# *DOD Insider Threat Management Analysis Center (DITMAC) Short*

## Student Guide

December 2023

*Center for Development of Security Excellence*

# Contents

# Introduction

Once a critical gap in security programs, insider threat detection has evolved from reactive methods to more proactive approaches by placing emphasis on risk prevention and mitigation before someone becomes a threat. Today, the Department of Defense, or DOD, Insider Threat Program aims to help trusted persons with authorized access to get on the right path—as opposed to continuing down a critical path, either wittingly or unwittingly, to commit espionage, sabotage, data exfiltration, unauthorized disclosure of national security information, or workplace violence.

Welcome to CDSE's Short on the DOD Insider Threat Management Analysis Center (DITMAC). This Short will cover the critical important part the DITMAC plays in offering a broader perspective and the tools needed to help leaders make the best risk-based decisions for their organizations.

# DITMAC Authorities

*[Newscaster] Aaron Alexis shot and killed 12 people last year at the Washington Navy Yard in Southeast Washington, DC. Alexis used a valid, temporary ID to get into building 197. Police eventually shot and killed him. —CBS This Morning*

DITMAC was created as a result of the tragic shootings at the Washington Navy Yard and Fort Hood to serve as a catalyst for information sharing and collaborative insider threat management. DITMAC's authorities stem from policies, regulations, and guidance enacted to combat the Insider Threat—specifically, the Washington Navy Yard Implementation Plan, the December 12, 2014, OUSD(I&S) DITMAC Memorandum, and the DODD 5205.16: DOD Insider Threat Program.

# DITMAC Functional Areas

The DITMAC provides the DOD enterprise with a capability to identify, assess, and mitigate risk from insiders; to oversee and manage unauthorized disclosures; and to integrate, manage, and professionalize insider threat capabilities. In this role, DITMAC supports 43 DOD Components and their 45 insider threat hubs by employing analysts and experts to operate within the functional areas that follow.

## *Analysis and Mitigation (A&M)*

- Receive reports from component insider threat hubs
- Triage and conduct analysis
- Information subject-matter consultations
- Provide analytic assessments with risk mitigation strategies
- Support expert consultations
- Oversee and track risk-mitigating actions

## *Behavioral Threat Analysis Center (BTAC)*

- Deliver subject-matter expertise to contextualize risk-based behaviors
- Support PAR Coordinators and Analysis & Mitigation
- Develop structured judgement tools to evaluate risk

- Provide training to PAR Coordinators

### *Enterprise Program Management Office (EPMO)*

- Enhance and mature DOD Component insider threat programs
- Assess DOD component compliance with national minimum standards
- Foster professionalization and certifications efforts

### *Prevention, Assistance, & Response (PAR)*

- Coordinate installation-level activities with leaders and functional experts
- Reach-back to inform risk-based decisions for Commanders
- Provide training on risk indicators at installation level

### *Performance, Reporting Information, Standards, & Metrics (PRISM)*

- Evaluate case management systems requirements
- Foster innovation and collaboration
- Tell the insider threat story through data and advanced metrics
- Improve reporting capabilities

### *User Activity Monitoring & Publicly Available Electronic Information (UAM & PAEI)*

- Design and execute program to conduct monitoring on NIPRNet
- Manage centralized capability for participating components
- Support governance of broader UAM program
- Integrate PAEI information into products to further contextualize behavior

### *Unauthorized Disclosure Program Management Office (UDPMO)*

- Coordinate reporting of unauthorized disclosures to the Department of Justice (DOJ)
- Support reporting entities in evaluation of information
- Facilitate the reporting of unauthorized disclosures to the DOJ
- Promote collaboration and information sharing across the DOD and Intelligence Community (IC)

# Role of DITMAC

DITMAC informs leadership, senior management, and first-line supervisors about risk indicators and encourages vigilance of concerning behaviors and active engagement with their workforce. DITMAC also emphasizes the importance for leaders to provide their workforce with training, resources, and assistive networks to help mitigate risk within their organizations. To this end, DITMAC supports the 43 DOD Components by analyzing threats and issues as they occur, promoting best practices, strengthening collaboration and information sharing among Departmental elements, and identifying and helping address risk at both the individual and organizational levels.

# DITMAC Support of Components

To holistically address the risks associated with the insider threat demands an enterprise approach that is highly collaborative. The DITMAC provides critical support to Component insider threat programs in their execution of the Minimum Standards for Executive Branch Insider Threat Programs. Components submit insider threat matters to the DITMAC when incidents meet specific reporting thresholds. There are 13 DITMAC reporting thresholds.

DITMAC will:

- Play a parallel and complementary role with the Component in the handling of specific incidents;
- Leverage multiple analytic disciplines and relevant insider threat data;
- Generate findings and risk assessments; and
- Provide recommendations for Components to mitigate the insider threat.

DITMAC will NOT supersede or run the DOD Component Insider Threat programs. Continue to report insider threat issues to your security office or insider threat office. Only the DOD Component Insider Threat Programs will report to DITMAC.

DITMAC will also NOT:

- Take action against or direct Components to take action against its people;
- Allow analysis to be dominated by a single discipline; or
- Set insider threat policy.

## *Minimum Standards*

The November 2012 Minimum Standards established requirements for Executive Branch Insider Threat Programs. These requirements have been reiterated in DODD 5205.16. Executive Branch Insider Threat Programs will—

- Designate a senior official responsible for the Insider Threat (InT) Program
- Obtain visible support from the agency head
- Form a working group/provide periodic feedback to the Community

- Review current requirements and guidance
- Seek legal input
- Protect privacy and civil liberties by applying appropriate safeguards
- Identify classified and other critical assets
- Write agency policy and implementation plan
- Obtain approval
- Establish Program Office
- Implement plan
- Conduct scheduled self-assessments
- Conduct Insider Threat Training for cleared personnel and Insider Threat Program personnel

### *Reporting Thresholds*

The 13 DITMAC Reporting Thresholds are as follows:

- Threshold 1: Serious Threat
- Threshold 2: Allegiance to the United States
- Threshold 3: Espionage/Foreign Consideration
- Threshold 4: Personal Conduct
- Threshold 5: Behavioral Considerations
- Threshold 6: Criminal Conduct
- Threshold 7: Unauthorized Disclosure
- Threshold 8: Unexplained Personal Disappearance
- Threshold 9: Handling Protected Information
- Threshold 10: Misuse of Information Technology
- Threshold 11: Terrorism
- Threshold 12: Criminal Affiliation
- Threshold 13: Adverse Clearance Actions

## DITMAC System of Systems

In support of DITMAC's functions, the DITMAC System of Systems (DSoS) is an enterprise capability that provides workflow management and enables the aggregation of relevant data and leveraging of advanced analytic tools. It serves as a single repository and case management system for insider threat information and enables information reporting, sharing, collaboration, analysis, escalation, and risk mitigation.

DITMAC receives insider threat incidents from the Component Hubs electronically through the DSoS, which is accessed through a Web portal on SIPRNet or JWICS. When the DSoS receives reported information, it correlates it with additional data sources and historical information. It then provides a mechanism to refer recommendations for action, synchronize responses, and oversee resolution of identified issues. DSoS ensures technical protections for the security and privacy of collected data.

## Employee Privacy and Civil Liberties

The Department of Defense is required to take a proactive approach to insider threat to ensure the safety and security of DOD assets, while at the same time protecting everyone's privacy. Keeping the balance right is central to what DITMAC does.

DITMAC only collects information from lawful sources and in full compliance with privacy and civil liberty protections, and does NOT collect people's personal emails or authorized personal use of government computers. This is NOT about identifying bad employees based on a single event or behavior. Instead DITMAC looks at combinations of behaviors that indicate an emerging threat and works to prevent that threat from being realized.

## Summary

Today's threat landscape demands a proactive approach to aggregating information and identifying the kinds of behaviors that indicate risk prior to them becoming attacks and crimes.

Consistent reporting to DITMAC provides the DOD a centralized capability to detect, deter, and mitigate insider threats and reduce harm to the United States and the DOD caused by malicious insiders. DITMAC enables DOD and its Components to meet this vital imperative.

For additional training, job aids, and resources on the insider threat, visit www.cdse.edu.