

Insider Threat Assessment and Mitigation

Objective: Gather, integrate, review, assess, and respond to information derived from multiple sources (e.g., CI, Security, Cybersecurity, Human Resources/Personnel Management, Behavioral Science, Legal, LE, and UAM) to identify and mitigate insider threats.

	1	2	3	4	5	6	7
	Define Requirements, approach, & resources	Identify and gather needed inputs	Prepare inputs and the environment	Execute core activities to produce intended results	Monitor Environment and Results	Adjust Products, Services, & Processes	Finish or Conclude the job
A	Describe Requirements of a Insider Threat Hub Regarding its Structure, Mission, Capability, Resources, & Policies	Monitor & Track Data Feeds for Anomalous Behaviors (e.g., UAM, Tip Lines, Walk-ins)	Validate Data to Ensure Quality and Applicability to the Inquiry	Evaluate, Integrate, Analyze, & Interpret all Data Against Local and/or DITMAC Reporting Threshold(s)	Participate in Local and External Reviews/Lessons Learned (e.g., Audits, AARs, Insider Threat-WGs, AMCOP, etc.) in Order to Assess Triggers, Redress Policies, and Follow Up		
B	Describe Requirements for Local & DITMAC Reporting Thresholds & Procedures for Information Sharing	Review Referrals & Reports of Anomalous Behavior(s) and/or Insider Threat Events Which Already Occurred But Were Not Being Tracked	Compile Data Obtained from Multiple Data Sources (e.g., Security, CI, UAM, etc.)	Coordinate with and Report to the DITMAC on all IgT-Related Anomalies, Events, and Mitigation Actions Taken if DITMAC Reporting Threshold(s) Were Met			Follow Established Policies and Procedures for Closing an Inquiry
C	Describe the Capabilities and Reporting Streams of Each of the Pillars	Validate that Referred/Reported Behavior(s) Events Meet Local and/or DITMAC Reporting Threshold(s)	Document any Information Gaps Identified During Data Aggregation & Identify Possible Courses of Action	Support the Insider Threat Hub in Facilitating and Monitoring an Appropriate Mitigation Strategy with all Relevant Stakeholders as required			
D		Access, Search, Query, and/or Monitor Relevant Data Feeds for Additional Relevant Information		Generate Report(s) of Assessment Results			
E		Consult with and/or Submit RFIs to the DITMAC or Other External Functional SMEs about Anomalous Behavior(s) or to Address Information Gaps about a Subject of Interest		Review Assessment Report(s) with Legal, the Appropriate Senior Leaders, and Stakeholders			