DoD Insider Threat Management Analysis Center (DITMAC) Short

Student Guide

August 2016

Center for Development of Security Excellence

DITMAC Short

Introduction

"The reviews identified troubling gaps in DoD's ability to detect, prevent, and respond to instances where someone working for us, a government employee, a member of our military, or a contractor, decides to inflict harm on this institution and its people…"

- Former Secretary of Defense Chuck Hagel, March 18, 2014

The insider threat is one of the most significant security challenges faced by the Department of Defense. "Someone" – one trusted person with authorized physical or logical access to DoD facilities or information systems can, wittingly or unwittingly, cause grave damage to our nation through espionage, terrorism, unauthorized disclosure of national security information, or the loss or degradation of departmental resources or capabilities. Welcome to CDSE's Short on the DoD Insider Threat Management Analysis Center, or DITMAC, which will cover DITMAC's role in the DoD Insider Threat Program.

The objective for this Short is to recognize the role of the DoD Insider Threat Management Analysis Center.

What Is DITMAC?

"Increasingly, threats—cyber, kinetic, all threats—they're inside the perimeter. What the Department of Defense should do is build security from within."

- Former Assistant Secretary of Defense Paul Stockton, March 18, 2014

DITMAC was established in the wake of the Washington Navy Yard shooting and other recent insider threat incidents to serve as a catalyst for information sharing and collaborative insider defense. 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) DITMAC Memorandum, and the DoDD 5205.16: DoD Insider Threat Program.

The DITMAC is an enterprise capability that leverages relevant data, a multidisciplinary team of analysts and experts; research, analysis, and risk assessment; and enabling tools and technologies to build an enterprise view of Insider Threat issues across the Department and in support of the DoD Components.

Role of DITMAC

"The DITMAC is a Department-wide initiative whose mission is to bridge the gaps that are exploitable by an insider in order to detect and deter threats."

- Director of DSS Daniel Payne

DITMAC focuses on detecting and responding to behaviors indicative of a potential insider threat. DITMAC informs DoD leaders and the Components to oversee threat mitigation, prepare risk assessments and recommendations, synchronize responses to potential threats, and enable sharing of relevant information. 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 systemic insider threat issues.

DITMAC Support Components

"The DITMAC will enable DoD to take a holistic look at systemic Insider Threat issues across all DoD Components and facilitate information sharing and collaboration. …to be effective, the DITMAC must rely an integrated approach that begins with each of you at the Component level… to prevent the insider from doing harm."

- Director of DSS Daniel Payne

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 November 2012 Minimum Standards for Executive Branch Insider Threat Programs. The Components 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

These requirements have been reiterated in DoDD 5205.16.

Components submit insider threat matters to the DITMAC when incidents meet specific reporting thresholds. Because the threat is dynamic, thresholds will evolve over time.

DITMAC will establish specific reporting requirements for the Components along with a format for submitting these potential risk indicators; 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. In support of DITMAC's functions, the DITMAC System of Systems, or DSoS, is as an enterprise capability that provides workflow management and enables the aggregation of relevant data and leveraging of advanced analytic tools.

Employee Privacy and Civil Liberties

"From its inception the DITMAC has been structured with robust checks and balances to ensure the civil liberties and privacy of DoD employees are protected at all times."

- Director of DSS Daniel Payne

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's goal is to detect insider threats before they do harm—that is, to deter individuals from becoming bad actors and help them if there is a problem.

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

"In my 50+ years in the intelligence business, I cannot recall a more diverse array of challenges and crises that we confront as we do today."

- Director of National Intelligence James Clapper

We cannot wait to defend ourselves from insiders intending to do us harm. The threat demands a proactive approach to aggregating information and identifying the kinds of behaviors that indicate risk prior to them becoming attacks and crimes. DITMAC will enable DoD and its

Components to meet this vital imperative. By working together, we can mitigate the risks associated with the insider threat. Visit the DITMAC website (http://www.dss.mil/about_dss/ditmac.html) for more information, and access additional training, job aids, and resources on the insider threat at www.cdse.edu.