WHAT MOTIVATES AN INSIDER THREAT TO ACT?

SHIFT IN PERSPECTIVE

An intense shift in an individual's viewpoint (a sudden recognition of divided loyalties) begins to make them believe extreme action is required to reinforce or convey their perspective.

PREPARATION FOR ACTION

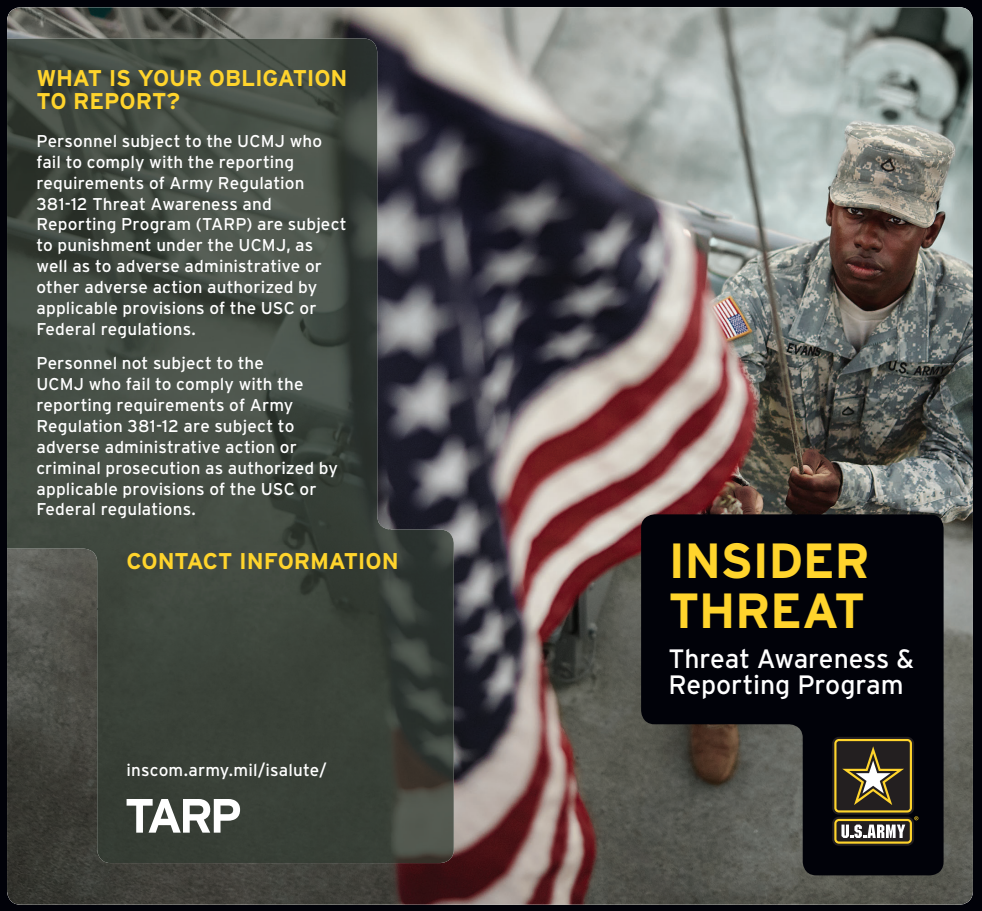
Once an individual begins to believe that extreme action is required, they may prepare to take action by, planning, organizing, training, and obtaining the required materials in preparation to take action against their intended target.

TAKING ACTION

Without intervention or reporting, an individual may progress to committing an extreme act, including an act of espionage, terrorism, or even treason.

REMEMBER

Not every person who experiences a shift in perspective will prepare to take action. Early detection and reporting can deter an INSIDER THREAT.



WHAT IS YOUR OBLIGATION TO REPORT?

Personnel subject to the UCMJ who fail to comply with the reporting requirements of Army Regulation 381-12 Threat Awareness and Reporting Program (TARP) are subject to punishment under the UCMJ, as well as to adverse administrative or other adverse action authorized by applicable provisions of the USC or Federal regulations.

Personnel not subject to the UCMJ who fail to comply with the reporting requirements of Army Regulation 381-12 are subject to adverse administrative action or criminal prosecution as authorized by applicable provisions of the USC or Federal regulations.

CONTACT INFORMATION

inscom.army.mil/isalute/

TARP

INSIDER THREAT

Threat Awareness & Reporting Program

U.S.ARMY

THE INSIDER THREAT IS AN INDIVIDUAL OR GROUP WHO IS INSIDE, GIVEN ACCESS, AND TRUSTED.

The Insider Threat uses his or her access to **wittingly or unwittingly** harm National Security or National Security interests through:

- Unauthorized Disclosure
- Data Modification
- Espionage
- Terrorism
- Subversion
- Sabotage
- Sedition
- Treason

Harm may also include violent actions that result in the loss or degradation of capabilities or resources, to include:

- Personnel
- Facilities
- Information
- Equipment
- Networks or Systems

"EVERYBODY COMES INTO THE MILITARY WITH...POTENTIAL DUAL LOYALTIES...
because people come from different parts of the world...[their dual loyalties] don't really become a problem until they become divided loyalties."

–Dr. Marc Sageman

ESPIONAGE

Intentionally obtaining, delivering, transmitting, communicating, or receiving national defense-related information that may be used either to HARM the United States or to ADVANCE a Foreign Nation.

Report the following espionage indicators to a U.S. Army Counterintelligence Agent:

- Unreported/unusual foreign connections and/or travel
- Undue interest in or soliciting others for information outside the "need to know"
- Unusual work behaviors, to include:
  - Working odd hours
  - Bringing unauthorized devices into secure areas
- Increased dissatisfaction with job, boss, employer
- Unexplained affluence, lavish displays of wealth

TERRORISM

The use of force or violence against persons or property for the purposes of intimidation, coercion, or ransom; promoting fear and the idea an established government is powerless; seeking to gain publicity for a political, religious, or ideological cause.

Report the following terrorism indicators to a U.S. Army Counterintelligence Agent:

- Supporting the unlawful use of force or violence against the DoD or the United States
- Receiving funds from or providing funds to terrorist organizations
- Social networking with, advocating for, or training with terrorist organizations

Place Contact or Business Card Here

CASE STUDIES

WILLIAM C. MILLAY

Convicted of ESPIONAGE, sentenced to 19 years in prison, rank reduction to PVT, pay forfeiture, and dishonorable discharge.

CASEY FURY

Convicted of SABOTAGE of USS Miami, sentenced to 17 years in prison and a $400 million fine.

NIDAL HASAN

Convicted of MURDER as a violent insider threat, sentenced to death.