

# Marine Corps Counter-Insider Threat Program



In recent years we've learned the devastating impact that malicious insiders can achieve against the organizations to which they belong through acts of espionage, sabotage, and targeted violence.



## What is an insider threat?

Any person who has authorized access to US government re-sources to include personnel, facilities, information, equipment, networks, or systems

AND

uses his/her authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat includes potential espionage, violent acts against the Government or the Nation including terrorism, unauthorized disclosure of national security information, or the loss or degradation of depart-mental resources or capabilities.

The Marine Corps Counter-Insider Threat Program (MCCINTP) is charged with preventing, detecting, deterring, and mitigating threats posed by malicious insiders to Marine Corps Personnel, Resources, and Mission Readiness.

The MCCInTP employs a robust analytic capability to identify, analyze, and act upon insider threat information in a manner that maintains continuous compliance with applicable **Privacy, Civil Liberties, and Whistle Blower Protections.**

The cornerstone of the Program is its analytic capability which resides within the Program Hub.

The Program Hub is comprised of a team of certified Insider Threat Analysts and Subject Matter Experts representing fields such as LE, CI, Cyber, HR and behavioral health.

This multi-disciplinary team works diligently to identify Marine Corps personnel that may be exhibiting **Potential Risk Indicators.**

Once identified, the Program works with the individual's Chain of Command to develop a Risk Mitigation Strategy to resolve the issue(s) and optimally assist that Marine, civilian, or contractor find their way back to being a trusted member of the Marine Corps team.

## This is a Team Effort

Preventing an insider from committing a malicious act and bringing them back into alignment with our Corps Values of Honor, Courage, and Commitment is the Program's primary objective.

This objective cannot be fully achieved without the willingness of every Marine, civilian employee, and contractor to seek assistance when they identify someone that appears to be trending towards becoming an insider threat.

## What to look for

Case studies indicate individuals at risk of being insider threats exhibit patterns of behavior prior to committing malicious acts. These **Potential Risk Indicators (PRI)** include a wide range of personal predispositions, stressors, choices, actions, and behaviors.

PRIs are not a "checklist" for predicting behavior. Insider Threat is a complex human problem. Not all PRIs will be evident in every situation and not everyone that exhibits these behaviors is doing something wrong.

PRIs are "clues" that require critical thought and analytic reasoning to interpret. **The sooner our Program can apply those principles the better our chances of success become.**

The Center for the Development of Security Excellence (CDSE) recognizes (9) PRI categories. This is not an all-inclusive list, only a sampling. A detailed list can be found at:

[https://www.cdse.edu/Portals/124/Documents/job\\_aids/insider/INTJ0181-insider-threat-indicators-job-aid.pdf](https://www.cdse.edu/Portals/124/Documents/job_aids/insider/INTJ0181-insider-threat-indicators-job-aid.pdf)

## PRI Categories & Examples

- 1. Access Attributes:** Has access to sensitive systems, information, facilities, and/or weapons and explosives
- 2. Professional Lifecycle and Performance:** Recently received NJP/formal reprimand; demonstrated decline in work performance; pending involuntary separation or termination.
- 3. Foreign Considerations:** Frequent or unexplained foreign travel; possesses a foreign passport; has foreign political or financial interest.
- 4. Security and Compliance Incidents:** Frequent security infractions/violations; accessing systems during off-hours; virtual access anomalies.
- 5. Technical Activity:** Suspicious emails; burning disc; data transfer to personal/suspicious account; disabling anti-virus or firewall settings.
- 6. Criminal, Violent, or Abusive Conduct:** Vocalizing threats; possessing unauthorized weapons; criminal affiliations: bullying or harassment.
- 7. Financial Considerations:** Loan default; foreclosures; filing for bankruptcy; unexplained affluence or change in financial status.
- 8. Substance Abuse and Addictive Behaviors:** Drug test failure, possession of illegal substance at work; substantiated report or drug related arrest.
- 9. Judgement, Character, and Psychological Conditions:** Falsifying hiring information, association with extremist organizations; anti-social behavior or mental instability.

## Doing Your Part

Preventing insider threat events from occurring starts with the Marine standing duty in the barracks, the civilian employee working at the exchange, or the contractor providing support at the motor pool. These people have the greatest insight into the individual well-being of the people that serve along side them day in and day out.

If you have observed behaviors, such as those outlined in the CDSE's PRI categories, or you're simply concerned about a recent change in a friend or coworker's behavior seek assistance immediately.

## Obtaining Assistance

- If there are signs that an insider threat incident is imminent, a crime has already occurred, or if you have dire concerns for your safety or the safety of others, **contact law enforcement immediately.**
- For non-imminent threats notify your Chain of Command, Command Security Manager, or designated Insider Threat Liaison.
- Personnel working in an independent duty status can obtain assistance through the nearest available Security Manager, Contracting Officer Representative, or Facility Security Officer.
- In situations where none of the options listed above are available or you don't feel comfortable with utilizing them, assistance may be obtained directly from the MCCInTP by sending an email to:

[insidethreat@usmc.mil](mailto:insidethreat@usmc.mil)

Insider Threat concerns can also be reported anonymously using the following web-based applications:

### NCIS TextTip

<https://www.ncis.navy.mil/Resources/NCIS-Tips/>

### Eagle Eyes

[www.usmceagleeyes.org](http://www.usmceagleeyes.org)

## Learn More

Countering Insider Threat is a complex problem; therefore, the more you know the better equipped you will be to contribute to this effort.

All Marine Corps personnel (active and reserve Marines, DoD Civilian Employees, and Contractors) are strongly encouraged to take advantage of the education opportunities supporting Counter Insider Threat offered by the Center for the Development of Security Excellence at:

<https://www.cdse.edu/Training/Insider-Threat/>

For information pertaining to the laws, authorities, and nationally mandated Program requirements visit:

<https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf>

September is **National Insider Threat Awareness Month**. Guidance on how to participate and a listing of Counter Insider Threat events and educational opportunities is published each August via Marine Corps Administrative Message.