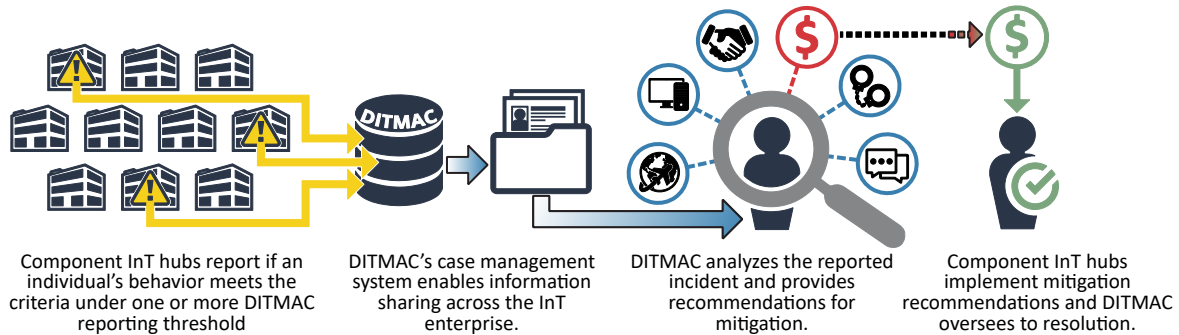




DOD INSIDER THREAT MANAGEMENT & ANALYSIS CENTER (DITMAC)

The DOD Insider Threat Management and Analysis Center, or DITMAC, was created as a result of the tragic shootings at the Washington Navy Yard. DITMAC's mission is to provide the DOD enterprise a capability to identify, assess and mitigate risk from insiders, to oversee and manage unauthorized disclosures, and to integrate, manage, mature and professionalize Insider Threat (InT) capabilities.



DITMAC Operations

Analysis and Mitigation (A&M) - provides the capability to consolidate and share information necessary to identify potential insider threats, develop a holistic picture of risk posed by insiders, and coordinate actions to mitigate risk across the Department.

Behavioral Threat Analysis Center (BTAC) - provides tailored InT case-specific recommendations in behavioral science, threat management, cyber, counterintelligence, law enforcement, and human resources.

Prevention, Assistance, Response (PAR) - InT support and coordination at the installation level primarily focused on preventing acts of workplace violence.

What is an insider threat? Anyone with authorized access who poses a risk to U.S. Government installations, facilities, personnel, missions, and/or resources.

How do I report an insider threat? DOD personnel should report potential insider threats via their Component Insider Threat Program.

DITMAC Enterprise Program Management

Assessments & Professionalization (A&P) - conducts assessments for both compliance, and efficiency and effectiveness, against InT program standards and maturity frameworks; supports InT career professionalization and associated certifications.

Mission Integration Office (MIO) - supports Enterprise User Activity Monitoring (UAM) efforts and integrates Publicly Available Information (PAI) into InT analytic products to contextualize risk.

Performance, Requirements, Information, Standards, and Metrics (PRISM) - provides key performance indicators and measures of effectiveness as well as oversees the development of requirements-based IT solutions for DITMAC and the broader DOD InT Enterprise.

Unauthorized Disclosure Program Management Office (UD PMO) - provides management and operational capability to improve identification, reporting, tracking, and mitigation of unauthorized disclosures.