



DoD INSTRUCTION 5205.83

DoD INSIDER THREAT MANAGEMENT AND ANALYSIS CENTER (DITMAC)

Originating Component: Office of the Under Secretary of Defense for Intelligence

Effective: March 30, 2017

Releasability: Cleared for public release. Available on the Internet from the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.

Incorporates and Cancels: Under Secretary of Defense for Intelligence Memorandum, "Incubation of the DoD Insider Threat Management and Analysis Center," December 12, 2014

Approved by: Todd R. Lowery, Performing the Duties of the Under Secretary of Defense for Intelligence

Purpose: In accordance with the authority in DoD Directives 5143.01 and 5205.16, this issuance:

- Establishes policy, assigns responsibilities, and prescribes procedures for the DITMAC, which serves as the DoD's enterprise-level capability for insider threat information integration and management.
- Provides for the establishment and operation of an automation-assisted enterprise-level capability for managing and analyzing insider threat information across the law enforcement, personnel security, human resources, counterintelligence, physical security, network behavior monitoring, and cybersecurity activities of all the components of the Department of Defense, pursuant to Executive Order 13587.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION	3
1.1. Applicability.	3
1.2. Policy.	3
SECTION 2: RESPONSIBILITIES	4
2.1. Under Secretary of Defense for Intelligence (USD(I)).....	4
2.2. Director, Defense Security Service (DSS).....	4
2.3. Director, Defense Intelligence Agency (DIA).....	5
2.4. Director, Defense Manpower Data Center (DMDC).....	5
2.5. DoD CIO.....	5
2.6. Director, Defense Information Systems Agency (DISA).	5
2.7. DoD Component Heads.	6
SECTION 3: DITMAC FUNCTIONS AND OPERATIONS.....	7
3.1. General.....	7
3.2. Director, DITMAC.	7
GLOSSARY	9
G.1. Acronyms.....	9
G.2. Definitions.....	9
REFERENCES	10

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This issuance applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the National Guard Bureau, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the “DoD Components”).

1.2. POLICY. The DITMAC:

a. Establishes and operates an automation-assisted enterprise-level capability for managing and analyzing insider threat information across the law enforcement, personnel security, human resources, counterintelligence, physical security, network behavior monitoring, and cybersecurity activities of all the components of the Department of Defense, pursuant to Executive Order 13587.

b. In accordance with Executive Order 13587 and DoD Directive 5205.16, integrates and centrally analyzes key threat-related information on the threat that insiders may pose to DoD and U.S. Government installations, facilities, personnel, missions, or resources; including damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

c. Will operate with the support of experts in counterintelligence, personnel security, law enforcement, human resources, physical security, network monitoring, cybersecurity, and privacy and civil liberties, and experts in information technology, large-scale data analysis, systems engineering, and program acquisition.

d. Will operate at all times in compliance with all applicable laws, Executive Orders, regulations and DoD policy issuances, including those regarding whistleblower, civil liberties, and privacy protections.

SECTION 2: RESPONSIBILITIES

2.1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I), as the senior official and principal civilian advisor to the Secretary of Defense on the DoD Insider Threat Program develops policy and guidance governing the DoD Insider Threat Program and directs and facilitates the establishment of the DITMAC.

2.2. DIRECTOR, DEFENSE SECURITY SERVICE (DSS). Under the authority, direction, and control of the USD(I) and in addition to the responsibilities in Paragraph 2.7, the Director, DSS:

a. Establishes the operation of the DITMAC to:

- (1) Oversee the mitigation of insider threats as set forth in Paragraph 1.2.b.
- (2) Assess enterprise-level risks, refer recommendations for action, synchronize responses, and oversee resolution of identified issues on the insider threats listed in Paragraph 1.2.b.
- (3) Develop enterprise-level risk criteria (thresholds) to facilitate Component reporting of potential threat information and assess the effectiveness of actions taken by Components to address, mitigate, or resolve insider threats as set forth in Paragraph 1.2.b.
- (4) Support the Office of the USD(I) in establishing standards to ensure that the DoD Insider Threat Program complies with applicable statutes, Executive Orders, and other National and DoD regulations and policies that specify insider threat program requirements.
- (5) Provide a single repository for enterprise-level DoD insider threat related information.
- (6) Promote collaboration and sharing of insider threat information among DoD Components.

b. Appoints the Director, DITMAC.

c. Collaborates with the Office of the USD(I) to further define DITMAC business and operational requirements, and the roles and responsibilities of DoD Components in supporting this activity.

d. Collaborates with the Chief Information Officer of the Department of Defense (DoD CIO) to carry out the functions of the DITMAC as assigned in this Instruction and other applicable issuances, to develop DoD strategy for the operation and protection of DITMAC enterprise-level information technology deployed to support insider threat management. This collaboration includes developing and publishing enterprise-wide architecture requirements and technical standards; operating and maintaining DITMAC systems; ensuring interoperability, collaboration,

and interface between DoD and non-DoD entities; and making cost-effective investments in information system acquisition and sustainment necessary for DITMAC operations.

e. Develops, maintains, implements, and administers security education, training products, and services related to deterring, detecting and mitigating insider threats across the industrial, information, personnel, and physical security disciplines, and other communities of practice as directed.

f. Coordinates the release to cleared industry of information about potential threats that insiders may pose to cleared contractors, their employees, or their facilities.

2.3. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). Under the authority, direction, and control of the USD(I), and in addition to the responsibilities in Paragraph 2.7, the Director, DIA, coordinates DIA activities supporting the DITMAC to identify potential insider threats present on the DoD Intelligence Information Systems domain and reports them to the appropriate DoD Component head and the Director, DITMAC.

2.4. DIRECTOR, DEFENSE MANPOWER DATA CENTER (DMDC). Under the authority, direction, and control of the Under Secretary of Defense for Personnel and Readiness through the Director, Department of Defense Human Resources Activity, the Director, DMDC:

a. Maintains data licenses and access to government and commercial databases on behalf of the enterprise, in support of DITMAC operations.

b. Supports the DITMAC by optimizing the acquisition of and access to data sources for cross-DoD Component use for insider threat analysis.

c. Supports various enterprise tools (e.g.; the Automated Continuous Evaluation System, the Case Adjudication Tracking System, the Defense Information System for Security, and the Identity Matching Engine for Security and Analysis), and coordinates with the Director, DITMAC, to help integrate relevant technical architecture across the DoD Components.

2.5. DOD CIO. The DoD CIO:

a. Establishes policies and develops DoD strategy to counter insider threats on the DoD Information Networks.

b. Collaborates with the USD(I), the Under Secretary of Defense for Policy, the Under Secretary of Defense for Personnel and Readiness, and the Director, DSS, to develop guidelines and procedures for implementing the requirements in the March 18, 2014 Secretary of Defense Memorandum.

2.6. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA). Under the authority, direction, and control of the DoD CIO and in addition to the responsibilities in Paragraph 2.7, the Director, DISA:

- a. Coordinates DISA activities to support interconnectivity between DITMAC information technology and DoD Component insider threat information systems.
- b. Identifies potential insider threats present on the segments of the non-secure internet protocol router network and secure internet protocol router network domains under DISA's authority and reports them to the appropriate DoD Component.

2.7. DOD COMPONENT HEADS. The DoD Component heads:

- a. Share insider threat information with the Director, DITMAC, using Component insider threat analysis centers.
- b. Collaborate with the Director, DITMAC, to assign Component personnel as detailees, liaison officers, or personnel in joint-duty assignments (subject to availability and resourcing) to support the DITMAC.
- c. Deliver to the DITMAC post-processed results of information system monitoring, as appropriate, in accordance with thresholds published by the DITMAC.

SECTION 3: DITMAC FUNCTIONS AND OPERATIONS

3.1. GENERAL. The DITMAC provides DoD with an enterprise-level capability for insider threat information management.

3.2. DIRECTOR, DITMAC. The Director, DITMAC, under the authority, direction and control of the Director, DSS:

- a. Oversees the management and analysis of insider threat information by a multi-disciplinary team of DITMAC personnel that:
 - (1) Assesses the information on potential insider threats as set forth in Paragraph 1.2.b.
 - (2) Disseminates information on insider threats to DoD Components.
 - (3) Provides information to DoD Components regarding insider threat program best practices.
 - (4) Tracks responses by DoD Components to insider threats within a DoD enterprise-level information management system.
 - (5) Generates relevant metrics and reports to inform DoD Component leaders of reported and identified insider threats.
- b. Oversees efforts to decrease the insider threat to DoD and U.S. Government as set forth in Paragraph 1.2.b.
- c. Assesses the enterprise risk, refers recommendations for action, synchronizes responses, and oversees resolution of identified issues on threats that insiders may pose as set forth in Paragraph 1.2.b.
- d. Establishes risk thresholds and requirements for DoD Component reporting of potential insider threats to the DITMAC.
- e. Supports developing standards for actions and compiles results to evaluate those actions on threats that insiders may pose to DoD personnel, missions, and resources.
- f. Maintains a single DoD System of Records Notice for an enterprise-level capability for insider threat information management.
- g. Provides an enterprise-level capability for insider threat information management to assess information on potential insider threats.
- h. Shares adverse personnel security information with the DoD Consolidated Adjudications Facility for consideration in the clearance adjudication process, and with DoD Components that have an official interest in the information.

i. Ensures the acquisition of, and access to, data sources for cross-DoD Component use for insider threat analysis in partnership with the DMDC.

j. Handles personally identifiable information for U.S. persons in accordance with Section 552a of Title 5, United States Code (also known as the “The Privacy Act of 1974”), DoD Directive 5400.11, DoD 5400.11-R, and DoD Manual 5240.01.

k. Handles protected health information in accordance with DoD Instruction 8580.02 and DoD 6025.18-R.

l. Ensures that DITMAC activities, including information sharing and collection, comply with DoD Instruction 1000.29.

m. Ensures that all records are maintained and managed in accordance with National Archives and Records Administration-approved schedules to ensure proper maintenance, use, accessibility, and preservation, regardless of format or medium.

n. Ensures that the collection of information for insider threat reports is performed in accordance with Volume 1 of DoD Manual 8910.01.

GLOSSARY

G.1. ACRONYMS.

DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DITMAC	DoD Insider Threat Management and Analysis Center
DMDC	Defense Manpower Data Center
DoD CIO	Chief Information Officer of the Department of Defense
DSS	Defense Security Service
USD(I)	Under Secretary of Defense for Intelligence

G.2. DEFINITIONS. Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

DoD Component insider threat analysis centers. A DoD Component's centralized capability or location where all insider threat-related information flows and is subsequently disseminated to the proper functional or operational entities (whether internal or external) for action or resolution.

insider. Defined in DoD Directive 5205.16.

insider threat. Defined in DoD Directive 5205.16

REFERENCES

- DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
- DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 24, 2003
- DoD Directive 5143.01, "Under Secretary of Defense for Intelligence," October 24, 2014, as amended
- DoD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense," January 7, 1980
- DoD Directive 5205.16, "DoD Insider Threat Program," September 30, 2014, as amended
- DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014
- DoD Instruction 1000.29, "DoD Civil Liberties Program," May 17, 2012, as amended
- DoD Instruction 8580.02, "Security of Individually Identifiable Health Information in DoD Health Care Programs," August 12, 2015
- DoD Manual 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities," August 8, 2016
- DoD Manual 8910.01, Volume 1, "DoD Information Collections Manual: Procedures for DoD Internal Information Collections," June 30, 2014, as amended
- Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 7, 2011
- Secretary of Defense Memorandum, "Final Recommendations of the Washington Navy Yard Shooting Internal and Independent Reviews," March 18, 2014
- United States Code, Title 5, Section 522a (also known as "The Privacy Act of 1974")