ARMY **REPORTING PROCEDURES**

Army employees must report potential threats to their organization's Insider Threat Program. Employees may also consult their security office or supervisor. Insider Threat Program personnel will coordinate with security, counterintelligence elements, and law enforcement, as appropriate. For incidents meeting specific thresholds or situations where the organization may not be able to acquire enough information to make a decision, reports to the U.S. Army Insider Threat Operations (Hub) may be required. Employees may also have additional reporting requirements under counterintelligence and security policies.

CLEARED CONTRACTOR **REPORTING PROCEDURES**

Employees of cleared industry must report potential threats to the facility Insider Threat Program Senior Official (ITPSO) or Facility Security Officer (FSO). Depending on the situation, the FSO and ITPSO will report the possible threat to the Defense Counterintelligence and Security Agency (DCSA) Industrial Security Representative, DCSA Counterintelligence Special Agent. The FBI is notified if the situation involves known or suspected espionage. Information related to the Adjudicative Guidelines and other reportable behaviors must also be reported per National Industrial Security Program Operating Manual (NISPOM) 102(a-b).

MITIGATION

The number one priority for any organization should be personnel readiness and mission accomplishment. Derogatory actions by a trusted workforce can have a negative impact on both of these priorities. Insider threat is a "people problem" and requires both an individual and organizational focus to effectively identify and mitigate identified issues. Nothing can replace the early recognition of concerning behaviors or personal warning signs, and nothing is more effective at preventing and mitigating insider threats than first rate leadership and management of subordinates. This includes genuine concern for employee well-being and fairness when addressing problem work behavior and mitigating insider threats.

COMMAND **REQUEST FOR ASSISTANCE** (RFA)

An RFA can be made to the Hub if it is reasonable to conclude that an individual, based on identified indicators (see InT Desk Reference Guide, OCT 19) may be a threat to classified systems or data, personnel or resources, or has the potential to engage in violent activity targeting DoD-affiliated personnel or resources.

The RFA process is as follows:

1. Potential Insider Threat is identified through the organization developed process (e.g., Individual Report, CMD Request, Result of PAR, Protection Working Group, etc.).
2. Referral Authority packages the RFA and submits to the InT Hub (sample Referral in InT Desk Reference Guide, OCT 19).
    - Encrypted submission via NIPR: usarmy.pentagon.hqda-dcs-g-3-5-7.mbx.g-34-int-hub-reports-cell@mail.mil
    - Classified submission via SIPR: usarmy.pentagon.hqda-dcs-g-3-5-7.mbx.g-34-int-hub-reports-cell@mail.smil.mil
3. InT Hub receives the report, triages report, determines InT nexus, and begins processing and collation.
4. InT Hub may need to reach back to Referral Authority for additional unit information on subject.
5. A referred report can take 5 to15 days.
    - Mitigation Recommendations are sent to the Referral Authority once the InT Hub Process is completed
    - Commands develop internal dissemination plans
    - Commanders make final decision on actions
    - Report of action taken is required to the Hub for Case Review Determination

U.S. ARMY INSIDER THREAT OPERATIONS (HUB)

400 ARMY PENTAGON

WASHINGTON, DC 20310

COMMAND
Insider Threat
OPERATIONS

Insider Threat OPERATIONS HUB

INSIDER

"A person who has or had been granted eligibility for access to classified information or eligibility to hold a sensitive position. These individuals include Active and Reserve Component (including National Guard) military personnel, civilian employees (including non-appropriated fund employees), and DoD contractor personnel; this includes officials or employees from federal, State, local, tribal and private sector entities affiliated with or working with DoD who have been granted access to classified information by DoD based on an eligibility determination made by DoD or by another federal agency authorized to do so."

INSIDER THREAT

"The threat insiders may pose to DoD and U.S. Government installations, facilities, personnel, missions, or resources. 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."

DoD Directive 5205.16, "The DoD Insider Threat Program," Incorporating Change 2, August 28,2017

Malicious Insider	Disgruntled or angry current or former employees, contractors or business partners that gain access to an organization's network resources, system or data and release this information without permission by the organization.
Violent Insider	Employees who have violent predispositions, stressors, grievances, or ideation who view a member(s) of an organization as the reason for their anger and seek retribution through violence.
Exploited Insider	Employees in this category have an exploitable vulnerability (ego, debt, addiction) and are targeted by external entities or organization. This can occur through phishing, blackmail, or bribery to gain a foothold inside an organization or obtain classified materials.
Negligent Insider	Careless / Complacent employees whose poor security habits too often put systems and offices at risk. Employees of this type may also believe that they are not a risk or that the security rules do not pertain to them.
External Insider	Contractors, Consultants, or Temps who have granted access and are trusted; and, unlike traditional insiders, external insiders are not subjected to as many internal controls enforced by the organization.

PRINCIPLES OF INSIDER THREAT

Insider threat principles represent the characteristics of successful insider threat integration and synchronization within Army operations and strategy. These principles allow the force to protect itself from actions by a perceived trusted workforce that can negatively impact the total range of Army services, programs, and operations.

RISK. The potential for an insider who uses his or her authorized access, wittingly or unwittingly, to do harm to Army assets and the security of the United States.

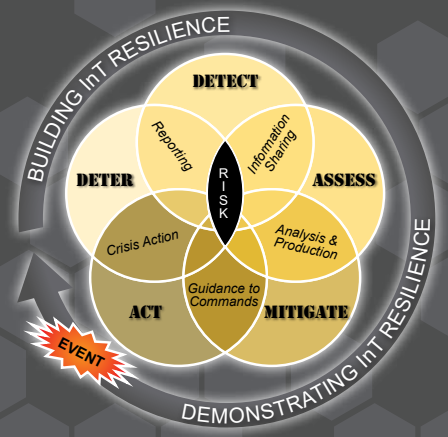
DETER. The delivery of training, awareness, visible security measures, and monitoring to discourage and report malicious and negligent acts. This includes clear organizational policies and procedures enforced consistently and fairly.

DETECT. Identify, discover or locate the potential for sabotage, espionage, unauthorized disclosure, theft or violent insider acts through active and passive measures.

ASSESS. Assessment is the method of evaluating and monitoring indicators and determining if there is an insider threat nexus and/or movement along a Critical Path.

MITIGATE. Reduce risk to Army assets and classified national security information while protecting the privacy, civil rights, and civil liberties of Army personnel.

ACT. Commander's action takes many forms, to include (1) making a referral, (2) making recommendations to behavioral health and other support programs, (3) implementing force protection measures, (4) or taking disciplinary action when a mitigation strategy is deficient in changing behavior.



BEHAVIOR REPORTING
EVERY SOLDIER IS A SENSOR

Leadership/Supervisor: Providing a safe work environment is essential to daily operations and is a responsibility that falls on each of us. Suspicious activity that should be discussed with a leader is any observed behavior either overt or implied, to commit an act of physical aggression, sabotage or theft of resources, or violations of security protocols and handling of classified information. If a supervisor becomes aware of an arrest or incident that falls within one of the thirteen adjudicative guidelines involving a cleared member of their organization they are required to ensure that the activity is reported through their security.

iWATCH Army: iWATCH Army encourages and empowers the Army community to identify and report suspicious behavior potentially associated with terrorist activity. iWATCH Army is a program and partnership between the community and the local Military Police and civilian law enforcement. Any member of the Army community can report behaviors and activities that make him or her feel uncomfortable and do not look right (suspicious behaviors).

iSALUTE: If related to espionage, sabotage, subversion, and international terrorism report using iSALUTE, which is the Army counterintelligence-reporting program. iSALUTE supports the Army's counterintelligence policy established in AR 381-12, Threat Awareness and Reporting Program (TARP) and seeks Army-wide community support to report threat incidents, behavioral indicators, and counterintelligence matters that are potential indicators of espionage, terrorist-associated insider threat, and extremist activity. iSALUTE website: https://www.inscom.army.mil/isalute/

Continuous Evaluation (CE): CE is a vetting process to review the background of an individual who has been determined to be eligible for access to classified information or to hold a sensitive position at any time during the period of eligibility. CE leverages a set of automated record checks and business rules to assist in the on-going assessment of an individual's continued eligibility.