prevention Efforts.....	57
5.3.2.2	Participation on an Incident Response Team	58
5.3.2.3	Consultation with Supervisor when an Incident is Reported	58
5.3.2.4	Response and Intervention	59
5.3.2.5	Follow-up to a Violent Event.....	59
5.3.2.6	Individual Interventions	59
5.3.2.7	Acting as Consultants to Management.....	59

5.3.3	Other EAP Considerations for the Agency Planning Group.....	60
5.3.3.1	Should the EAP Take the Incident Report?.....	60
5.3.3.2	Should the EAP be the First to Intervene?	61
5.3.3.3	Should the EAP Perform Psychological Exams?	61
5.4	Organizational Recovery Post-Incident.....	61
5.4.1	Management Steps to Help an Organization Recover	61
5.4.1.1	Share Information with Employees.....	62
5.4.1.2	Bring in Crisis Response Professionals.....	62
5.4.2	Critical Incident Stress Management Process.....	63
5.4.2.1	Purpose of Behavioral Health Response	64
5.4.2.2	Response Team	64
5.4.3	The Psychological First Aid Model	64
5.4.4	Is a Behavioral Health Response Warranted?.....	65
5.4.5	Conclusion	66
6.0	Development of Written Policy	67
6.1	Advantages of Written Policies.....	67
6.2	Policy Statement Contents.....	67
6.3	Recommend Approaches.....	68
7.0	Acknowledgements.....	70
7.1	ISC Working Group Participants (2019 Edition).....	71
7.2	ISC Working Group Participants (2013 Edition).....	73
7.3	ISC Working Group Participants (2010 Edition).....	74
7.4	OPM Working Group Contributors (1998 Edition).....	75
	Abbreviations / Acronyms / Initialization List.....	76

1.0 Introduction

This document supersedes and updates both the ISC publication *Violence in the Federal Workplace: A Guide for Prevention and Response* (2013) and the handbook *Dealing with Workplace Violence: A Guide for Agency Planners*, produced by the U.S. Office of Personnel Management (OPM) in 1998. It provides a framework for Federal departments and agencies to use in the protection of the Federal workforce and Federal facilities from acts of violence, as well as guidelines for creating workplace violence prevention and response programs. The document also addresses facility security issues unique to such incidents.

Workplace violence has the potential to affect every Federal employee throughout the United States. It is the responsibility of Federal managers and supervisors to plan for a wide variety of incidents that could impact their employees and facilities. Organizations such as the National Institute for Occupational Safety and Health (NIOSH) and OSHA play a leading role in helping employers recognize and respond appropriately to the risks and consequences of workplace violence.

The continuum of violent acts ranges from more common non-physical acts (such as incivility, bullying, gestures, expressions, and verbal threats) to less common physical acts (such as battery, aggravated assault, suicide, homicide, and acts of terrorism). Public interest and media attention tend to focus on dramatic but rare incidents of violence, such as shootings in office settings. This focus presents the dual challenge of reducing employees' anxiety about rare risk factors while focusing their attention on more likely but less dramatic sources of danger. Anxiety about relatively infrequent incidents can stand in the way of identifying more significant risk factors such as poorly lit parking lots or gaps in employee training programs. This anxiety can make it more difficult to cope with one of the most common workplace violence problems: the employee whose language or behavior frightens coworkers. Victims and coworkers who survive this type of workplace violence may experience psychological distress or physical injury.

Violence or threats of violence can occur anywhere. For the purpose of this document, "the workplace" includes numerous types of environments such as, but not limited to, office space, retail settings, and field work. Examples of workplace violence incidents in these settings can be found in Appendix C of this guide.

Any Federal worker, including office workers with little public contact, can be exposed to workplace violence. Acts of violence in the workplace generally fall into one of four categories:

- **Criminal Intent:** The perpetrator has no legitimate relationship to the agency or its employees and is usually committing a separate crime, such as robbery, in conjunction with the violence.
- **Customer/Client:** The perpetrator has a legitimate relationship with the agency and becomes violent while being served by the agency. This category includes customers, clients, patients, students, inmates, and any other group to whom the agency provides

services. Employees working for government agencies servicing large segments of the public on a daily basis are likely to be exposed to this type of workplace violence.

- **Employee on Employee:** The perpetrator is a current or former employee who attacks or threatens another employee or employees in the workplace.
- **Personal Relationship:** The perpetrator usually does not have an association with the agency but has a personal relationship with an agency employee. This category includes domestic violence that spills over into the workplace.

A comprehensive workplace hazard prevention and response program should be designed to address the categories of workplace violence listed above. A good program begins with management commitment and employee involvement. The program's success depends on collaboration within and outside the organization. As such, it is important to involve any recognized labor organizations in the early stages of program development. As employee representatives and advocates, labor organizations can provide valuable input on programs affecting the health and safety of the Federal workforce. Planning team members should include, for example, facility security staff and local and state law enforcement and emergency personnel when developing actual plans and programs (discussed in Chapter 4).

2.0 Purpose

The purpose of this document is to provide guidance on how Executive Branch agencies can execute their general duty to protect Federal employees.

The Occupational Safety and Health Act of 1970 (the Act) was written, “...to assure safe and healthful working conditions for working men and women...” While OSHA did not promulgate a regulation specific to workplace violence, 29 Code of Federal Regulations (CFR) §1960.8(a) requires, “the head of each agency [furnishes] to each employee employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm”. Much like Section 5(a)(1) of the Act is the General Duty Clause for private sector employers, which tasks Executive Branch agencies with the general duty of protecting Federal employees from workplace hazards not covered by specific OSHA standards.

Among its specifications, the Act stipulated:

- The development and promulgation of occupational safety and health standards by the Department of Labor (DOL) (Section 6 of the Act, 19 U.S. Code (USC) §655) that led to the creation of OSHA. OSHA is tasked with, among other things, developing, promulgating, and enforcing the standards required by Section 6 of the Act.
- The requirement for Federal agencies to establish and maintain occupational safety and health programs (Section 19 of the Act, 29 USC §668) that led to the development of EO 12196, *Occupational Safety and Health Programs for Federal Employees*, issued February 16, 1980. EO 12196 prescribes additional responsibilities for the heads of Federal agencies. The Secretary of Labor, through OSHA, is required to issue basic program elements for Federal agency occupational safety and health (OSH) programs. These basic program elements are set forth in 29 CFR §1960.
- The creation of NIOSH as part of the Centers for Disease Control and Prevention (CDC) in the Department of Health and Human Services (HHS) (Section 22 of the Act, 29 USC §671) that performs research in fields related to occupational safety and health, and provides OSHA-related information, education, and training. NIOSH is a world leader in helping to prevent work-related illness, injury, disability, and death through its activities of gathering information, conducting scientific research, and translating the resulting knowledge gained into a variety of products and services, such as training materials and recommendations for improving safety and health in the workplace.

Section 19 of the Act, EO 12196, and the basic program elements under 29 CFR §1960 apply to all agencies of the Executive Branch except military personnel and uniquely military equipment, systems, and operations. Within OSHA, the Office of Federal Agency Programs provides Federal agencies with the guidance necessary to implement effective occupational safety and health programs.

Additionally, EO 12977, *Interagency Security Committee*, issued October 19, 1995, called for the creation of the ISC. EO 12977 mandated that the ISC establish security policies and standards to enhance the quality and effectiveness of security in and protection of buildings and facilities in the United States occupied by Federal employees for nonmilitary activities.

3.0 Contributors

The ISC recognizes the Federal partners who provided resources and staff time for the preparation of this document. These partners include: Administrative Office of the United States Court (AOUSC), Department of Commerce (DOC), Department of Energy (DOE), Department of Homeland Security (DHS), Department of Justice (DOJ), Environmental Protection Agency (EPA), Federal Aviation Administration (FAA), Federal Bureau of Investigation (FBI), Federal Protective Service (FPS), General Services Administration (GSA), Internal Revenue Service (IRS), Office of Personnel Management (OPM), Pentagon Force Protection Agency (PFPA), and the U.S. Customs and Immigration Services (USCIS).

This guide builds upon the contributions of experts from many professions and Federal agencies. A special thanks to those individuals who lent their expertise, experience, and talents in providing answers to some of the more difficult questions about handling potentially violent situations. For a list of individual contributors to *Violence in the Federal Workplace: A Guide for Prevention and Response*, please see the end of this document.

4.0 Planning, Prevention, and Response

While some cases of workplace violence can be dealt with swiftly by a supervisor with the assistance of just one specialist or one office, cases can be resolved more easily and effectively if there is a joint effort planned in advance by trained specialists from different key disciplines.

Many people who have never experienced workplace violence believe it will never happen in their office. Violent incidents are relatively rare, but they do occur and can cause injury or death. A little preparation and investment in prevention could save a life. There is no strategy that works for every situation, yet the likelihood of a successful resolution is much greater if there are preparations.

In dealing with the more common incidents generated by an employee, the experience of agencies with developed programs show that supervisors are more willing to confront an employee who exhibits disruptive and intimidating behavior when they are supported by a group of trained and experienced specialists. Supervisors who receive training are prepared to reach out to others when they know a situation is beyond their expertise. This team approach promotes creative solutions and much needed support for supervisors in dealing with difficult situations that might otherwise be ignored.

Ignoring a situation usually results in escalation of the problem. Morale and productivity are lowered, which may result in employees leaving the organization. By contrast, dealing effectively with situations like hostility, intimidation, and disruptive conflict creates a more productive workplace. This proactive approach demonstrates to employees that improper actions have consequences and that their organization does not tolerate disruptive behavior. This can have a deterrent effect on anyone contemplating or prone to committing acts of physical violence.

4.1 Program Development

All Federal agencies should develop and codify effective workplace violence prevention policies and programs, supported by clear procedures and training. Successful workplace violence prevention strategies are multi-dimensional, encompassing a structured training program as well as clearly established reporting and incident communication procedures. Training ensures that workers are aware of potential hazards and understand how to respond when a violent situation occurs. Employees should be encouraged to report incidents with the assurance that management will take such reports seriously and act on them promptly and appropriately. The agency's communication procedures should be defined for all levels. Employees should receive training on communication strategies and techniques.

Agencies can take many different approaches in developing plans to prevent workplace violence. An approach that works well in one agency may not be suitable for another. This section outlines some broad guidelines to assist agencies in the following tasks:

- Analyze the agency’s current ability to handle potentially violent situations;
- Fill any existing skill gaps;
- Develop response plans;
- Develop a policy that includes procedures for employees to report incidents; and
- Develop standard operating procedures for those responsible to intake, assess, and act on reported incidents.

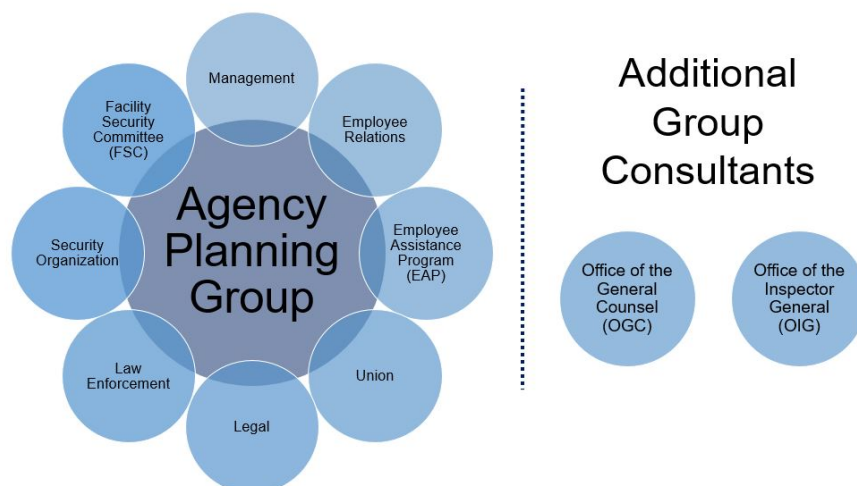
All workplace violence prevention and response programs should meet the minimum requirements set forth in Section 19 of the Act, EO 12196, and the basic program elements under 29 CFR §1960. In addition, it is important to conduct an annual audit of the program to determine any changes that need to be addressed. A sample workplace violence prevention and response program checklist is provided in Appendix B.

In an effective workplace violence prevention and response program, law enforcement, security officers, and the designated Facility Security Committee (FSC) members (if applicable) should be involved in all stages of the planning process. These participants can play an active role in prevention, intervention, and response to threatening situations, in addition to their traditional role of responding to actual incidents of physical violence.

4.1.1 Forming an Agency Planning Group

Successful programs usually start by forming an agency planning group. The agency planning group evaluates the agency’s current ability to handle violent incidents and recommends ways to strengthen its response capability.

The agency planning group should identify the office with primary responsibility for developing and implementing the organization’s workplace violence prevention and response policy and programs. Typically, members of an agency planning group include representatives from management, employee relations, the employee assistance program (EAP), unions, the legal department, law enforcement, and security. Organizations that do not have a law enforcement or security component may wish to consult Federal or local law enforcement when organizing their agency planning group. Depending on the size and structure of the agency, membership may also include representatives from the safety or health unit, medical department, office of Equal Employment Opportunity, public affairs, and other appropriate offices.



The Office of the General Counsel (OGC) and the Office of Inspector General (OIG) should always be extended an invitation to participate in the agency planning group. When these offices are not represented on the agency planning group, they usually act as consultants.

While many offices may be represented on the agency planning group, only a few of them will be involved in responding to reported incidents. For example, representatives from employee relations, EAP, and security often make up the incident response team. Typically, representatives from the other offices will not be involved in responding directly to incidents, but they will act as consultants to the incident response team. Only in certain types of situations will they play an active response role. In addition to individual agencies' response plans, co-located agencies should have a unified response plan in place.

4.1.1.1 Fill the Skill Gaps

Skill deficiencies exist even in large agencies with numerous resources at hand. In some organizations, hostile work environment, risk management, and threat assessment training is needed. However, crisis situations occur infrequently, and it is often not practical to maintain in-house expertise for every aspect of the agency's response plan. The following are suggested sources of outside assistance.

Other Government Agencies

Get to know specialists in other government agencies. Federal agencies often share expertise, especially when crisis situations occur. They are also an invaluable source for learning about new training materials and effective training approaches.

Other Community Resources

Locate and work with resources in the community. For example, if there is no immediate access to emergency mental health consultation, work with the local community mental health

department, hotline staff, hospital, or emergency crisis center. A nearby university may have faculty who are willing to be consulted.

4.1.1.2 Law Enforcement and Security Assistance

If either in-house law enforcement or FPS is available, get to know the responders. Keep in mind that many personnel may find interaction with security somewhat intimidating. Invite the responders to an informal meeting that allows for positive dialogue and an opportunity for non-security personnel to ask questions. In addition, add them to the agency planning group. In-house law enforcement and FPS can provide valuable insight as to how they will respond and assist your group.

In the event law enforcement or FPS is not available, get to know local law enforcement officers. Invite them to work with the agency planning group. During the planning phase, law enforcement/security officers can:

- Identify which situations they have the authority to address;
- Identify when and how they should be notified of an incident;
- Indicate whether their officers have arrest authority;
- Identify jurisdictional restrictions and alternative law enforcement agencies that may assist;
- Identify threat assessment personnel who partner with the agency to protect threatened employees;
- Explain what evidence is necessary after an incident and how it can be collected or recorded;
- Utilize collected or recorded evidence to decide the appropriate level of action to take;
- Explain anti-stalking laws applicable in the agency's jurisdiction;
- Explain where to obtain restraining orders; and
- Suggest security measures to be taken for specific situations.

Additionally, ask whether local law enforcement can arrange for supervisor/employee briefings or training on workplace violence issues such as:

- Personal safety and security measures;
- Types of incidents to report to law enforcement/security;
- Types of measures that law enforcement/security may take to protect employees during an incident;
- Suggestions for reacting to an armed attacker;
- Suggestions for dealing with angry customers or clients;
- How to identify and handle suspicious packages;
- Bomb threats;
- Hostage situations; and
- Telephone harassment and threats.

When potentially violent situations arise, law enforcement/security officers can work with the incident response team to:

- Provide an assessment of the information available;
- Determine whether law enforcement intervention is immediately necessary;
- Identify what plan of action they deem appropriate; and
- Determine who will gather what types of evidence.

4.1.1.3 GSA Designated Officials

DHS is the department responsible for ensuring the safety and security of people while on Federal property owned or leased by GSA. Each GSA-owned or leased facility has a designated official. A designated official is either the highest ranking official of the primary occupant agency of a Federal facility or a designee selected by mutual agreement of occupant agency officials. The designated official is responsible for developing, implementing, and maintaining an Occupant Emergency Plan (OEP) that consists of procedures developed to protect life and property in specific Federal-occupied space under stipulated emergency conditions. In addition, the designated official's responsibilities include establishing, staffing, and training an Occupant Emergency Organization, comprised of agency employees designated to perform the requirements established by the OEP.

According to GSA regulations, GSA must assist in the establishment and maintenance of such plans and organizations. All agencies occupying a facility must fully cooperate with the designated official in the implementation of the emergency plans and the staffing of the emergency organization. GSA must:

- Provide emergency program policy guidance;
- Review plans and organizations annually;
- Assist in training of personnel; and
- Ensure proper administration of OEPs.

In leased space, GSA will solicit the assistance of the lessor to aid in the establishment and implementation of plans.

The regulation states that decisions to activate the Occupant Emergency Organization shall be made by the designated official or by the designated alternate official. Decisions to activate shall be based upon the best available information, including an understanding of local tensions, the sensitivity of target agencies, and previous experience with similar situations. Advice shall be solicited from the GSA buildings manager, the appropriate FPS official, and from Federal, state, and local law enforcement agencies.

4.1.1.4 Working with Your Union

An agency should involve the recognized facility labor union(s) early in the process of planning workplace violence prevention and response programs. Unions are the elected representatives of

bargaining unit employees and are legally entitled to negotiate over many conditions of employment. Although some of the substantive issues relating to workplace violence, including issues concerning internal security, may be outside the duty to bargain, this does not negate consultation and discussion with the union.

Union involvement is particularly appropriate where there are labor management partnership councils. It is a good practice to involve recognized unions before policy decisions are made; this provides them the opportunity to express employees' concerns and bring to bear their expertise and knowledge.

4.1.1.5 Working with Your Insider Threat Program

EO 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, requires Executive Branch Departments and Agencies with access to classified information to implement an insider threat detection and prevention program. If your Department or Agency has an established insider threat program, this program can be an additional resource for reporting, monitoring, and tracking workplace violence. Departments and Agencies with mature, proactive insider threat programs are better postured to deter, detect, and mitigate insider threats before they reach a critical point and potentially harm national security.

The National Insider Threat Task Force (NITTF) published a guide in 2017 that identified best practices to assist relevant organizational components (e.g., employee relations, security) with establishing functional insider threat programs.⁵ The same organizational components that a supervisor would use to report and monitor workplace violence can also provide relevant insider threat awareness information.⁶

Specific best practices listed in the 2017 NITTF Insider Threat Guide are:

- **Proactive Notification:** When a component identifies behaviors that are suspicious or meet the predefined indicator thresholds, the component packages the relevant information and refers the matter to the insider threat program in an expeditious manner.
- **Collaboration:** Mature programs do not develop reporting guidelines in a vacuum. Instead, programs work with the relevant organizational components to collaboratively develop the reporting indicators and thresholds. This enhances relevance and encourages buy-in from stakeholders and participating offices.

⁵ For access to the NITTF guide, refer to: <https://www.dni.gov/files/NCSC/documents/nitff/NITTF-Insider-Threat-Guide-2017.pdf>

⁶ For access to this reference, refer to: [https://www.dni.gov/files/NCSC/documents/nitff/Insider-Threat-Guide-2017-one-page-view\(032618\).pdf](https://www.dni.gov/files/NCSC/documents/nitff/Insider-Threat-Guide-2017-one-page-view(032618).pdf)

- **Risk-Based Approach:** Most Departments and Agencies make a risk-based assessment of the reporting guidelines developed with the components. Programs prioritize indicators based on the value, volume, and time associated with the proactive notification while realizing that every Department and Agency, and every component therein, will be different.⁷

It is essential that the organization's insider threat program and workplace violence program are complementary and mutually reinforcing. For additional information on insider threat mitigation strategies, refer to DHS's Cybersecurity and Infrastructure Security Agency (CISA) website on Insider Threat Mitigation: <https://www.dhs.gov/cisa/insider-threat-mitigation>

4.1.2 Assessment and Analysis

Once the agency planning group is established, the next step is to perform analyses of the current state of your agency's existing risks and response strategies.

4.1.2.1 Analyze Your Agency's Current Ability to Handle Potentially Violent Situations

When beginning the planning process, the agency planning group should:

1. Conduct a risk assessment and analysis of the agency's current ability to handle potentially violent situations (including psychological violence).
2. Review previous incidents that occurred at the agency and in the surrounding area.
3. Evaluate the causes and how effectively they were handled by identifying patterns of risk and potential prevention strategies; for example, when a particular working group has received a number of complaints in a given period of time.
4. Determine whether the agency is prepared to handle incidents of workplace violence by reviewing the example case studies outlined in Appendix C of this guide.

Level of Security and Jurisdictional Issues

An important part of the analysis is to examine the current level of security at the facility. Seek the advice of in-house security, law enforcement, or FPS about recommended basic security measures. Determine in advance all jurisdictional issues among the various security and law enforcement entities that may be involved in an emergency situation.

⁷ NITTF, 2017

Response Time and Incident Reporting Procedures

Response time is one of the critical factors in addressing incidents of workplace violence. All employees should be told which security and/or law enforcement entities to contact in the event of an incident. Contact information for those security and/or law enforcement entities should be made available to all employees.

4.1.2.2 Review Existing OEPs

Agencies should use their existing OEPs as the starting point when developing a workplace violence prevention and response program. The plan should address (where applicable), but is not limited to:

- Notification protocols for reporting incidents;
- Plan initiation and communication;
- Employee notification, communication, and instructions;
- Procedures for determining whether to evacuate or shelter in place;
- Contingency plans for maintaining facility operations;
- Establishment of threat assessment teams (legal, security, human resources, and operational psychology personnel);
- Chain of command and notification protocols;
- Perimeter security, if applicable;
- Protective force communication/protocols;
- Protective force equipment-donning guidelines;
- Plans for conducting training exercises, drills, and other response and preparedness evaluations;
- Initial responder notification protocols;
- Incident command hierarchy and instructions;
- Medical response and resources; and
- Coordination and response planning with other compound facilities (e.g., adjacent childcare facilities or other neighboring entities).

4.1.2.3 Physical Security Assessment

Maintaining a physically safe workplace is part of any good prevention program. Workplace violence should be a consideration when conducting facility security risk assessments to ensure appropriate security measures are employed. Agency planning groups should review security measures and procedures as well as make recommendations for modifications and improvements.

A physical security assessment, which is conducted by a law enforcement or security specialist, is a tool for establishing protection measures for Federal employees and visitors by pinpointing

high-risk areas in Federal buildings. The survey is a comprehensive, detailed, technical, onsite inspection and analysis of the current security and physical protection conditions.

If the agency does not have a current physical security assessment, the head of the agency may ask the agency's security office (if a non-FPS facility) or a regional FPS office to conduct a physical security survey in the effort to ensure that employees are working in a safe and secure environment.

4.1.2.4 Physical Security Measures

The following are some examples to improve office and/or building security:

- Post a security guard at the main building entrance or at entrances to specific offices;
- Install a metal detector or video surveillance system (VSS);
- Issue all employees photo identification cards;
- Assign temporary passes to visitors;
- Require contract guards to call Federal offices to confirm an appointment as necessary;
- Request an escort for all visitors (e.g., customers, relatives, friends);
- Brief employees on an action plan should a threatening or violent incident occur;
- Establish code words to alert coworkers and supervisors that immediate help is needed; and
- Install silent, concealed alarms at reception desks.

The following are some examples to improve security in the event of a threatening or violent individual:

- Ensure officers or guards have a clear view of the customer service area at all times;
- Arrange furniture and partitions so front-line employees are surrounded by a barrier;
- Provide an under-the-counter duress alarm system to signal a supervisor or security officer;
- Establish an area in the office for employees and/or customers to escape; and
- Provide an access-control combination lock on access doors.

Many Federal agencies have numerous security measures in place that can reduce the risk of workplace violence. These include but are not limited to:

- Appropriately displaying employee photo ID badges at all times;
- Onsite guard services and/or individually coded key cards for access to buildings and areas within buildings according to individual needs;
- Guard-enforced assistance in registering, badge issuing, and directing visitors in larger facilities;
- VSS;
- Silent alarms;

- Metal detectors;
- Two-way mirrors;
- Electronic access systems;
- Barriers to prevent cars from driving too close to the building;
- Emergency internal code words;
- Extra lighting in the parking lots; and
- Escorts (armed if available) to and from parking lots after dark.

Appendix A contains additional suggestions for preventive security measures. Appendix B contains resources for obtaining additional information on those measures.

4.1.3 Develop a Procedure for Employees to Report Incidents

The primary consideration in developing a reporting procedure in the context of a workplace violence prevention and response program is to make sure the procedure encourages employees to report all incidents, even minor ones. Employees should report to management when:

- They are the victims of violence;
- They believe they have been threatened with violence;
- They witness an act or threat of violence towards someone else; or
- They have reason to believe they may be victimized in the future, either at the workplace or as a result of employment with the agency.

Generally the agency's OEP or other emergency plan contains established reporting mechanisms. Planners should review those procedures to determine whether, for purposes of workplace violence incidents, any specialized procedures are appropriate. Credibility for any reporting system will depend upon whether reports are quickly, effectively, and confidentiality handled.

Before a reporting procedure is announced to employees, ensure the agency staff who will be responding to reported incidents are properly trained.

Another key element of the success of any reporting system is management team's encouragement for reporting incidents. Agency managers must create an environment that demonstrates they will always respond quickly and appropriately, both to reports of incidents and to employee concerns. This demonstrates to employees that management is willing and able to protect them from danger. It also reduces unnecessary anxiety among employees regarding their own welfare, and reduces the loss of productivity stemming from such anxiety.

The reporting procedure should be reviewed on a periodic basis to provide feedback for lessons learned.

4.1.3.1 Reporting

Accurate and early reporting provides for a well-timed intervention. This can be instrumental in resolving issues of workplace incivility and bullying before such issues escalate into physical violence. Developing and implementing reporting procedures for workplace bullying and incivility is just as important as establishing procedures for reporting physical violence.

If an employee believes they are the victim of bullying, verbal or electronic harassment/cyber-bullying, psychological violence, or emotional abuse, they should report the problem. These behaviors, if left unreported, can negatively impact the victim, the work environment, and employee productivity. The employee may wish to keep contemporaneous documentation to assist in remembering the details, dates, and frequency of the incidents.

Early reporting of perceived abuse allows management to quickly address and correct a problem before it becomes more severe. The level of the management chain where an employee reports this type of incident will depend on who is committing the non-physical violence. If a direct supervisor is the perpetrator, then the employee needs to move up one level on the management chain to report the violence.

Procedures for reporting workplace violence incidents vary according to the type and intensity of violence involved. Most Federal workplaces have a variety of reporting options. Depending on the nature of the situation, resources available in-house, and the need for security/law enforcement involvement, the report may go to one or more of the following:

- The employee's supervisor;
- In-house security;
- The threat assessment team;
- Appropriate law enforcement;
- The Department or Agency's insider threat program office; and/or
- The employee's union representative.

In addition to established reporting procedures, agencies should allow for employees who have safety or reprisal concerns to submit anonymous reports.

Regardless of the specific reporting procedures, maintaining a successful workplace violence prevention and response program requires agencies to investigate all reports and follow up with the appropriate actions where necessary. However, agencies should keep in mind that if there is no complainant, a law enforcement entity may feel there is no crime to investigate.

4.1.3.2 Field Worker Concerns

Circumstances related to field work present a different set of concerns for workplace violence incidents. Workers may encounter violence while conducting compliance inspections, home visits, customer service duties, and other field assignments. Special measures should be

implemented for workers assigned to field locations or who perform their duties outside a Federal facility so they can report incidents to their leadership.

Each field assignment involves its own set of risk factors for violence. It is essential employees on assignment in the field be trained and provided with assignment-specific safety guidelines. Techniques useful for increasing the safety of field assignments and working environments include but are not limited to:

- A communication system including a designated contact at the home office;
- A daily work plan, schedule, and predetermined phone call check-in times;
- A buddy system (e.g., a partner); and/or
- Law enforcement backup.

4.1.4 Develop Plans to Respond to Workplace Violence Incidents

Given the wide range of incidents and situations that can occur at the worksite, it can be difficult for agencies to specifically define the responsibilities of all offices potentially involved in responding to an incident. Agencies may find it useful to classify incidents in broad categories such as:

- Emergency/non-emergency;
- Domestic violence/threats/bullying/disruptive behavior; or
- Coworker/outsider.

Using these broad categories, agencies can determine the offices that would generally respond to each type of incident and what role each office would play in the response effort. Agencies can appropriately plan for both immediate responses and long-term responses.

The vast majority of violent incidents in the workplace arise from client-professional interactions. As such, some agencies belong to industry groups with predictable risks, such as health care, corrections, and education. Those agencies may require formal standing approaches to threat assessment and management. For example, the Veterans Health Administration (VHA) developed the Disruptive Behavior Committee and Patient Record Flagging process. These interdisciplinary committees are standing groups trained to assess incidents, evaluate the risk of recurrence, and provide guidance on prevention in the future. Training addresses clinical threat assessment and law enforcement issues.

Employee threat assessment teams function under a different set of rules, such as patient care delivery, in a clinical system and has different rules than human resources regulations under OPM. Corrections facilities have other obvious regulatory constraints and opportunities, and those influence fundamental strategies in threat assessment and management. Agencies must consider their administrative rules and processes in order to remain within the appropriate boundaries before such incidents occur. To facilitate developing a plan that works for a given agency, a series of case studies are provided in Appendix C of this guide.

Plans for a coordinated response to reported incidents must be kept flexible. Responsibility for overall coordination and direction is usually assigned to a specific office. The coordinator from that office must have the flexibility to use the plan as a guideline and not a mandatory set of procedures. More importantly, the coordinator must have the latitude to tailor the recommended response to the particular situation. It is important to recognize that threatening situations often require creative responses; thus, the importance of flexibility cannot be overemphasized.

The case studies in Appendix C highlight the need for backup plans in situations calling for an immediate response where the individual responsible for a certain aspect of the response effort is unavailable. Taking a team approach in responding to a potentially violent situation is an ideal way to provide backup coverage. A team approach ensures all staff in employee relations, EAP, security, and other offices are trained and prepared to work together with management to deal with potentially violent situations. This ensures coverage regardless of which staff member in each of the offices is on duty when an incident occurs.

Violent incidents are not always predictable; thus, violence cannot always be prevented. However, risk can be reduced by planning ahead and being prepared to act swiftly to deal with threats, intimidation, and other disruptive behavior at an early stage.

4.1.4.1 Workplace Violence Incident Response

The safety and security of all employees must be a top priority for any response personnel. It is important to understand that workplace violence incidents do not necessarily get reported via a phone call to security. The security response process must be flexible enough to handle any situation that manifests in the workplace, in whatever manner it is reported. While Federal agencies already have a variety of emergency response-oriented plans, the workplace violence response plan must also consider that the threat may arise internally rather than externally.

4.1.4.2 Communication

Prompt, accurate communication during a workplace violence incident or any other type of emergent event is essential. The communication section of the workplace violence prevention and response program should identify:

- How the agency will notify the affected employees and facility occupants, and
- Who will provide that notification.

This section of the plan must include provisions for communicating information to employees who have vision or hearing issues, as well as those for whom English is not their primary language.

4.1.4.3 Supportive Resources and Care

Immediately after a violent incident, the main priority is to provide a safe and secure environment and necessary medical attention by first responders. These designated personnel will secure the scene and assess the possibility of any continued threat. It is important to account for all building occupants.

Victims, intended victims, bystanders, and coworkers may experience both short-term and long-term psychological distress as the result of a workplace violence incident. Exposure to traumatic events often leads to a range of strong emotional and physical responses, so it is important to engage and use available resources to evaluate at-risk individuals who may be in need of treatment. Agencies will likely have a variety of options for evaluating and providing support for those who may be affected. Some of those options may include:

- EAPs;
- Private practice mental health services;
- Community mental health resources;
- Educational sessions on stress responses, coping, and available services;
- Facilitating existing support networks; and
- Providing opportunities for private, individual discussions.

EAP staff members generally assist in policy and strategy development and help determine the EAP's role on the agency's workplace violence incident response team. EAPs bring a special expertise to the planning process. They are in an optimal position to assist with many of the activities conducted by the agency planning group.

4.1.4.4 Facility Response

A threat of workplace violence, whether external or internal, may result in the need to evacuate the facility, shelter in place, or initiate lockdown. The facility's OEP should address what action is appropriate for the situation.

- If **evacuation** of the facility is necessary, then following the emergency evacuation plan procedures will result in a prompt and orderly evacuation of occupants.
- In an instance where the threatening situation is occurring from the exterior or perimeter of the facility, **sheltering in place** may be the safest course of action. The shelter-in-place location should be a predesignated internal location chosen to protect individuals when conditions outside the facility are more dangerous than inside, or when outside conditions are unknown.

- Some types of workplace violence events may result in a **lockdown** mode being ordered. During a lockdown, employees will be told to stay in their current locations, lock doors and other access points, and refrain from moving to other locations within the facility until the threat has been mitigated.

To ensure employees are prepared for potential evacuation, the agency should distribute to each employee the facility's OEP outlining procedures to follow in the event of fire, bomb threats, civil disturbances, threats of violence both inside and outside the office, natural disasters, etc.

4.2 Prevention

Prevention is a major component of any workplace violence prevention and response program. This section will focus on providing general ideas and considerations that can help agency planning groups gain a greater understanding of the additional measures that can be taken to reduce the risk of violent behavior, including a greater understanding of the law enforcement and security issues that may affect them.

4.2.1 Warning Signs of Violence

The first question many people ask when starting to develop a workplace violence prevention and response program is: How can we identify potentially violent individuals? “Early warning signs” and “profiles” of a potentially violent employee are mentioned in much of the literature on the subject of workplace violence. It would save time and solve problems if supervisors could recognize ahead of time what behaviors and personality traits are predictive of future violent actions.

It is difficult to predict violent behavior. The below indicators were identified by the FBI National Center for the Analysis of Violent Crime, Profiling and Behavioral Assessment Unit in its analysis of past incidents of workplace violence:⁸

- Direct or veiled threats of harm;
- Intimidating, belligerent, harassing, bullying, or other inappropriate/aggressive behavior;
- Numerous conflicts with supervisors and other employees;
- Blatant or intentional disregard for others;
- Disruptive, aggressive, or angry language;
- Wrongfully damaging or destroying property;
- Extreme changes in behavior;
- Statements showing fascination with incidents of workplace violence, approval of the use of violence to resolve a problem, or identification with perpetrators of workplace homicides;

⁸ Main FBI website <https://www.fbi.gov/services/cirg#Investigative-%20Operations%20Support>. Workplace violence resources: www.fbi.gov/stats-services/publications/workplace-violence. Accessed March 29, 2013.

- Bringing a weapon to the workplace, brandishing a weapon in the workplace, making inappropriate references to guns, or showing a fascination with weapons;
- Delusional statements or paranoid ideas;
- Statements indicating desperation (over family, financial, or other personal problems) to the point of contemplating suicide;
- Drug or alcohol abuse; and
- Pending or recent layoffs.

Each of these behaviors is a clear sign that something is wrong. None of these signs should be ignored. By identifying the problem and dealing with it appropriately, supervisors may be able to prevent violence from happening.

One cannot tally the factors, arrive at a “score,” and then render from that score a probability that violence will occur. Because each violence risk factor is embedded in a unique context, any given factor may contribute to the risk formulation to varying degrees. The subject who exhibits only one of the factors listed may in fact pose an extreme risk of violence if that one factor is something like “brandishing a weapon in the hospital workplace while staring intently at her doctor.”

A thorough threat assessment will also consider any “good news” in relation to the subject; i.e., mitigating factors against the risk of violence. For example, a disruptive employee with a strong desire and commitment to complete their Federal career and retire may present less actual risk of further violence than another employee who has no expectation of reaching retirement. A subject with strong family connections and no wish to disappoint others similarly may pose less of a risk. Sometimes strong religious conviction will mitigate violence. These and other possible mitigating factors should be evaluated as part of a complete threat assessment while maintaining the subject’s privacy.

Agency planning groups should ensure the appropriate staff member (or an incident response team) is prepared to assist supervisors and other employees in dealing with incidents of violence and bullying in the workplace. Some behaviors require immediate law enforcement or security involvement, others constitute actionable misconduct and require disciplinary action, and others indicate an immediate need for an EAP referral.

On the other hand, it is seldom (if ever) advisable to rely on what are inappropriately referred to as “profiles” or “early warning signs” to predict violent behavior. Profiles often suggest people with certain characteristics, such as loners and men in their forties, are potentially violent. This kind of categorization will not help predict violence, and it can lead to unfair and destructive stereotyping. The same can be said of reliance on early warning signs that include descriptions of problem situations such as someone who is in therapy, had a death in the family, suffers from mental illness, or is facing a reduction in force. Everyone experiences stress, loss, or illness at some point in life. All but a very few people weather these storms without resorting to violence. Supervisors should, of course, be trained to deal with the kinds of difficulties mentioned here,

such as bereavement or mental illness. However, this training should focus on supporting the employee in the workplace, and not in the context of, or the potential for, workplace violence.

When an analysis of indicators for increased risk of violence is paired with a review of risk mitigating factors, the threat assessment team should be alert to the situation in which the subject appears to have nothing to lose. For those individuals, the fear of disciplinary action or even dismissal or incarceration is no longer a deterrent.

4.2.2 Pre-Employment Screening

Pre-employment screening is an important part of workplace violence prevention. Prior to hiring an employee, the agency should check with its personnel and legal departments, if necessary, to determine what pre-employment screening techniques (such as interview questions, background and reference checks, and drug testing) are appropriate for the position under consideration and consistent with Federal laws and regulations. EO 10450 and Homeland Security Presidential Directive 12 (HSPD-12) require a background investigation for Federal employees, contractors, and affiliates.

4.2.2.1 Hiring Process

Because individuals who exhibit violent or bullying behavior usually have a history of such actions, a thorough hiring process can serve as one important step in helping prevent violence in the workplace. Agencies should make use of three vital tools during the hiring process:

1. A face-to-face interview with the applicant;
2. An assertive check of work references; and
3. Use of a probationary period for new employees.

Face-to-Face Interview

A face-to-face interview can provide some sense of how the applicant interacts with people, responds to problems and unfamiliar environments, and handles other workplace challenges. However, since an interview is only a snapshot of behavior, some applicants may be able to deceive even a seasoned hiring manager and conceal possible future performance issues behind a well-rehearsed, seemingly professional appearance.

Assertive Check of Work References

If the applicant is suitable based on the interview, the hiring authority should perform a thorough, comprehensive check of past references and other background information. Previous employers, supervisors, colleagues, and subordinates can often provide valuable insight into the applicant's personality and behavior; past performance is often an accurate predictor of future success.

As a precaution, employers must be alert because the reference list is usually provided by the applicant, who is not likely to list persons who will provide unfavorable reports. In addition, most bullying behavior is covert and typically is not reported officially, so the previous employer/supervisor may not be aware of such behavior.

An additional consideration is that many previous employers will only provide an acknowledgement of employment. Therefore, a complete check of the applicant's work history, including their military service, and a check of any possible criminal record, should also impact the hiring decision.

Use of a Probationary Period

If, after the interview and reference check, the decision is made to move forward and hire the individual, proper use of a probationary period is in the best interest of both the new employee and the Federal employer. A probationary period allows time for the employee, supervisor, and other staff members to determine whether the employee can perform the job. The U.S. Merit Systems Protection Board's (MSPB's) August 2005 report, *The Probationary Period: A Critical Assessment Opportunity*, provides additional information.⁹

4.2.2.2 Challenges to the Hiring Process

The processes of interviewing the applicant, checking references, and assessing adequacies during the probationary period are standard management procedures. However, on occasion, one or more of the steps is omitted or not thoroughly completed, thereby increasing the possibility of allowing a potentially violent applicant into the workplace. Various factors can tempt managers to circumvent or omit one or more steps in the hiring process.

Among these factors:

- Vacant positions can create hardship for organizations, causing missed deadlines, increasing the workload on the existing employees, and increasing the difficulty of accommodating leave requests.
- Managers may rely on their "intuitive ability" to spot the "real person" under the polite façade and choose to base their hiring decision on an interview alone.
- The legalities surrounding background checks and interviews may intimidate some managers into avoiding both processes. EO 10450 and HSPD-12 require a background investigation for employees, contractors, and affiliates.

⁹ MSPB, *The Probationary Period: A Critical Assessment Opportunity*, August 2005. Available online: <https://www.mspb.gov/netsearch/viewdocs.aspx?docnumber=224555&version=224774>

- Those checking references may not be experienced at assertively probing in the questioning of former employers, superiors, colleagues, and subordinates.

4.2.2.3 Resources and Support

Senior management should be made aware of the challenges their hiring personnel face during the hiring process. Managers also need to use the resources available to them in departments such as human resources, Equal Employment Opportunity, and general counsel. Professionals from these departments can advise managers on how to conduct a thorough and legal evaluation of the applicant. Guidance from these subject matter experts can reduce managers' liability and help them navigate the hiring process thoroughly and efficiently.

4.2.3 Training

Training for all agency personnel is an important part of any workplace violence prevention and response program. The training may differ based upon the target audience and type of employee groups. At a minimum, agencies should provide initial and recurring training on the following topics to all current employees, newly hired employees, supervisors, and managers:

- An overview of the various aspects and types of bullying and violence in the workplace;
- Symptoms and behaviors often associated with those who commit aggressive or violent actions;
- Security hazards found in the agency's workplace;
- The Department or Agency's workplace violence prevention policies and procedures;
- Reporting requirements and processes;
- Specialized training on how to create a positive work environment and develop effective teams;
- Escalation of subtle behaviors that could lead to violence;
- Training to improve awareness of cultural differences (e.g., diversity);
- Tips for protecting oneself and fellow coworkers;
- Response plans, communication, and alarm procedures;
- Supervisory training in how to conduct a peaceful separation from service; and
- Active Shooter Response Training – Run, Hide, Fight.

One example of a training program is the VHA's Prevention and Management of Disruptive Behavior (PMDB) employee education program. PMDB uses a tiered approach to training that maps onto the results of a comprehensive workplace violence risk assessment and is generally well-received by the VHA's individual facilities. Such an approach allows the VHA's individual medical centers to tailor their training programs to address the unique needs of their own diverse workforce.

PMDB is organized into four levels of training:

- **Level I: Violence Prevention Awareness Training.** Online, web-based training (1.5 hours). Appropriate as a curriculum element in new employee orientation training.
- **Level II: Observational and Verbal De-escalation Skills.** Face-to-face training (four hours). Appropriate for an employee assessed to be at low risk for workplace violence and/or for an employee whose job duties require excellence in customer service interactions.
- **Level III: Personal Safety Skills.** Face-to-face training (four hours). Appropriate for an employee who would benefit from having knowledge of basic self-protection and physical attack evasion and escape techniques. The combination of Level II and Level III training is appropriate for an employee assessed to be at moderate risk for workplace violence.
- **Level IV: Therapeutic Containment Skills.** Face-to-face training (four hours). Appropriate for an employee who may need to contain physically disruptive individuals in order to protect themselves and others from serious injury. The combination of Levels II, III, and IV training is appropriate for an employee assessed to be at high risk for workplace violence.

Levels I, II, and III of the PMDB program may be adapted for use in any Federal agency. Level IV might be appropriate for an employee of any Federal agency who at times may have to safely physically constrain patients, inmates, or customers without intentionally using the infliction of pain to effect containment.

It is important to communicate management's commitment at all levels during the training. The presence of senior management at training sessions will increase the visibility and credibility of the organization's top-level commitment to preventing workplace violence.

Training should also be provided to an affected employee whenever management is made aware of a new or previously unrecognized hazard and to an employee given a new job assignment for which specific workplace security training for that job assignment has not previously been provided.

Training sessions conducted by the agency's EAP, security, and employee relations staffs are particularly helpful, enabling an employee to get to know experts within the agency who can help them when potentially violent situations arise. Employees and supervisors seek assistance at a much earlier stage when they personally know the agency officials who can help.

Providing appropriate training indicates to employees that management will take threats seriously, encourages employees to report incidents, and demonstrates management's commitment to deal with reported incidents. The following sections include types of training that have proven effective in preventing violence and other threatening behavior.

4.2.3.1 Employee Training

All employees should know how to identify and report incidents of violent, intimidating, threatening, and other disruptive behavior. All employees should also be provided with phone numbers for quick reference during a crisis or an emergency.

In addition, workplace violence prevention training for employees should follow a specific curriculum and lesson plan and may include topics such as:

- Explanation of the agency's workplace violence policy or program;
- Encouragement to report incidents;
- Ways of preventing or diffusing volatile situations or aggressive behavior;
- How to deal with hostile persons;
- How to identify and respond to behavior brought about by medical conditions, such as the onset of diabetic coma or the abuse of drugs;
- Managing anger;
- Techniques and skills to resolve conflicts;
- Stress management, relaxation techniques, and wellness training;
- Security procedures (e.g., the location and operation of safety devices such as alarm systems);
- Personal security measures; and
- Programs operating within the agency that can assist employees in resolving conflicts (e.g., EAPs, the Ombudsman, mediation).

The following programs are examples of training offered by various Federal Departments and Agencies:

- OSHA recommends that employees in health care and social services organizations should receive formal instruction on the specific safety and security hazards associated with their particular job or facility. Detailed information is available in OSHA's *Guidelines for Preventing Workplace Violence for Health Care and Social Service Workers*.¹⁰
- NIOSH also discusses the importance of training tailored to the specific risks in the employee's workplace. NIOSH's *Violence in the Workplace*, Current Intelligence Bulletin 57, *Risk Factors and Prevention Strategies*¹¹ discusses clearly identifiable workplace risk factors, such as dealing with the public, and emphasizes that training will

¹⁰ OSHA, *Guidelines for Preventing Workplace Violence for Health Care and Social Service Workers*, 2016. Available online: <https://www.osha.gov/Publications/osh3148.pdf>

¹¹ NIOSH, *Violence in the Workplace*, Current Intelligence Bulletin 57, *Risk Factors and Prevention Strategies*, July 1996. Available online: <https://www.cdc.gov/niosh/docs/96-100/risk.html>

be more useful and credible when it addresses risk factors specific to job tasks or locations.

- DHS initiated a training program called the Physical Security Outreach Program that addresses crime prevention as well as workplace violence awareness training. In addition, the Federal Emergency Management Agency (FEMA) hosts an online course titled *IS-906 Workplace Security Awareness Training*.¹²

Your agency's training program, including a plan for emergency evacuation, should be designed and practiced. The evacuation plan should include not only procedures for getting workers out of a facility, but some method for those evacuated to assemble or check in to determine who is safe and who may still be missing. Evacuation plans should include provisions for employees with disabilities and other issues: for example, ensuring employees with hearing issues receive warnings and a system for safely evacuating anyone who uses a wheelchair.

The amount and frequency of retraining and response drills (reinforcing skills competency) is a determination also driven by the needs of employees based upon the results of the workplace violence risk assessment. At a minimum, skill competency assessments are recommended at least once every two years and face-to-face retraining every four years. Individual work groups often request training at more frequent intervals (e.g., annually) and such requests should be enthusiastically honored.

4.2.3.2 Supervisor Training

In addition to the training suggested above, special attention should be paid to general supervisor training. The same approaches that create a healthy, productive workplace can also help prevent potentially violent situations. It is important that supervisor training include basic leadership skills including but not limited to:

- Setting clear standards;
- Addressing employee problems promptly;
- Conscientiously using the probationary period;
- Performance counseling;
- Discipline; and
- Other management tools.

These interventions can keep difficult situations from turning into major problems. Supervisors do not need to be experts on violent behavior, but they do need to be willing and knowledgeable about seeking advice from experts.

Some agencies include training on workplace violence as part of general supervisor training, while others conduct separate training sessions on workplace violence. Some agencies even

¹² <https://training.fema.gov/is/courseoverview.aspx?code=IS-906>

include it in crisis management training. Regardless of the approach taken, supervisor training should cover:

- Ways to encourage employees to report incidents that made them feel threatened for any reason by anyone inside or outside the organization;
- Skills in behaving compassionately and supportively towards employees who report incidents;
- Skills in taking disciplinary actions;
- Basic skills in handling crisis situations;
- Basic emergency procedures;
- How to ensure that appropriate screening of pre-employment reference is completed;
- Bullying; and
- Confidentiality procedure awareness.

Training sessions conducted by the agency's EAP, security, and employee relations staffs are particularly helpful, enabling employees to get to know experts within the agency who can help when potentially violent situations arise.

4.2.3.3 Incident Response Team Training

The members of the incident response team need to be competent in their own professions; they also need to know when to call for outside resources. Participating in programs and training sessions sponsored by government and professional organizations, reading professional journals and other literature, and networking with others in the profession are all helpful in gaining knowledge about dealing with workplace violence situations.

Team members also need to understand enough about each other's roles to allow them to work together effectively. Response team training should allow discussion of policies, legal constraints, technical vocabulary, and other considerations that each profession brings to the interdisciplinary group.

Much of the incident response team training can be accomplished by practicing responses to different scenarios of workplace violence. The case studies in Appendix C of this guide are intended for this purpose. Practice exercises help Department and Agency personnel understand each other's responses to various situations to eliminate confusion or misunderstanding during an actual incident. In addition, practice exercises prepare the staff to conduct the supervisory training suggested above.

Tailoring the appropriate response training to the specific source of violence represents a critical consideration that affects both the composition of and the rules that may govern the response. For example, patients who threaten or attack providers still have a provider-patient relationship: laws, regulations, and other patient care practice topics will influence both composition and response framework. Corrections and educational institutions have their own set of processes.

Threats by coworkers involve administrative operations, underlie OPM regulations and Federal administration laws, and in most settings are driven by administrative oversight.

The team members also need to consult regularly with other personnel within the organization who may be involved in dealing with potentially violent situations. Those who are consulted on an ad hoc basis should receive some level of training as well.

4.2.4 Using Alternative Dispute Resolution as a Preventive Strategy

Some agencies use ombudsman programs, facilitation, mediation, and other methods of alternative dispute resolution (ADR) as preventive strategies in their workplace violence programs. ADR approaches often involve a neutral third party who can assist disputing parties in resolving disagreements. ADR is most helpful in workplace violence prevention and response programs at the point when a problem first surfaces: i.e., before an employee's conduct rises to a level that warrants disciplinary action. The following is a short description of some ADR techniques agencies found useful in dealing with potential workplace violence problems at the very earliest stages.

4.2.4.1 Ombudsmen

Ombudsmen are individuals who rely on a number of techniques to resolve workplace disputes. These techniques include counseling, mediating, conciliating, and fact-finding. Usually, when an Ombudsman receives a complaint, they interview the parties, reviews available information and policies, and offers options to the disputants. Ombudsmen do not typically impose solutions. The effectiveness of the ombudsman lies in their problem-solving ability. Generally, an individual not accepting an option offered by the ombudsman is free to pursue a remedy using another forum for dispute resolution.

4.2.4.2 Facilitation

Facilitation techniques improve the flow of information in a meeting between parties to a dispute. The term "facilitator" is often used interchangeably with the term "mediator," but a facilitator does not typically become as involved in the substantive issues as a mediator does. The facilitator focuses more on the process involved in resolving a matter. Facilitation is most appropriate when the intensity of the parties' emotions about the issues in dispute are low to moderate, the parties or issues are not extremely polarized, or the parties have enough trust in each other that they can work together to develop a mutually acceptable solution.

4.2.4.3 Mediation

Mediation uses an impartial and neutral third party who has no decision-making authority. The objective of this intervention is to assist the parties in voluntarily reaching an acceptable resolution of issues in dispute. Mediation is useful in highly polarized disputes where the parties

are either unable to initiate a productive dialogue or in cases where the parties have been talking and have reached a seemingly insurmountable impasse.

A mediator, like a facilitator, makes primarily procedural suggestions regarding how parties can reach agreement. A mediator may occasionally suggest some substantive options as a means of encouraging the parties to expand the range of possible resolutions under consideration. A mediator often works with the parties individually to explore acceptable resolution options or to develop proposals that might move the parties closer to resolution.

4.2.4.4 Interest-Based Problem Solving

Interest-based problem solving is a technique that creates effective solutions while improving the relationship between the parties. The process separates the person from the problem, explores all interests to define issues clearly, brainstorms possibilities and opportunities, and uses a mutually agreed upon standard to reach a solution. It is often used in collective bargaining between labor and management in place of traditional, position-based bargaining. However, as a technique, it can be effectively applied in many contexts where two or more parties are seeking to reach agreement.

4.2.4.5 Peer Review

Peer Review is a problem-solving process whereby an employee takes a dispute to a panel of fellow employees and managers for a decision. The decision may or may not be binding on the employee and/or the employer, depending on the conditions of the particular process. If the decision is not binding on the employee, they would be able to seek relief in traditional forums for dispute resolution if dissatisfied with the decision under peer review. The principal objective of the method is to resolve disputes early before they become formal complaints or grievances.

4.2.4.6 Termination of Employment

Terminating an employee may be an appropriate response to a particular situation, but doing so in the heat of the moment without any time for evaluation or preparation may be precisely the wrong thing to do. Any removal or employment termination process must follow all established agency procedures. The manager should strive to maintain an atmosphere of dignity and respect and should use all available resources including professional assistance in assessing the potential physical and psychological consequences.

If the removal is due to downsizing, restructuring, or some other business issue, managers should not increase the employee's distress by treating them as potentially dangerous. Instead, the manager should treat the employee with respect, be supportive of the employee's job search, and ensure the employee is aware of the available resources such as placement services, job search training, and career counseling. In the rare instance when someone could become violent, properly trained coworkers are likely to notice behavioral changes signaling the need for more focused attention and development of safe termination strategies.

If the removal is “for cause,” particularly if it is due to bullying or violent behavior, other forms of misconduct, or illegal actions, there may be potential for violence. Training supervisors to recognize the warning signs and make use of available resources can help them defuse the potential for workplace violence. While most EAPs provide services to current employees, allowing recently terminated employees to access the program may be beneficial.

4.2.5 Computer Security

Agency planning groups should address ways to safeguard computer systems. There are cases where employees sabotaged computer equipment, computer systems, and computer records. Therefore, whenever a threat of sabotage is suspected, procedures should be initiated to prevent the person from having access to the facility’s computer system.

It is important to act quickly whenever there is reason to believe an employee or former employee may commit such an act. It is standard practice to collect identification cards, building passes, keys, parking passes and revoke Personal Identity Verification (PIV) certificates when employees leave their jobs; however, blocking access to computer systems or networks is sometimes overlooked.

4.2.5.1 Revocation of Access after Termination

A termination occurs when an individual departs their organization and ends their association with the agency. A termination may be considered voluntary or involuntary. In either case, the individual must be denied access to all resources in a timely manner.

When an individual terminates or transfers, many people are responsible for ensuring the individual’s access privileges are updated. Initial responsibility lies with the individual’s supervisor and the Information System Security Manager (ISSM) or Information Security System Officer (ISSO) of each information technology (IT) resource, and the insider threat program representative, to which the individual has access.

When terminating employees, some agencies bar the individual from the premises and eradicate their passwords to computer systems that are accessible from outside the premises. When crafting the response plan, the agency planning group should communicate with the information security officer or computer system administrators to ensure the former employee is locked out of the agency’s systems.¹³

Identifying all the accesses an individual has is sometimes difficult; often, this information is not readily available in one central place. For example, information technology administrators may know who has access to various computer systems, and the facilities manager may know who has access to the computer systems that control the building's heating, air-conditioning, and other support functions for the facility. The agency planning group, as part of the response plan, should talk to the information/computer security officer or computer system administrators to determine

¹³ https://www.fbiic.gov/public/2008/jan/OEP/OEP_Guide_Supplement_1_situations.pdf

the vulnerability of the computer networks and the procedures that need to be implemented to lock individuals out of these systems.

4.3 Conclusion to Planning, Prevention, and Response

This document provides information related to the establishment of practical workplace violence prevention and response and facility preparedness programs within the Federal government framework. Recognizing that each government facility is unique in its physical environment, the goal of this document is to assist Federal agencies in developing and implementing agency-specific workplace violence prevention and response programs. Agency leaders will be able to use this document and the reference documents to create sustainable programs. A sample of a checklist for creating a workplace violence prevention and response program, as well as a workplace violence prevention and response program framework, are located in Appendix B.

In addition to the resources found in Appendix B, additional information on indicators of potential violence can be found here: <https://emilms.fema.gov/is907/groups/39.html>

5.0 Administrative Inquiries and the Assessment Process

The information in this chapter provides guidance for the agency planning group that may be comprised of members of an agency’s human resources, EAP, legal, and security offices as well as representatives of the agency’s FSC, union(s) (if present) and senior management, among others. The information contained here is not technical, not for professional investigators, and not a summary of fact-finding or investigating procedures. Rather, it is intended to provide the agency planning group with a general overview of fact-finding considerations, administrative inquiries, and assessment.

5.1 Fact Finding

“I can’t work here anymore. I’m afraid he may actually kill one of us.”

The supervisor hears the details of the incident causing the employee to feel threatened. Now the supervisor has to do something. The incident cannot be ignored. It must be reported. Once reported, the members of the incident response team (along with the supervisor) must look into it.

5.1.1 Incident Intake and Inquiry

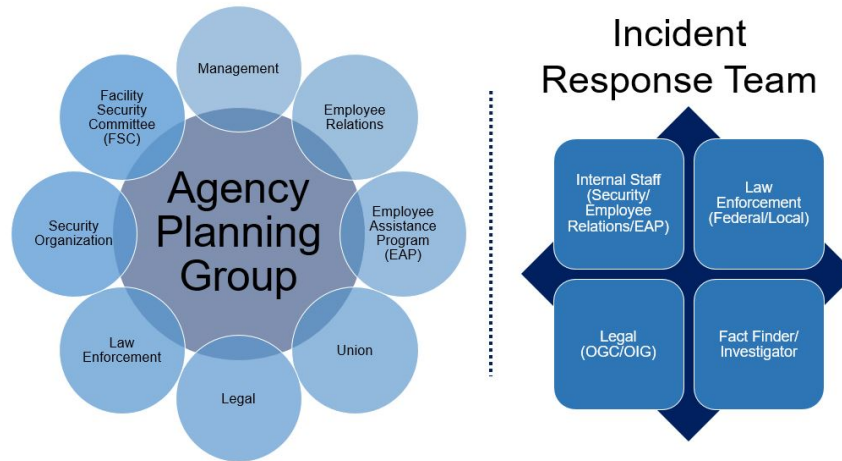
Often an incident intake and inquiry will be conducted by either trained internal staff and/or outside law enforcement at the time as part of any post-incident intervention. The process can be particularly disturbing for employees who are personally involved in, witnessed, or knew coworkers involved in the workplace violence event. It is important that the administrative inquiry and assessment process be conducted in a professional and sensitive manner. The information gathered during an incident inquiry is invaluable in the effort to assess the risk potential of a reported safety concern.

As the agency begins its incident fact finding, it is important to ensure that actions taken by the agency during the fact finding do not impede potential criminal prosecutions.

The incident response team representatives should:

- Visit the scene of the incident as soon as possible;
- Treat respectfully any evidence that needs to be preserved until the scene is cleared;
- Interview injured and threatened employees and witnesses;
- Remind witnesses who are being interviewed that the goal is to prevent future incidents;
- Inform witnesses of their rights;
- Inform witnesses that they can refuse to answer questions and can stop the interview at any time;

- Examine the workplace for security risk factors associated with the incident, including any reports of inappropriate behavior by the perpetrator;
- Determine the cause of the incident;
- Take mitigating action to prevent the incident from recurring;
- Record the findings and mitigating actions taken; and
- Refer findings to the appropriate offices, including Workplace Violence Prevention, Insider Threat, and Personnel Security.



5.1.2 Understanding the Situation

As in all other serious administrative matters that come to the agency’s attention, there is a need to learn more about what is going on in this situation. Additional information includes:

- **What** happened;
- **Who** was involved;
- **Where** did it happen;
- **When** did it happen;
- **Why** did it happen; and
- **How** did it happen?

5.1.3 Consider Immediate Security Needs

Sometimes taking a few minutes for a cursory overview will give enough information to know what to do next. Of course, if there is imminent danger, law enforcement must be notified immediately. If there is no imminent danger, deciding what to do next will depend on agency procedures and the strategy/relationship developed ahead of time within the agency’s OGC, OIG, and the law enforcement organization that has jurisdiction over the work site. In most Federal agencies, these offices are notified immediately when certain types of reports are made, and they advise team members (or agency officials) on how to proceed with the investigation of the case.

Note that the fact-finding team may need to consider chain of custody if an incident turns into a criminal matter. If the team believes an incident could become a criminal manner, the team should consult with law enforcement to determine the appropriate course of action so as to not break the chain of custody.

5.2 Types of Investigations and Inquiries

Often, one of the first decisions to be made is whether to conduct an administrative inquiry or a criminal investigation. The answer will depend on whether the facts as presented indicate possible criminal behavior. Since arriving at a decision generally involves discussions with law enforcement personnel, OGC, OIG, and employee relations representative, it is imperative to coordinate efforts fully with these offices ahead of time. As discussed below, an important point of these discussions is to ensure actions taken by an agency during administrative inquiries do not impede potential criminal prosecutions.

5.2.1 Administrative Inquiries

The following sections discuss administrative inquiries.

5.2.1.1 Use a Trained and Appointed Fact Finder

If the decision is made to conduct an administrative inquiry, it is important to use a qualified and experienced professional workplace violence fact finder or investigator. The agency planning group should identify one or more personnel for inquiries before the need arises. The agency must identify its own agency assessment team and train them in observation skills and enhanced cognitive interview techniques, such as asking direct and non-direct questions, non-confrontational approaches, and questioning and listening techniques.

Additional considerations for the agency planning group, such as having well-defined agency policies on handling inquiries, are discussed at the end of this section.

Places to look within the agency might be employee relations, the Insider Threat Program Office, and security. In some agencies, these offices have their own fact finders or investigators; in others, they contract with private investigators or leverage the services of trained staff or investigators from other Federal agencies. In any case, they should be able to help locate trained, qualified fact finders ahead of time.

It is important to use a fact finder who conducts the inquiry in a fair and objective manner. The inquiry should be conducive to developing truthful responses to issues that may surface. The inquiry must be conducted with full appreciation for the legal considerations that protect individual privacy. It is imperative to maintain an atmosphere of candor and propriety.

5.2.1.2 Ensure Criminal Prosecutions are Not Compromised

Criminal prosecutions must not be compromised by actions taken during administrative inquiries. It is necessary to ensure the fact finder, management, and all members of an incident response team understand actions taken during an administrative inquiry may compromise potential criminal prosecutions. If the agency obtains statements from the subject of the inquiry in the wrong way, the statements can impede or even destroy law enforcement's ability to criminally prosecute the case. On the other hand, if handled correctly, statements made in administrative inquiries could prove vital in subsequent criminal proceedings.

Therefore, in a case where a decision is made to conduct an administrative inquiry and there is potential criminal liability, it is good practice to give the subject of the inquiry what are usually called non-custodial warnings and assurances. The person is given the option of participating in the interview after being warned that any statements they make may be used against them in criminal proceedings. The option not to participate in the interview is exercised by the person's invocation of their Fifth Amendment right against self-incrimination. It should be noted that, since the person is not legally in custody, they are not entitled to an attorney.

If the fact finder decides to compel the subject of an inquiry to participate in an interview instead of being given an option to participate, then the fact finder should give the Kalkines warning. This means the person is told: (1) they are subject to discharge for not answering; and (2) statements they make (and the information gained as a result of these statements) cannot be used against them in criminal proceedings. Even if a fact finder does not actually give the Kalkines warning, if they compel the subject to give a statement, the information in the statement (and the information gained as a result of the statement) cannot be used in criminal proceedings. Therefore, it may be advisable to only use this approach if there is a great degree of certainty the person being questioned will not be subject to criminal proceedings.¹⁴

Since this may make criminal prosecution impossible, a fact finder should never give the Kalkines warning or compel statements from the subject of an investigation without the permission of the appropriate U.S. Attorney's or prosecutor's office. Such permission is usually obtained by the agency's OGC or OIG. Since this is an extremely complicated consideration, be sure to work closely with your OGC, OIG, and law enforcement organization. In potentially violent situations, it is often difficult to determine whether the misconduct is a criminal offense. If there is the slightest doubt, it is advisable to refer to one of the aforementioned offices for further guidance.

5.2.1.3 Guidance for Information Gathering and Interviewing

A thorough and professional administrative inquiry is the result of significant preparation and quality procedures. Personally obtaining information from individuals will constitute a significant part of any inquiry. An awareness of the skills and techniques necessary for effective

¹⁴ Derived from *Kalkines v United States*, 473 F. 2d 1391 (Ct. Cl. 1973).

interviewing is required. Incident response teams, particularly those members whose role is to conduct interviews, should be trained in observation skills and enhanced cognitive interview techniques, such as asking direct/non-direct questions, non-confrontational approaches, and questioning and listening techniques. In preparing for and conducting inquiries, experienced professional administrative investigators found the approaches in the following subsections to be effective.

5.2.1.4 Reviewing Available Information

The fact finder, after thoroughly reviewing the information that gave rise to the inquiry, should be ready to begin the fact finding process. Discrepancies or deficiencies in the information should be noted so they can be addressed during the interviews.

5.2.1.5 Selecting an Interview Site

Since the fact finder is conducting an official inquiry, they should conduct as many interviews as possible in an official environment, i.e., in government work space (instead of restaurants, cars, or private homes). Privacy is the most important consideration in selection of an interview site. The fact finder should guarantee the room will be available for the entire interview, so there is no disruption of the interview once it begins. The interview room should be comfortably furnished with as few distractions as possible.

5.2.1.6 Scheduling the Interview

Depending on the circumstances of the situation, the fact finder may or may not want to contact the individual in advance. In either event, the fact finder should advise the individual of the general nature and purpose of the interview. If the individual declines the interview, the fact finder should attempt to dissuade the individual and, if unsuccessful, ascertain and record the reasons for the declination. If the individual fails to appear more than once for the interview, the fact finder should follow whatever policy has been decided upon by the agency ahead of time.

5.2.1.7 Allowing the Presence of Additional Persons

There may be instances when the fact finder or the individual being interviewed wishes to have an additional person present (for cases involving bargaining unit employees, see the discussion in the next section). Fact finders sometimes prefer to have an agency representative present when interviewing the subject of the inquiry. In any event, the fact finder should follow whatever policy has been decided upon by the agency ahead of time.

5.2.1.8 Adhering to the Law Regarding Bargaining Unit Employees

The provisions of law set forth in 5 USC §7114(a) (2) (B), commonly known as Weingarten rights, covers any examination of a bargaining unit employee by a representative of the agency in

connection with an inquiry.¹⁵ Since interpretation of this law is very complex, consult with your labor relations specialists or OGC when faced with such situations.

Note: As of the publication of this document, the law is currently unsettled as to whether inspector general investigations are subject to 5 USC §7114(a) (2) (B). If a bargaining unit employee reasonably believes an inquiry may result in disciplinary action and requests union representation, the agency has three options:

- Immediately terminate the interview;
- Continue the interview with the employee's representative present; or
- Give the employee the option of proceeding with the interview without a representative.

5.2.1.9 Taking Notes

Since watching an interviewer take notes can be intimidating to some people, it is important to establish rapport before beginning to take notes. The interviewer should concentrate on observing the individual during the interview. Notetaking should not unduly interfere with observation. Notetaking materials should be positioned inconspicuously and should not become a focus of attention. The interviewer should learn and exercise the skill of taking adequate notes while still observing the individual and without distracting the person being interviewed. Preferably, an interview should always be conducted by two individuals for the purposes of taking notes, corroboration of the statements given, and to ensure a third party is present to validate/invalidate claims if the subject accuses the interviewer of misconduct or prejudice during the interview.

Should notetaking have a materially adverse effect on the interview process, the interviewer may explain the purpose of notetaking. The notes are intended for the interviewer's use in preparing a report and are not a verbatim transcript of the interview. The interviewer can modify or cease notetaking so long as the information can be recorded in adequate detail after the interview.

5.2.1.10 Maintaining Control of the Interview

Questions developed ahead of time can be memorized, but they should never be read verbatim from a list or recited in a perfunctory manner. The interviewer should know in advance the topics of concern to be covered. The interviewer should maintain a singleness of purpose during the interview and resist any efforts to shorten the interview or drift from topics of concern.

5.2.1.11 Developing Rapport

The interviewer should have a comfortable style that projects professionalism and competence. Their style should generate rapport with the person being interviewed. An open approach that conveys a willingness to communicate generally fosters rapport. Rapport is evident when the

¹⁵ See *National Labor Relations Board v. Weingarten, Inc.*, 420 US 251 (1975)

individual appears comfortable with the investigator and is willing to confide personally sensitive information. Continuing rapport can often be maintained if the investigator does not become judgmental when disagreeable conduct or information is disclosed. The interviewer who can project empathy when appropriate to do so often gains special insight but, at the same time, no interviewer or fact finder should get personally involved with the case.

5.2.1.12 Handling Hostility

If the fact finder feels threatened by the individual being interviewed, the fact finder should stop the interview and report the situation to the appropriate authorities. When conducting information gathering through interviews, assessors should consider whether security preparations would be appropriate (e.g., having security personnel present or nearby).

Fact finders may encounter argumentative individuals. When this type of hostility is encountered, the fact finder can seek to defuse it by explaining the purpose of the interview and that the interview is a required part of the inquiry. The fact finder has full authority to conduct the interview and the interviewee is required to cooperate; reiterating this may encourage the interviewee to participate.

Recognizing and acknowledging the person's hostility and the reason for it will sometimes let both parties reach the mutual understanding that the interview will proceed (whether or not the topics under discussion are related to the hostility).

If, after repeated attempts in various ways by the fact finder, an individual refuses to answer a specific question, the fact finder should attempt to learn the reason. The fact finder should record the refusal to answer any question and the reason. If the individual wants to terminate the interview, the fact finder should attempt to learn the reason and to dissuade the individual by addressing the concerns. If the individual persists, the fact finder should conclude the interview.

5.2.2 Other Considerations for the Agency Planning Group

This section covers other fact finding issues the agency planning group should address ahead of time.

5.2.2.1 Agency Policy

Agency policy should be formulated ahead of time regarding matters including but not limited to the following:

- No-shows for an interview;
- Whether to allow tape recording of an interview; and
- Whether to allow the presence of additional persons during an interview.

Any agency policy should be based on sound legal analysis.

5.2.2.2 Administrative Details

Routine administrative details cannot be ignored. Prior to beginning the actual inquiry, the fact finder should be given all administrative details, including but not limited to:

- The person(s) to whom the fact finder will deliver their report; and
- The person(s) to contact regarding other administrative matters, such as pay, parking, and overtime.

5.2.2.3 Factors in Credibility Determinations by MSPB

It may be helpful to give the fact finder the list of factors that will be considered by MSPB in making credibility determinations, should the investigation lead to a case before the Board.

These factors are:

- The witness's opportunity and capacity to observe the event or act in question;
- The witness's character;
- The witness's bias or lack of bias;
- The witness's demeanor;
- Any prior inconsistent statement(s) by the witness;
- Any contradiction of the witness's version of events by other evidence or its consistency with other evidence; and
- The inherent improbability of the witness's version of events.

5.2.2.4 Contents of the Final Inquiry Report

Every step of the inquiry should be objective, impartial, and unbiased. The inquiry report should contain:

- Statements of witnesses; and
- Documentary evidence.

Appendix C, Case Study 6 provides practical examples of some of the issues discussed in this section.

Additionally, the analysis of the report:

- Should be objective, impartial, and unbiased; and
- Can contain a letter signed by the agency head or high-level designated official authorizing the inquiry and requiring employees to cooperate. (See the information above regarding warnings to the subjects of administrative inquiries when it is necessary to require cooperation.)

Ensure all appropriate agency personnel are aware of the requirements discussed above regarding warnings when compelling statements from the subject of an administrative inquiry.

5.2.3 The Behavioral Risk Assessment Process

As the case studies in Appendix C illustrate, many cases involving threatening behavior can be handled expeditiously and effectively with the assistance of one or more members of the agency's incident response team or threat assessment team. After gathering more information from the administrative inquiry, the threat assessment team uses the information to: assess the situation's level of violence risk potential; make recommendations for appropriate strategies and security measures to manage concerning behavior; and protect others in the workforce. In addition, it may be helpful for the agency planning group or the threat assessment team to identify experts in threat assessment in case a situation requires more expertise than the threat assessment team can provide.

5.2.3.1 Framework and Methodology

To minimize subjectivity when evaluating the risk level of known concerning behavior to the attention of the agency's threat assessment team, the agency planning group and threat assessment team may seek to evaluate available threat assessment resources and structured professional judgment tools to use as part of its evaluation and recommendation process. The FBI's *Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks* (2017) is a starting resource agencies can use to gain a better understanding of behavioral risk assessment and management methodology and strategies.

5.2.3.2 Resources

It is possible there will be situations and behavior brought to the attention of an agency's trained threat assessment team that will present challenges. It is important to find a qualified professional to assist you if the need arises. Several Federal agencies may have experienced threat assessment professionals within their organizations or within their criminal investigative services. Law enforcement agencies, such as FPS, FBI, and state and local police may be able to assist in identifying experts in threat assessment. An agency may also consider using a threat assessment professional who is outside the organization. In that case, agencies must ensure the threat assessment professional is aware of all relevant Federal laws and regulations.

Another valuable resource is the Association of Threat Assessment Professionals (ATAP), a non-profit, multi-disciplinary professional association that includes psychologists; behavioral health, legal, and corporate security professionals; and members from Federal, state, and local law enforcement agencies. ATAP educates the public on cutting-edge violence prevention research and operational best practices for workplace violence prevention.

5.2.3.3 Considerations and Fundamental Principles

"Threat Assessment" is the term used to describe the set of information gathering and operational techniques used by threat assessment teams, law enforcement, and other collaborative stakeholders to identify, assess, and manage risks of targeted violence and the individuals who

are considering using violence as a solution to their problems. It is important to note that individuals who may come to the attention of a threat assessment team as displaying concerning behavior may or may not pose a threat. Individuals utter threats for many reasons and not all intend to commit a violent act. In contrast, an individual can present a grave and impending threat without articulating a threat. Agency planning groups and threat assessment teams should know the distinction between making and posing a threat. For example, some persons who make threats ultimately pose a threat; many persons who make threats do not pose threats; and some persons who pose threats never make threats. It is imperative the threat assessment team use a threat assessment methodology to ascertain the context of the information gathered on a person of concern to distinguish whether they pose a threat and to manage the concerning behavior to risk reduction.

The importance of using threat assessment methodology and framework is growing, but many agencies may not consider the systematic thinking required for establishing a strong threat assessment program. Four fundamental principles underlie threat assessment inquiry and management:

1. Violence is a process, as well as an act. Violent behavior does not occur in a vacuum. Careful analysis of violent incidents shows violent acts are often the culmination of long-developing, identifiable trails of problems, conflicts, disputes, and failures.
2. Violence is the product of an interaction among three factors:
 - a. The individual who takes violent action;
 - b. A stimulus or triggering conditions that lead the subject to see violence as an option, way out, or solution to problems or life situation; and
 - c. A setting that facilitates or permits the violence, or at least does not stop it from occurring.
3. A key to investigation and resolution of threat assessment cases is the identification of the subject's attack-related behaviors. Perpetrators of targeted acts of violence engage in discrete behaviors that precede and are linked to their attacks; they consider, plan, and prepare before engaging in violent actions.
4. Threatening situations are more likely to be successfully investigated and managed if other agencies and systems—both within and outside law enforcement or security organizations—are recognized and used to help solve problems presented by a given case. Examples of such systems are those employed by prosecutors; courts; probation, corrections, social service, and mental health agencies; EAPs; victim assistance programs; and community groups.

5.2.3.4 Threat Assessment Program Process and Framework

The three major functions of a threat assessment program are (1) identification of a potential perpetrator, (2) assessment of the risks of violence posed by a given perpetrator at a given time, and (3) management of both the subject and the risks that they present to a given target.

Function 1: Identifying Person(s) of Concern

This process includes:

- Defining criteria that could lead to a person becoming a subject of a threat assessment inquiry or investigations;
- Determining the areas within the law enforcement or security organization responsible for receiving information about possible subjects and applying the threat assessment and management process;
- Notifying those individuals and organizations that might come in contact with—or know of—potential subjects about the existence of a threat assessment program; and
- Educating notified individuals and organizations about the criteria for bringing a concern about potential violence to the attention of the threat assessment team.

Function 2: Assessing and Managing Behavioral Risks

The second goal of a threat assessment program is to evaluate the risks that persons under suspicion may pose to particular targets. Behavioral risk assessment involves three primary functions: (1) information gathering; (2) assessment; and (3) providing recommendations to manage the behavior. The primary objective of a risk assessment investigation is to gather information on a subject and on potential targets.

Multiple sources of information should be consulted to learn about a subject’s behavior, interests, and state of mind at various points in time. Areas of information to consider include:

- Personal interviews with the subject;
- Material created or possessed by the subject (including journals and letters) and materials collected by the subject (such as books and magazines) that may relate to the investigation;
- Persons who know or have known the subject, including family members, friends, coworkers, supervisors, neighbors, landlords, law enforcement officers, social service or mental health staff, and previous victims of unacceptable behavior (including violence) committed by the subject;

- Record or archival information, including police, court, probation, and correctional records;
- Mental health and social service records;
- Notes made by those aware of the subject's interest in a particular target, such as security personnel, managers, victims, or colleagues; and
- Detailed descriptions of the subject's behaviors and actions that prompted other persons to notice the subject.

Of particular importance is information about attack-related behaviors:

- The subject expressed interest in possible targets, including particular, identifiable targets;
- The subject communicated with or about potential targets;
- The subject considered and/or attempted to harm self or others;
- The subject secured or practiced with weapons; and
- The subject followed or approached potential targets, either with or without weapons, at events or occasions.

Function 3: Interviewing the Subject

Whether to interview the subject of a threat assessment can be a key question, and that decision depends on several factors:

- The threat assessment team's need for information;
- The facts leading to the initiation of the threat assessment process;
- The threat assessment team's standing in relation to the subject;
- The resources available to the threat assessment team;
- The threat assessment team's training and experience in interviewing;
- The stage of the threat assessment; and
- The threat assessment team's strategy for resolving the case.

A decision to interview a subject should be made based on case facts. Generally, after a face-to-face contact between subject and target or after the subject communicated a threat to the target, an interview is a good idea. An interview under such circumstances may have several goals. It may signal the subject's behavior has been noticed, permit the subject's story to be related to a third party, gather information forming the basis for corroboration, and provide an opportunity for communicating that the subject's behavior is unwelcome, unacceptable, and must cease.

Any interview is a vehicle for gathering information about the subject that can be used to assess and manage the threat the subject may pose. Therefore, threat assessment interviews are most productive if conducted respectfully and professionally. The task of the threat assessment team is

twofold: (1) to gather information about the subject's thinking, behavior patterns, and activities regarding the target(s); and (2) to encourage change in the subject's behavior.

By showing an interest in the subject's life that is neither unduly friendly nor harsh, a threat assessment team interviewer can increase the likelihood of the interview's success. In some cases, however, an interview may intensify the subject's interest in the target or increase the risk of lethal behavior. For example, a desperate and suicidal subject, self-perceived as having been abandoned, who has been stalking a former partner, may sense time is running out and be prompted by an interview to engage in more extreme behavior before "they put me away." In such circumstances, the threat assessment team may need to expend additional resources, perhaps increasing security for the target, arranging hospitalization or arrest of the subject, or monitoring or screening the subject. Subject interviews, therefore, should be considered and conducted within the context of overall behavioral risk (threat) management strategy.

Information about the Target

A man, who over days and weeks, follows a secretary whom he met once but has no relationship, appears to have picked out a potential target. An employee, fired by a manager whom he blames for discriminating against him and causing the breakup of his family, has told former coworkers that he will "get even." Once again, a potential target appears to have been selected. To prevent violence, the threat assessment team requires information on the targeted individual. Relevant questions about the target might include the following:

- Are potential targets identifiable or does it appear that the subject, if considering violence, has not yet selected targets for possible attack?
- Is the potential target well known to the subject?
- Is the subject acquainted with a targeted individual's work and personal lifestyle, patterns of living, or daily comings and goings?
- Is the potential target vulnerable to an attack?
- Does the targeted individual possess resources to arrange for physical security?
- What change in the target's lifestyle or living arrangements could make attack by the subject more difficult or less likely; e.g., is the targeted individual planning to move, spend more time at home, or take a new job?
- Is the target afraid of the subject? Is the targeted individual's degree of fear shared by family, friends, and/or colleagues?
- How sophisticated or naive is the targeted individual about the need for caution? How able is the individual to communicate a clear and consistent "I want no contact with you" message to the subject?

Evaluation

A two-stage process is suggested to evaluate information gathered about the subject and the potential target(s). In the first stage, information is evaluated for evidence of conditions and behaviors consistent with planning an attack. The second stage of evaluation seeks to determine whether the subject appears to be moving toward or away from an attack. After analyzing the available data, the threat assessor is left with these questions:

- Does it appear more or less likely that violent action will be directed by the subject against the target(s)? What specific information and reasoning lead to this conclusion?
- How close is the subject to attempting an attack? What thresholds, if any, were crossed (e.g., the subject violated court orders, made a will, gave away personal items, expressed willingness to die or to be incarcerated)?
- What might change in the subject's life to increase or decrease the risk of violence? What might change in the target's situation to increase or decrease the risk of violence?

Case Management Overview

Once the threat assessment team determines that a given subject presents a risk of violence to a targeted individual, the first task is to develop a plan to manage the subject and the risk. The second task is plan implementation and monitoring. The plan must remain flexible to accommodate changes in the subject's life and circumstances. The final management component is formal closing of the case.

Step 1: Case Management Development

The evaluator proceeds to identify those internal and external systems that may be helpful in managing the problems presented by the subject. In certain situations, such as those in which the subject is stalking an identifiable target in a jurisdiction with an enforceable and effective anti-stalking law, the best way to prevent violence and minimize harm to the targeted individual may be to prosecute the case vigorously. A good relationship between threat assessment teams and prosecutors can influence the priority assigned to the case and the extent to which prosecutorial and judicial processes facilitate its resolution. Such relationships also may affect the court's disposition of the case, including sentencing of a convicted offender.

Even conviction and imprisonment, however, do not guarantee the target will be safe from the subject. If the subject is unable or unwilling to let go of the idea of a relationship with the target, or if the subject attributes the pains and misfortunes of their life to the targeted individual, it may make sense to consider strategies in which the subject is encouraged to change the direction, or intensity, of their interest. A subject engaged in activities that bring success and satisfaction is less likely to remain preoccupied with a failed relationship. Family, friends, neighbors, or associates may play a role in suggesting and supporting changes in the subject's thinking and behavior. In addition, mental health and social service staff may be of great assistance in aiding

the subject to formulate more appropriate goals and develop skills and strengths likely to result in life successes.

At least one aspect of a case management plan concerns the target. If the subject is to be prohibited from contact with the target, the target needs to understand what to do (i.e., whom to call and how to contact the official handling the case) if the subject initiates direct or indirect contact.

Step 2: Case Management Implementation

The most carefully crafted plan will have little effect if it remains in the threat assessment team's files and is not translated into action. Although no procedures or techniques can guarantee that a subject of comprehensive threat assessment will not attempt violent action towards a target, two activities are known to help reduce the risk of violence and assist the threat assessment team in any post-incident review.

First, documentation of data and reasoning at every stage of the threat assessment process is essential. Undocumented or poorly documented information gathering and analysis provide little foundation for review or for efforts to learn from or improve on experience. Without clear documentation, threat assessment teams are left with only their recollections, which can be partial and faulty and are subject to criticism as retrospective reconstruction. A carefully and comprehensively documented record may be criticized for imperfect data gathering or flawed analysis, but such a record also demonstrates both thoughtfulness and good faith—critical questions in any post-incident review.

Second, consultation at every major stage of the threat assessment process can be a significant case management tool. Consultants may be members of the threat assessment unit or external experts. To be effective, a consultant should be knowledgeable in areas relevant to the case and be known and trusted by the threat assessment team. For example, in a case where a subject has a history of diagnosed mental disorders and the primary threat assessor is unfamiliar with mental health language and concepts used in the records, an expert in psychology or psychiatry can provide invaluable insight and advice.

In addition to providing special expertise, consultants may notice and raise unanswered or unexplored questions in a case. Even proficient threat assessment teams are occasionally vulnerable to missing the obvious in front of them. A consultant, such as a fellow threat assessment specialist not involved with the case, may offer a comment that can redirect or sharpen an ongoing investigation. Appendix C provide practical examples of the application of the process discussed in this section. In the event of a bad outcome, use and documentation of consultant expertise may demonstrate that the threat assessment team sought additional perspectives and ideas and did not suffer from “tunnel vision.”

Step 3: Closing the Case

The final task of threat assessment case management is closing the case. When a threat assessor determines the subject has moved far enough away from possible violent action toward the target to no longer causing appreciable concern, the case can be considered for closing. At this time, it may be important to ask:

- What changed in the subject's life that appears to lessen the likelihood the subject is interested in or will attempt violent action toward the target?
- Which components of the case management plan seemed to affect the subject's thinking or capacity to initiate violent action and to what extent?
- What life circumstances might occur that would again put the subject at increased risk of contemplating, planning, or attempting violent action toward the original target or other potential targets?
- Are there supports, either already in place or that can be developed, that will be known and available to the subject at a future time when the subject is again at risk of moving toward violent behavior?

While social commentators and analysts may debate the myriad reasons that lead to growing national concern about targeted violence, law enforcement and security organizations are increasingly being called on to examine individual situations and make judgments and determinations about the risks of violence a single person might present to an identifiable target. In cases related to stalking behaviors, workplace violence, attacks on public officials and figures, and other situations where targeted violence is a possibility, a comprehensive and carefully conducted threat assessment process can safeguard potential targets, deter potential attackers, and serve the public. For further information about threat assessment, refer to Appendix B.

5.3 EAP Considerations

EAP participation can be important to the success of an agency's workplace violence program. The EAP's role generally begins with participation on the agency planning group where decisions are made about the role the EAP will play in the workplace violence prevention and response program.

EAPs usually play an active role in early prevention efforts, sometimes participate on the incident response team, and generally assist with organizational recovery after an incident of workplace violence has occurred. This section provides an overview of the EAP and discusses considerations specific to workplace violence.

5.3.1 Overview of the Employee Assistance Program

Every Federal agency has an EAP that provides short-term counseling and referral services to its employees at no cost. These programs are staffed by professional counselors who are available to discuss problems that can adversely affect job performance, conduct, and reliability. EAP counselors are required to help employees deal with alcoholism, drug abuse, and marital and financial problems. EAP counselors often refer employees to other professional services and resources within the community for further information, assistance, or long-term counseling.

EAPs differ from agency to agency in their structure and scope of services. Some are in-house programs, staffed by employees of the agency. Others are contracted or operated through an interagency agreement with HHS's Division of Federal Occupational Health. Services differ among contracted programs depending on the terms of the contract and the relationship between the agency and the contractor.

Confidentiality is an important issue for EAPs. Employees who seek EAP services are afforded considerable privacy by laws, policies, and the professional ethics of EAP professionals. It is common practice for EAPs to inform employees in writing about the limits of confidentiality on their first visit.

Agency planning group members should familiarize themselves with the structure, scope, and special considerations of their agency's EAP. As the agency planning group explores the range of services provided, it may identify needs for expanding the program's existing array of services. EAP professionals should advise the agency planning group on the relevant laws, policies, and professional ethical constraints under which they operate, including the Privacy Act provisions of 5 USC §552a and the HHS Alcohol and Drug Patient Confidentiality Regulation provisions of 42 CFR § 2. This will allow cooperative arrangements to be worked out for an appropriate EAP role.

5.3.2 EAP's Role in Dealing with Workplace Violence

The following sections discuss the EAP's role in dealing with workplace violence.

5.3.2.1 Role in Early Prevention Efforts

- **Promotion of the EAP.** The effectiveness of a workplace violence program is greatly enhanced in an organization with an active, well-known EAP presence. Agencies with active programs promote the EAP by issuing periodic statements from top management endorsing the program and reminding employees of the services offered by the EAP, having counselors attend staff meetings to familiarize agency employees with the counselors, and having counselors give special briefings and seminars for managers, employees, and union stewards.

- **Information dissemination.** EAPs often provide booklets, pamphlets, and access to books and videos about such topics as domestic violence, stress reduction, and dealing with angry customers.
- **Early involvement in organizational change.** When an agency is facing reorganization, restructuring, or other organizational change that may have a negative effect on employees, the EAP can help by creating individual or group sessions. These sessions provide a means to keep information flowing, keep feelings under control, prevent potential outbursts, provide constructive outlets for feelings, and help employees plan for the future.
- **Employee and supervisory training.** Much of the employee training described in Chapter 4 is conducted by EAP staff. For example, counselors can train employees on such topics as dealing with angry coworkers and customers, conflict resolution, and communication skills. Since EAP staff understands how important it is that supervisors (and coworkers) refrain from diagnosing an employee's problem, they are in an excellent position to explain the delicate balance between identifying problem behavior early on and labeling an individual as potentially violent.

5.3.2.2 Participation on an Incident Response Team

Since every reported incident of workplace violence is different and every agency is structured differently, EAP participation on an incident response team will depend on many factors. Issues need to be clarified ahead of time to avoid misunderstanding and conflict. Team members need to understand that if a case is being discussed and the counselor indicates that they cannot provide assistance, they should neither expect an explanation nor assume the counselor is being uncooperative. Advance planning can help to identify ways of coping with these types of issues. If, for example, the EAP is large enough, then different staff members may play different roles or the staff may be able to identify other professionals who can be brought in to ensure all needs are addressed. Working with other members of the agency planning group and the incident response team in advance can clarify the EAP's role when an incident arises.

5.3.2.3 Consultation with Supervisor when an Incident is Reported

Depending on the type of incident reported, it is often important for a counselor, along with an employee relations specialist and security officer, to be part of the incident response team that consults with the manager. In some situations, such as potential suicides, the EAP can play a major role. In other situations, such as dealing with an employee who frightens coworkers, but who has not actually done or said anything warranting discipline, the EAP can assist other team members in working with the supervisor to plan an effective response.

5.3.2.4 Response and Intervention

The counselor can help with conflict resolution in situations reported early enough for such an intervention. The counselor can work with the victim by giving advice and guidance, or with the perpetrator by helping to diffuse the anger/hostility that could lead to violence. The counselor can help clarify options and procedures for situations where substance abuse or mental illness seems to be a factor. For example, states differ in their laws regarding civil commitment for psychiatric treatment. The counselor can explain to other team members the EAP role in such a situation and can coordinate with other community resources to develop contingency plans for various emergency situations. These and other examples are illustrated in the case studies in Appendix C.

5.3.2.5 Follow-up to a Violent Event

Many EAPs are prepared to respond promptly to a variety of needs that may exist after a violent incident. Prompt individual interventions with employees who had particularly stressful experiences are sometimes necessary. Debriefing sessions for groups are often conducted two or three days after the incident. The EAP can also act as consultants to management in helping the organization to recover.

5.3.2.6 Individual Interventions

Though most employees will need only brief intervention, provision should be made for the few who may need longer-term professional assistance. Strategies for identifying these employees and guiding them as smoothly as possible from emergency-centered interventions to more extensive mental health care should be included in the planning.

The EAP may approach these responsibilities in different ways, depending on the size and experience of its staff. In some cases, internal EAP resources may be sufficient, but in others, additional staffing will be necessary. EAP staff members who do not have expertise in traumatic incident counseling may wish to develop in-house expertise or keep close at hand the phone numbers of resources to contact should an incident occur. Potential sources of additional help (e.g. private contractors, community mental health resources, university or medical school programs) may be explored.

5.3.2.7 Acting as Consultants to Management

Since management, which typically bears the responsibility after a violent incident, may find dealing with unfamiliar and highly stressful situations challenging, the EAP can be helpful in facilitating an optimal response. It can provide managers with information on traumatic events and can assist them in analyzing the situation and developing strategies for the organization's recovery. An effective EAP needs to be familiar not only with post-disaster mental health care, but also with management practices facilitating recovery and with other resources that may need to be mobilized.

In thinking about an organization's recovery, there is a temptation to focus narrowly on care-giving responses such as debriefings and counseling discussed above. Essential as these services are, they are only part of the picture. The way the manager conveys information, schedules responsibilities, sets priorities, and monitors employee performance after a violent incident can play a vital role in helping or hindering recovery. Some EAPs are trained to provide this type of consultation. Agencies will find *A Manager's Handbook: Handling Traumatic Events* helpful in this regard. A link to the *Manager's Handbook* can be found in Appendix B.

5.3.3 Other EAP Considerations for the Agency Planning Group

The following sections discuss other EAP considerations for the agency planning group.

5.3.3.1 Should the EAP Take the Incident Report?

Most agencies do not use the EAP as the office responsible for taking incident reports on workplace violence. The following paragraphs outline some of the reasons cited by agencies.

Because confidentiality requirements prohibit EAP counselors from disclosing information, having a counselor manage an incident report could lead to serious misunderstandings among agency employees who do not have the same inside knowledge as the counselor. Additionally, this could harm the credibility of the EAP. It sometimes takes years to build the EAP into a viable program trusted by employees to keep any contacts confidential; the dual role could diminish this viability.

In addition, the incident reports could become confused with EAP records covered by the agency's internal system of records. Records filed and retrieved by name or other personal identifier are subject to the Privacy Act provisions of 5 USC §552a. Since each agency's system of records is different, it is a good idea to check with the agency's Privacy Act Officer regarding the systems notice for the agency's EAP. The systems notice covers who can gain access to the records and how amendments are made to the records.

Many times the EAP counselor will be the person who first hears about an incident involving threatening behavior, even though the agency's reporting system provides for another office to take incident reports. Managers and employees often feel comfortable telling the counselor about a situation that frightens them. The agency planning group should decide ahead of time what types of reports the counselors should handle alone and the types that should be reported to the other team members, always making sure each member of the team understands the confidentiality requirements of the EAP.

5.3.3.2 Should the EAP be the First to Intervene?

Agencies which have had experience with the EAP as the first intervener in workplace violence situations report they do not recommend using the EAP as the first group to intervene for the following reasons:

- Issues of confidentiality cause numerous conflicts for the counselors; and
- It could lead to a perception of treating perpetrators of workplace violence as victims needing counseling rather than as perpetrators needing discipline.

The agency planning group should ensure procedures allow for flexibility and do not require counselors to be the first interveners in situations where this would be inappropriate.

5.3.3.3 Should the EAP Perform Psychological Exams?

Organizations with experience in offering psychological or psychiatric examinations usually recommend that these not be performed by the EAP staff. The process of conducting examinations is not only time consuming and highly specialized, but fits poorly with other EAP responsibilities. Thus, most agencies find it preferable, if offering such an examination, to have it done by an outsider such as an external contractor. Some agencies have professional mental health staffs in addition to the EAP and use them for this type of evaluation. The EAP can then take the role of teacher and facilitator, helping everyone involved to understand the report of the examination and put its recommendations into practice.

Appendix C, Case Studies 1, 2, 4, 6, 7, 11, and 14 provide practical examples of some of the issues discussed in this section.

5.4 Organizational Recovery Post-Incident

Despite the best-laid plans of any Federal agency, violence in the workplace occurs. Agencies should develop both written policies and procedures designed to head off these occurrences as well as preparations to deal with the aftermath of such incidents. Quite often, management focuses on continuity of operations; however, mitigating the impact incidents have on office personnel is equally important. This section provides information designed to assist management with helping an organization to recover after an incident of workplace violence.

5.4.1 Management Steps to Help an Organization Recover

When incidents of workplace violence occur, management may take several initial steps to assist their employees. This may begin with managers spending ample time with their employees. Employees need to be reassured of their concern, and they need to be able to ask questions. Senior management should ensure immediate supervisors are supported in this role, relieved of unnecessary duties, and not pulled away from their subordinates unnecessarily.

5.4.1.1 Share Information with Employees

It is important for managers to share information with the rest of the workplace community as rapidly and honestly as possible, so false reports and irrational fears do not spread and make the situation worse. Employees will have many questions, and they need the answers, often more than once, if they are to resolve the experience for themselves. Information will develop over time; therefore, information strategies need to be simple and fluid. A notice board at the elevator or a recorded message on a “hotline” number may suffice for the basics, and organizations might consider establishing a user-friendly system for individual questions. Union representatives can also help in reassuring employees after an incident and in getting information to employees.

5.4.1.2 Bring in Crisis Response Professionals

Prior to an incident, the agency planning group should identify trained mental health professionals in the agency’s EAP or the community who would be available to respond in the event of an incident. Some organizations may wish to develop their own in-house capacity to deliver best practices in psychological aspects of incident response, since these may not be available locally. Psychological services can offer victims and their coworkers comfort, information, support, and help with practical needs. It can also spot those who appear most troubled by the event and may need more intensive psychological attention in the future.

When an incident occurs, involve emergency mental health consultants as soon as possible. They will generally meet with management first, working down the chain, and then with employees. Based on the findings, consultants will offer various services. Examples of possible services include the following:

- **Support Informal Debriefing:** The formal debriefing does not end the recovery process. Provide opportunities for employees to talk informally with one another when they feel a need to discuss the experience. A comfortable break area and flexibility about break times may be all that is needed.
- **Support Caregiving within Work Groups:** Keep work units together as much as possible and try not to isolate employees from their normal support groups at work. Show respect and support for employees’ efforts to care for one another.
- **Handle Critical Sites with Care:** Initially, the site of a violent incident may be secured as a crime scene. After the authorities clear the scene and collect necessary information, management needs to be sensitive to a number of issues. It is helpful if employees don’t have to return to work and face painful reminders such as blood stains or broken furniture. But on the other hand, the area should not be so “sanitized” that it gives the appearance that management is pretending nothing happened. If someone has died, that person’s work area will be a focus of grieving and should be respected as such.

- **Buffer Those Affected from Post-Event Stresses:** Effective coordination with the media and timely dissemination of information can help reduce media pressure on those who are the most vulnerable. Questions from the news media relating to incidents of workplace violence should be forwarded to the appropriate public affairs staff for the agency. Assistance with benefits and other administrative issues can reduce the burden on victims and families.
- **Help Employees Face Feared Places or Activities:** Returning soon to a feared site, if only briefly, can help prevent lasting effects such as phobic responses. Having a friend or loved one along or being supported by close work associates may make the first step much easier.
- **Remember the Healing Value of Routine:** Getting back to a regular routine can be reassuring. The sense of having a mission to perform at work can help the group recover its morale. The return to work must be managed in a way that conveys appropriate respect for the deceased, the injured, and the traumatized.
- **Follow Up with Those Exposed to Extreme Stressors:** Some individuals may be especially at risk for continuing emotional problems due to the nature of their exposure (e.g., survivor of a severe physical assault; sexual assault survivor). Following up with these individuals can facilitate monitoring of continuing stress reactions and enable increase in intensity of services as needed.

5.4.2 Critical Incident Stress Management Process

Following traumatic events in the workplace, employees often experience short-term behavioral and mood adjustment problems or symptoms of post-traumatic stress disorder. Agency managers should address these issues by advising all employees to access the agency's EAP service to assist with any strong negative emotions, anger, sleep problems, or other normal reactions to the abnormal event. In addition, most Federal employees will have mental health services available through their Federal health insurance benefits. Seeking help for adjustment problems should be characterized by managers in a normalizing manner, but should not be pushed or mandated. Not all EAP services have immediately accessible emergency response capability. It is important to determine that this capacity exists, that EAP providers have been trained, and that the planned response is consistent with best response practices.

Generally, immediate behavioral health responses should not be attempted except by a mental health professional well-versed in the risks and benefits of Psychological First Aid (PFA) and crisis counseling methods. However, many EAPs are trained to participate on Critical Incident Stress Debriefings (CISD) teams. In more recent years, research studies of the most commonly used formal crisis intervention process, stress debriefing, consistently show that stress debriefing does not prevent development of post-traumatic stress disorder (PTSD) or depression, and some investigators found a risk of possibly exacerbating mental health symptoms when CISD and related approaches are applied. Methods of PFA have been endorsed by groups of experts as an

alternative to stress debriefing for immediate response in the first hours and days post-incident. However, PFA alone is not an adequate post-incident response. Rather, it should be part of a more comprehensive set of activities that would also include survivor education, ongoing monitoring and follow-up, and referral for more intensive services as needed. Such comprehensive approaches have sometimes been called Critical Incident Stress Management.

None of the information provided in this section should take the place of specialized training in the field.

5.4.2.1 Purpose of Behavioral Health Response

Behavioral health responses to traumatic events should form part of an integrated system of services and procedures with a purpose to achieve several goals:

- Prevention of traumatic stress;
- Mitigation of traumatic stress;
- Intervention to assist in recovery from traumatic stress;
- Acceleration of recovery whenever possible;
- Restoration to function; and
- Maintenance of worker health and welfare.

5.4.2.2 Response Team

A response team, generally comprised of mental health professionals and trained peer support personnel, provides a variety of services including:

- PFA;
- Defusing;
- Demobilizations after a disaster;
- Informal discussions;
- Significant other support services;
- Work support groups;
- Individual consults (one-on-one); and
- Follow-up services.

For the purposes of this discussion, the focus will be on PFA.

5.4.3 The Psychological First Aid Model

The impact of a critical incident on an individual's life appears to be mitigated, to some degree, by the availability of intervention resources used at various stages following the incident. The PFA model assists the victims of critical incidents with their recovery process.

The PFA model involves a set of core actions described below.

#	Core Action	Goal
1	Contact and Engagement	Respond to contacts initiated by affected persons or initiate contacts in a non-intrusive, compassionate, and helpful manner.
2	Safety and Comfort	Enhance immediate and ongoing safety and provide physical and emotional comfort.
3	Stabilization (if needed)	Calm and orient emotionally-overwhelmed or distraught survivors.
4	Information Gathering: Current Needs and Concerns	Identify immediate needs and concerns, gather information, and tailor PFA interventions.
5	Practical Assistance	Offer practical help to the survivor(s) in addressing immediate needs and concerns.
6	Connection with Social Supports	Assist in establishing opportunities for brief or ongoing contacts with primary support person(s) or other sources of support, including family members, friends, and community resources.
7	Information on Coping	Provide information about stress reactions and coping to reduce distress and promote adaptive functioning.
8	Linkage with Collaborative Services	Link survivor(s) with needed services and inform them about available services that may be needed in the future.

These core goals of PFA constitute the basic objectives of providing early assistance (e.g., within days or weeks following an event). They should be addressed in a flexible way, using strategies that meet the specific needs of affected groups. The amount of time spent on each goal will vary from person to person and with different circumstances according to need.

5.4.4 Is a Behavioral Health Response Warranted?

One determination to make is whether a formal behavioral health response consultation with mental health experts is warranted. Though not all-inclusive, some examples of important questions to explore when assessing the need for such a response are:

- What is the nature of the incident?
- Is the incident of sufficient magnitude as to cause significant emotional distress among those involved?
- How many individuals are affected by the incident?
- What signs and symptoms of distress are being displayed by the witnesses to the incident? Are the signs and symptoms growing worse as time passes?

- Are any of the following key indicators of a need for a response present: behavior change, regression, continued symptoms, intensifying symptoms, new symptoms arising, or group symptoms?

As these and other questions are explored, some instances may not warrant a formal debriefing. There may be a decision to briefly meet with the group(s) affected by the incidents to further assess the need for a formal debriefing. Under these circumstances, a critical incident stress defusing may be appropriate.

5.4.5 Conclusion

Although it is well established that incidents of workplace violence and other traumatic events can sometimes lead to development of PTSD and other problems in some survivors, the effectiveness of PFA and other early interventions after these events is less clear. CISD has been shown not to prevent mental health problems, but PFA, although based on expert consensus, has not yet been tested in research. PFA and other educational and supportive methods should be employed following potentially traumatic events and delivered by trained mental health professionals and other trained behavioral response team personnel.

6.0 Development of Written Policy

The following sections discuss the development of a written workplace violence prevention and response policy.

6.1 Advantages of Written Policies

Once a workplace violence prevention and response program is ready to be implemented, agencies must decide whether to issue a written policy statement. There are advantages to issuing a statement. Agencies that choose to implement a written policy grant the employees a resource to refer to, as needed. The written policy may inform employees that the agency's policy covers intimidation, harassment, and other behavior that encompasses what a reasonable person would view as inappropriate. It may also encourage employees to report incidents, inform employees about how to report an incident, and demonstrate senior management's commitment to dealing with reported incidents.

Agency programs can also be implemented without a written policy statement. In agencies without a written policy statement, employees are often given information about the program (e.g., how to report an incident) in training sessions, on posters, in newsletter articles, or by other similar methods. It is important to note that agencies have an inherent right to take action against employees who engage in disruptive or threatening behavior regardless of whether or not the agency issued a written policy statement.

6.2 Policy Statement Contents

A workplace violence policy statement should convey the following:

- Employees are responsible for maintaining a safe work environment;
- Employees are obligated to act appropriately on the job;
- The policy covers not only acts of physical violence, but also harassment, intimidation, and other disruptive behavior;
- The policy covers individuals outside the agency, including interns, contractors, guests, visitors, and others (as determined by the agency) who present the risk of violence;
- The agency will respond appropriately to all reported incidents; and
- The agency will act to stop inappropriate behavior.

The policy should emphasize that offices involved in responding to incidents will be supported by agency management, in accordance with their individual agency's plans, in their efforts to deal with violent and potentially violent situations. The policy statement should also provide examples clearly indicating some of the behaviors that constitute workplace violence, along with specifying prohibited actions and their consequences.

Examples of prohibited behaviors could include but are not limited to:

- Direct threats or physical intimidation;
- Implications or suggestions of violence;
- Bullying;
- Stalking;
- Assault of any form;
- Physical restraint or confinement;
- Dangerous or threatening horseplay;
- Blatant or intentional disregard for the safety or well-being of others;
- Commission of a violent felony or misdemeanor on agency property;
- Any act that a reasonable person would perceive as constituting a threat of violence;
- Loud, disruptive, or angry behavior or language that is clearly not part of the typical work environment; and
- Possession of weapons of any kind on agency property, including parking lots and other exterior agency premises, or while engaged in agency activities in other locations or at agency-sponsored events, unless such possession or use is a requirement of the job.

6.3 Recommend Approaches

A written policy statement should be brief and simple. Implementation details can be provided in training and in more detailed backup documents. For example, roles and responsibilities of the various offices involved in responding to potentially dangerous situations can be outlined in a memorandum of understanding or in operating manuals or instructions rather than in the written policy statement issued to all agency employees. This approach gives agency staff the flexibility to deal creatively with fluid, unpredictable situations.

There are disadvantages to using defined terms such as violence, threats, and harassment in a written policy statement. Definitions may discourage an employee from reporting incidents they do not believe fall within the definition. The reporting system should not deter an employee from reporting situations they feel are of a threatening nature. An employee knows a threat or intimidation or other disruptive behavior when they experience it; definitions are not necessary. The scope of the organization's concept of one or more of the terms in the policy can be clarified by use of examples.

Another consideration is that definitions are often restrictive and may create legal problems in the future when taking disciplinary actions against perpetrators of workplace violence. Use of definitions can make it more difficult to defend a case on appeal. For example, there may be negative consequences from employing the term "zero tolerance." Use of the term could make it more difficult to defend a case on appeal because a third party could conclude, however mistaken and inappropriate, that the agency did not consider an appropriate penalty for the particular offense. Bear in mind that the list of terms included in this guide are merely examples and may not include all possible scenarios and circumstances.

There are other possible consequences. The term “zero tolerance” might appear to eliminate any flexibility an agency has in dealing with difficult situations even if there is a lack of intent on the part of the perpetrator. The appearance of inflexibility can also discourage employees from reporting incidents because they do not want to get their coworker terminated when they just want the behavior stopped. This appearance of inflexibility may also discourage early intervention in potentially violent situations.

Consult your agency’s legal support for the implications of the draft policy. Agencies wishing to issue a written policy statement can use the sample provided in Appendix B, changing the format and tone as appropriate and adapting it for their own situations.

7.0 Acknowledgements

The ISC wishes to thank the following organizations for their participation in the ISC Workplace Violence Working Group (2017-2019):

- Administrative Office of the United States Courts
- Department of Commerce
- Department of Energy
- Department of Homeland Security
- Department of Justice
- Environmental Protection Agency
- Federal Aviation Administration
- Federal Bureau of Investigation
- Federal Protective Service
- General Services Administration
- Internal Revenue Service
- Office of Personnel Management
- Pentagon Force Protection Agency
- U.S. Citizenship and Immigration Services

7.1 ISC Working Group Participants (2019 Edition)

ISC Program Director

Daryle Hernandez
Interagency Security Committee
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

ISC Operations Director

Bernard Holt
Interagency Security Committee
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

ISC Workplace Violence Working Group Chair

Mary Good
Office of the Chief Human Capital Officer
U.S. Department of Homeland Security

ISC Workplace Violence Working Group Members and Contributors (2017-2018)

Alexis Brown
Office of Personnel Management

Gregg Bursey
Administrative Office of the U.S. Courts

Michelle Calhoun
U.S. Citizenship and Immigration Services

Jeffrey Campbell
Environmental Protection Agency

Julia Crawley
Federal Bureau of Investigation

Robert Eilets
Federal Protective Service

Teddy England
Department of Homeland Security

Tony Evernham
Interagency Security Committee

Sarah Golden
Interagency Security Agency

Lisa Grealish
Pentagon Force Protection Agency

Scott Harrington
Federal Protective Service

Sheryl Hollins
Department of Commerce

Aaron Irvin
Pentagon Force Protection Agency

Parker Larson
Department of Homeland Security

William McHale
Federal Aviation Administration

Jimmy Ogletree
Department of Homeland Security

Dennis Ouellette
Internal Revenue Service

Curtis Purinton
Federal Protective Service

Yvonne Rutherford
Interagency Security Committee

Scott Tuttle
General Services Administration

Heather Walker
Department of Justice

JoAnda Weaver-Lillard
General Services Administration

Josh Williams
Department of Energy

Eric Windham
Pentagon Force Protection Agency

Christopher Yingling
Federal Protective Service

Michelle Zayas
Federal Protective Service

7.2 ISC Working Group Participants (2013 Edition)

ISC Workplace Violence Working Group Chair

Bernard Holt

DHS Interagency Security Committee

ISC Workplace Violence Working Group Participants (2010-2012)

Alexis Adams-Shorter, Ph.D.
Office of Personnel Management

Michelle B. Baker-Dubbs
Federal Deposit Insurance Corporation

David Brummond, Ph.D.
Veterans Health Administration

Ingrid Burford
Office of Personnel Management

Jeffrey Cavanaugh
Interagency Security Committee

James Gallagher
Department of the Interior

Michael Hodgson, MD
Veterans Health Administration

Jeffrey Jenkins
Department of Homeland Security

Marie L'Etoile
Office of Personnel Management

Javier Perez
Office of Personnel Management

Josef I. Ruzek, Ph.D.
Veterans Health Administration

Lynn Van Male, Ph.D.
Veterans Health Administration

Teresa Williams
Office of Personnel Management

7.3 ISC Working Group Participants (2010 Edition)

ISC Workplace Violence Working Group Members and Contributors (2008 – 2009)

Harlan Amandus
Department of Health and Human Services

Gregory Barber, Sr.
Department of Labor

Patricia Billeter
Department of Commerce

Mike Bryan
Interagency Security Committee

Brian Farrow
Federal Protective Service

Paula Grubb
Department of Health and Human Services

Daniel Hartley
Department of Health and Human Services

Gwainevere Hess
Interagency Security Committee

Jerome Huggins
United States Postal Inspection Service

Marie L'Etoile
Office of Personnel Management

Ronald Martin
Department of Health and Human Services

Donna Peterson
United States Postal Inspection Service

Lucy Polk
Office of Personnel Management

Shanika Ratliff
Department of Commerce

Susan Reider
Department of Health and Human Services

Sydney Smith-Heimbrock
Office of Personnel Management

Timothy Sullivan
Department of Defense

Mary Tyler
Uniform Services
University of the Health Sciences

7.4 OPM Working Group Contributors (1998 Edition)

Contributors to OPM's Dealing with Workplace Violence: A Guide for Agency Planners (OPM, 1998)

Melvin Basye Federal Protective Services	Gary Beard Federal Protective Services
Bernard Beidel U.S. House of Representatives	Thomas Bresson Smithsonian Institution
Cathleen Civiello, Ph.D. Department of Defense	Scott Cooper, Esq. Department of Justice
Ben Elliot Department of Justice	Robert L. Eufemia, Ed. D Government Printing Office
Yvonne Fair Department of the Navy	Robert A. Fein, Ph.D. Consultant
Cynthia Field Consultant	Michael Gelles, Psy. D Naval Criminal Investigative Service
Lauretta Grier Department of Housing and Urban Development	Lana Katz American Federation of Government Employees, retired
Mark Maggio Federal Justice Center	Peter McCauley Internal Revenue Service, retired
Randi Mendelsohn Federal Emergency Management Agency	Lloyd Reese Department of Veterans Affairs, retired
Milagro Rodriguez American Foundation of Government Employees	Eugene Rugala Federal Bureau of Investigation
Lisa Teems Department of Health and Human Services	Bryan Vossekui United States Secret Service
Janice Walker Department of the Navy	Patricia Willman Department of Interior
John D. Zielinski National Labor Relations Board	

Abbreviations / Acronyms / Initialization List

ADR	Alternative Dispute Resolution
AOUSC	Administrative Office of the United States Court
ATAP	Association of Threat Assessment Professionals
CDC	Center for Disease Control and Prevention
CFR	Code of Federal Regulations
CISA	Cybersecurity and Infrastructure Security Agency
CISD	Critical Incident Stress Debriefing
DHS	Department of Homeland Security
DOC	Department of Commerce
DoD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOL	Department of Labor
EAP	Employee Assistance Program
EEOC	Equal Employment Opportunity Commission
EO	Executive Order
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FPS	Federal Protective Service
FSC	Facility Security Committee
GSA	General Services Administration

HHS	Department of Health and Human Services
HSPD	Homeland Security Presidential Directive
IRS	Internal Revenue Service
ISC	Interagency Security Committee
ISSM	Information System Security Manager
ISSO	Information Security System Officer
MSPB	Merit System Protection Board
NIOSH	National Institute for Occupational Safety and Health
NITTF	National Insider Threat Task Force
OEP	Occupant Emergency Plan
OGC	Office of General Counsel
OIG	Office of the Inspector General
OPM	Office of Personnel Management
OSH	Occupational Safety and Health
OSHA	Occupational Safety and Health Administration
PFA	Psychological First Aid
PFPA	Pentagon Force Protection Agency
PMDB	Prevention and Management of Disruptive Behavior
PTSD	Post-Traumatic Stress Disorder
USC	United States Code
USCIS	United States Citizenship and Immigration Services
VHA	Veterans Health Administration
VSS	Video Surveillance System