DITMAC

AUGUST 2025

NITAM NOTES

THREAT ASSESSMENT & THREAT MANAGEMENT (TATM)

TATM CONTRIBUTIONS

TATM is a multidisciplinary and systematic approach to identify potential risks/threats and determine mitigation strategies to best protect the organization as well as support the individual when possible. By proactively addressing behaviors of concerns, organizations can better protect their assets, resources and personnel.

BARRIERS & CHALLENGES

A Lack of Cross-Functional Collaboration

- Siloed communication and data due to misunderstanding about national security standards and expectation for data sharing
- Overly cautious interpretations of legal standards or risk appetite by leadership, can hinder timely intervention risking escalation

Challenges with Staffing and Resources

- Organizations and/or local partners may not have the resources or personnel to establish a full-time threat management team
- Many organizations do not have mature threat management programs and rely on law enforcement or security resources that limit perspective on insider threat mitigation and lead to reactive processes

CASE SUPPORT

- TATM evaluates indicators to distinguish credible threats from non-credible threats. While TATM is traditionally used to identify and mitigate threats of violence, the same principles can be applied to all types of InT
- External partnerships with law enforcement, mental health advisors, legal advisors, and employee management
- Privacy compliant information sharing: Threat Management Teams are authorized to share information under federal law when a credible threat exists identified

BUILDING STRONGER PARTNERSHIPS

- Partner with TATM professionals that support other agencies, departments, or organizations to amplify expertise as well as reach in other geographical areas
- Coordinate a meet and greet to introduce the teams, share missions and available resources, and conduct tabletop exercises
- Establishing relationships before a crisis expedites communications in the moment and allows InT to more quickly address potential threats when identified
- Leveraging national level professional organizations in the threat/violence prevention, and cleared industry security gives InT programs access to partners with these available resources, as well as an ability to stay up to date on the latest research in the field of risk/threat prevention
- To facilitate information sharing, organizations should clearly identify legal boundaries and privacy regulations to maximize proactive threat identification while preserving an individual's rights

KEY CONTRIBUTIONS

DETER

- Proactive support from leadership encourages a positive organizational culture and morale
- Develop awareness training for organizational stakeholders that focuses on the expanded DoD definition of Insider Threats

DETECT

- Offer training on potential risk indicators and bystander reporting as they relate to InT, to increase information as identification of behaviors of concerns
- Coordinating multidisciplinary teams across stakeholders (i.e. cyber, LE/CI, HR) informs holistic threat detection methods using TATM principles and best practices

MITIGATE

- Coordinating initial multi domain mitigation plans with stakeholders and managing ongoing risk through periodic follow up and case tracking
- Including a full range of resources gives InT a full scope view of the individual, potential risks, and opportunities for mitigation