

## Concerning Behaviors

Prompt reporting of suspicious or concerning behaviors can help disrupt an emerging threat, or at least minimize any damage inflicted.

Examples include:

- Breaking security-related rules and norms
- Careless handling, or inappropriate attempts to access or remove classified information
- Suspicious changes in work habits or schedule, inconsistent with operational need
- Unreported foreign contacts or foreign travel
- Signs of divided national loyalty or antagonism toward U.S. policies, interests or values
- High animosity toward other employees, leaders, or the organization itself
- Escalating rage, desperation or suicidality for which the individual will not accept help
- Threatening, aggressive, or very irrational behavior which concerns others
- Apparent sympathy with groups that promote violence as a means of achieving their social, political, or ideological goals

## Your Responsibility - “What to Do”

- Take all threats and threatening gestures seriously
- Understand that even well-regarded individuals can become malicious and destructive in certain circumstances
- Trust your instincts about whether someone might pose a direct or indirect threat to workforce safety and security
- If you are fearful of becoming a target, communicate this to those in charge so that appropriate safety planning can be incorporated

## Reporting Instructions

Promptly report any concern to your immediate supervisor and/or Chief Security Officer.

For any imminent threats or danger, notify FBI police or local authorities.

---

*Need to report a possible insider threat concern?*

Referrals – Send email on your internal FBINET system to:  
HQ-DIV00-INSIDER-THREAT-OFFICE-REFERRALS

*Have a general question about insider threat?*

Questions – Send email on your internal FBINET system to:  
HQ-DIV00-INSIDER-THREAT-OFFICE-COMMUNICATIONS

---



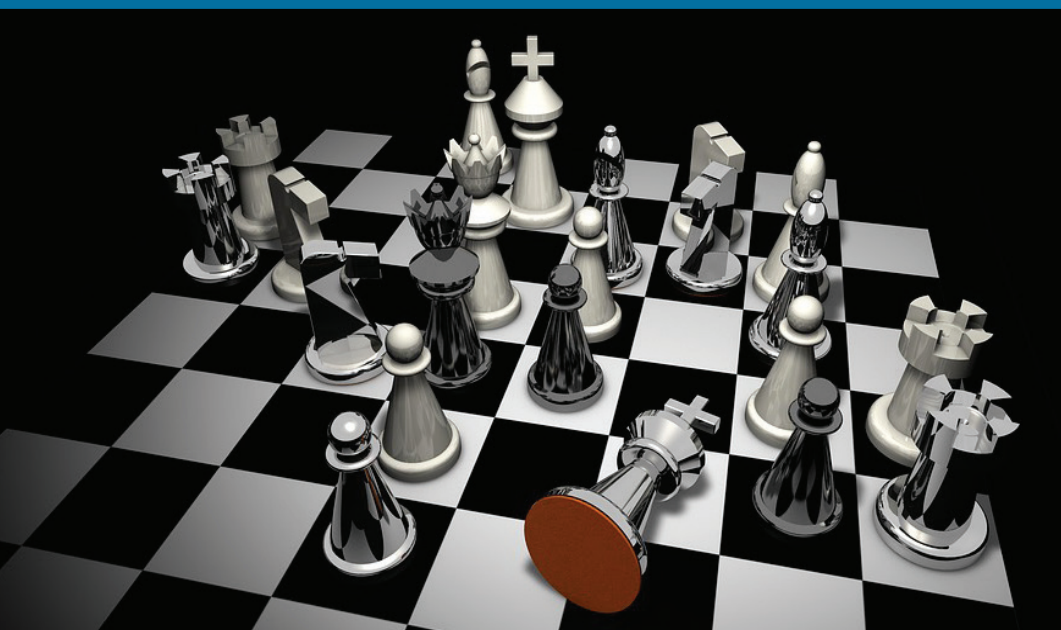
**Insider Threat:**

# You are the First Line of Defense



The FBI's Insider Threat Program consists of the Counterintelligence Division, Security Division, Inspection Division, Human Resources Division, Office of the General Counsel and the Information Technology Branch, with oversight by the FBI Insider Threat Risk Board. The Insider Threat Office provides centralized coordination and focused support to the major program components.

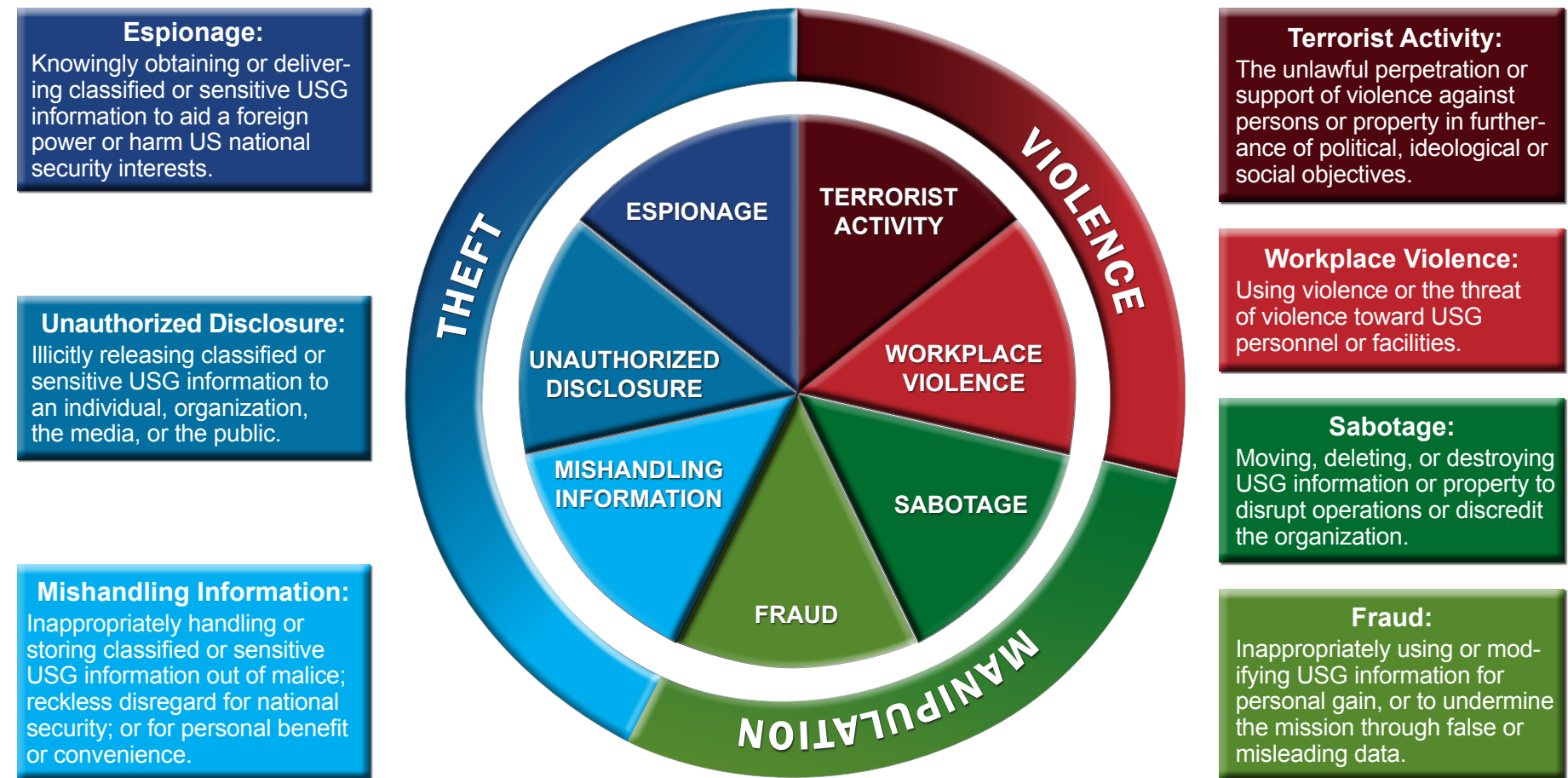
**Insider Threat Definition** - *The threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities. In addition, the FBI has expanded this definition to include workplace violence.*



The expanded FBI definition of intentional insider threat is represented in the "Typology" diagram below. It presents three major "Threat Domains" - generalizable themes of insider threat activity which capture primary concerns for U.S. Government (USG) organizations.

Categorized within the Threat Domains are seven "Threat Impacts" describing specific types of harm to personnel, USG resources or national security.

## FBI Typology of Intentional Insider Threat



This typology represents a synthesis of current academic and professional literature on insider threat, and FBI subject matter expert analysis.