

WHAT IS WORKPLACE VIOLENCE?

Behaviors and actions, including harassment, intimidation, non-verbal threats, verbal threats, verbal abuse, sexual assault, stalking, assault, and homicide, occurring in or related to the workplace.

WARNING SIGNS

Typically, acts of violence are preceded by some form of behavior which signals the violence to come. Identifying early and seeking intervention could de-escalate the potential for violence. Direct or indirect threats may or may not proceed an event. The following is a list of risk factors that may serve as warnings. However, these do not necessarily mean someone will commit a violent act. No one type of conduct can predict violence.

MODERATE RISK WARNING SIGNS (Concerning; yet do not indicate a clear/immediate threat of violence toward an identified target)

- Distorted perception of being picked on.
- Unusual weight gain or loss
- Significant change in hygiene/appearance
- Holding grudges
- Non-violent criminal behavior
- Belligerence/Insubordination
- Encourages disruptive behavior
- Inappropriate communications
- Feelings of rejection
- Fascination with workplace violence incidents
- Racism/Sexism
- Social Withdrawal/Isolation
- Low work interest/poor performance
- Chronic victimization of violence/bullying
- Life-changing event
- Obsession
- Diminishing inhibitions
- Sense of inevitability
- Idolization of infamous people
- Mental Health Issues

HIGH RISK WARNING SIGNS (Threat is real, yet lacks immediacy or a plan. Target may not be identified)

- Substance abuse
- Preoccupation with violence
- History of discipline problems
- Statements indicating desperation
- Morbid jealousy/Irrational thoughts

- Persistent pursuit/stalking
- Aggressive sexual behavior
- Uncontrolled Anger
- Impulsive/chronic hitting or bullying
- Identification with hate/extremist groups
- Sympathetic to violence promoting organizations
- Supports/Advocates terrorism
- Expresses hatred/intolerance of American culture
- Comparing terrorists to freedom fighters
- Outrage against military operations

EXTREME RISK WARNING SIGNS (Clear and immediate threat of violence; target has been identified)

- Physical abuse of spouse/children
- History of violent/aggressive behavior
- Misuse of firearms/weapons
- Homicidal/suicidal thoughts/expressions
- Active psychotic symptoms (hearing voices, delusions)
- Advocate violence for political, religious, or ideological reasons
- Seeks/researches items that would be useful for mass violence or terrorism (bomb-making material, etc.)
- Provides financial or material support to a terrorist
- Expresses obligation to support terrorism/violence
- Engages in training with anti-U.S. individuals
- Expresses intent to commit a terrorist act

WORKPLACE VIOLENCE REPORTING OPTIONS

- Immediate Threat: Call Law Enforcement/911
- Not Imminent:
 - Chain of Command/Supervisor. If in your chain of command, utilize another supervisor.
 - Violence Prevention Officer
 - Human Resources Office
 - NCIS 24/7 Anonymous Tip Line: Text "NCIS" to 274637
 - NCIS: www.NCIS.navy.mil or download App (Tip Submit Mobile)

WHAT IS TERRORISM?

The unlawful use of violence or threat of violence, often motivated by religious, political, or other ideological beliefs, to instill fear or coerce governments or societies in pursuit of goals that are usually political. Please note that workplace violence can also be terrorism if both definitions are met.

TERRORISM PRE-ATTACK INDICATORS

- Surveillance: Drawing, measuring, photographing/recording facilities
- Elicitation: Probing (questioning)
- Test of Security: People in secure/restricted areas without official purpose
- Acquiring Supplies: Purchase/Theft of explosives, weapons, ammunition, chemicals, equipment, or counterfeiting/stealing IDs
- Dry Runs: An example would be calling in a bomb threat to record response procedures

TERRORISM IMMINENT THREAT INDICATORS

- Deploying assets/getting into position for an attack
- Unattended briefcases, bags, packages
- Vehicles left in No Parking areas
- Chemical smells or fumes
- A person wearing clothes that are too big/hot for weather

TERRORISM REPORTING OPTIONS

- Immediate Threat: Call Law Enforcement/911
- Not Imminent: USMCEagleEyes.org



FLIP FOR SUSPICIOUS ACTIVITY REPORTING BEST PRACTICES AND INSIDER THREAT (COUNTERINTELLIGENCE) INFORMATION

SUSPICIOUS ACTIVITY REPORTING

Providing law enforcement with as many details as possible greatly enhances their ability to investigate suspicious activity. The following are recommendations for how to remember what to gather:

Vehicles (CYMBALS):

- Color - What is the color of the vehicle?
- Year - Do you know the year?
- Make - Chevrolet, Ford, Honda, etc.
- Body - Truck, car, SUV, big, little, hybrid
- Additional Features - Stickers, loud muffler, damage
- License Plate # - Whole number or groups of numbers
- State - State of issuance

People (SALUTE):

- Size - Number of people, or size of person
- Activity - What are they doing?
- Location - Where at?
- Uniform - What are they wearing?
- Time—When were they doing it?
- Equipment - Did they have anything with them?

INSIDER THREAT (COUNTERINTELLIGENCE)

A unit can often detect/control when an outsider (non-employee) tries to access data either physically or electronically, and can mitigate the threat of an outsider stealing unit property. However, the thief or spy who is harder to detect and who could cause the most damage is the insider - the employee with legitimate access.

PERSONAL FACTORS

There are a variety of motives or situations that may increase the likelihood someone will spy:

Greed or Financial Need: A belief that money can fix anything. Excessive debt or overwhelming expenses.

Anger/Revenge: Disgruntlement to the point of wanting to retaliate against the organization.

Problems at work: A lack of recognition, disagreements with co-workers or managers, dissatisfaction with the job, a pending layoff.

Divided Loyalty: Allegiance to another person or company, or to a country besides the United States.
Adventure/Thrill: Want to add excitement to their life, intrigued by the clandestine activity, “James Bond Wannabe.”

Vulnerability to blackmail: Extra-marital affairs, gambling, fraud.

Ego/Self-image: An “above the rules” attitude, or desire to repair wounds to their self-esteem. Vulnerability to flattery or the promise of a better job. Often coupled with Anger/Revenge or Adventure/Thrill.

PERSONAL FACTORS

Ingratiation: A desire to please or win the approval of someone who could benefit from insider information with the expectation of returned favors.

Family problems: Marital conflicts or separation from loved ones.

Compulsive and destructive behavior: Drug or alcohol abuse, or other addictive behaviors.

BEHAVIORAL INDICATORS

Inappropriately seeks or obtains proprietary or classified information on subjects not related to their work duties.

Interest in matters outside the scope of their duties, particularly those of interest to foreign entities.

Unnecessarily copies material, especially if it is proprietary or classified.

Works odd hours without authorization; notable enthusiasm for overtime work, weekend work, or unusual schedules when clandestine activities could be more easily conducted.

Unreported foreign contacts (particularly with foreign government officials or intelligence officials) or unreported overseas travel.

Unexplained affluence; buys things that they cannot afford on their household income.

YOU CAN MAKE A DIFFERENCE

Organizations need to do their part to deter espionage:






- Educate and regularly train on security or other protocols.
- Ensure that information is adequately protected.
- Routinely monitor computer networks for suspicious activity.
- Ensure security (to include computer network security) personnel have the tools they need.
- Remind employees that reporting security concerns is vital to protecting personnel and information.

Remember if you see something, say something!

REPORTING

If you believe one of you members is committing espionage or is stealing information seek assistance from trained counterintelligence experts. The 2d MAW Counterintelligence Staff Officer can provide security and counterintelligence awareness training for you and your unit upon request. Call (252) 466-2771

Reporting is simple, and methods are available 24/7:

-  Local NCIS Office
-  www.ncis.navy.mil
-  Text “NCIS” + your tip info to CRIMES (274637)
-  “Tip Submit” Android and iPhone App (select NCIS as the agency)
-  1.800.543.NAVY (6289)

Web, text, and smartphone reporting is anonymous.

If you cannot report to NCIS, notify your security officer, supervisor, or command. Per DoDD 5240.06, they are required to notify NCIS within 72 hours.

NCIS may pay rewards up to \$5,000 for information leading to a felony arrest or the prevention of certain felony crimes.

FLIP FOR WORKPLACE VIOLENCE AND TERRORISM INFORMATION