DCMA Manual 3301-05

Insider Threat Program

==========

Office of Primary Responsibility	Agency Mission Assurance
Effective:	November 30, 2018
Releasability:	Cleared for public release
New Issuance	
Implements:	DCMA-INST 3301, "Agency Missions Assurance," May 14, 2018
Incorporates and Cancels:	DCMA INST 563, "Insider Threat Program" July 20, 2016
Internal Control:	Process flow and key controls are located on the Resource Page
Labor Codes:	Located on the Resource Page
Resource Page Link:	https://360.dcma.mil/sites/policy/MA/SitePages/3301-05r.aspx
Approved by:	David H. Lewis, VADM, USN, Director

Purpose: This issuance, in accordance with the authority in DoD Directive 5105.64:

- Establishes the Insider Threat Program in compliance with Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information" and DoD Directive 5205.16, "The DoD Insider Threat Program."
- Assigns responsibility and issues broad program guidance intended to establish a framework that will facilitate the further development and implementation of specific processes and procedures supporting a comprehensive Insider Threat Program.
- Implements DCMA Instruction 3301, "Agency Mission Assurance."

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This Manual applies to all DCMA personnel (military and civilian to include local nationals), employees of other Federal agencies assigned or detailed to DCMA, Contractors and other non-DoD entities that have authorized access to DCMA resources as required by their contract or agreement and individuals who volunteer and donate their services to DoD Components, including non-appropriated fund instrumentalities.

1.2. POLICY. It is DCMA policy to:

a. Develop and implement an Insider Threat (InT) Program, specifically tailored to the unique DCMA mission, that complies with DoDD 5205.16 and other applicable laws and DoD policies.

b. Through an integrated capability to monitor and audit information for insider threat detection and mitigation, the DCMA InT Program will gather, integrate, review, assess, and respond to information derived from the antiterrorism (AT), counterintelligence (CI), security, Human Capital (HC), investigations, and information assurance (IA)/cybersecurity programs to prevent, deter, detect, and mitigate actions by malicious insiders using their authorized access to do harm to the security of the United States, DoD, and/or DCMA personnel, infrastructure, information, networks, operations, and other resources.

c. Formally designate and train personnel from the following functional areas to implement the InT Program: AT, CI, HC, General Counsel (GC), security, investigations, IA/Cybersecurity, and Privacy and Civil Liberties. This collective multifunctional cadre will form the basis for an integrated information sharing and analysis capability that will identify matters that raise InT concerns and develop sufficient information from appropriate and lawful inquiries and/or investigations to resolve concerns or initiate appropriate referrals for action.

d. Collect, use, maintain, disseminate, and retain InT-related information and records in compliance with applicable laws and DoD policy, including those regarding whistleblower, civil liberties, and privacy protections.

e. Execute this Manual in a safe, efficient, effective, and ethical manner.

SECTION 2: RESPONSIBILITIES

2.1. DIRECTOR, DCMA. The Director, DCMA will:

a. Establish, maintain, and resource a comprehensive InT Program that complies withDoDD 5205.16, and other applicable policies.

b. Designate, in writing, an InT Senior Official (SO) with responsibility for the overall development, implementation, and oversight of the InT Program.

2.2. InT SO. The InT SO will:

a. Provide executive leadership, management, direction, and oversight to the InT Program and comply with DoDD 5205.16, and other applicable policies.

b. Serve as the senior advisor to the Threat Management Team (TMT).

c. Review and approve InT implementation business practices, the annual InT Report, and other applicable materials and reports.

d. Resolve staff conflicts and other matters of contention as it relates to InT Program implementation.

e. Advocate for resources to support a comprehensive InT Program.

2.3. GC. In addition to the requirements established in Paragraph 2.14., the GC will:

a. Provide legal advice and support to the SO and InT Program to assist them in carrying out their responsibilities under this Manual.

b. Appoint a representative to serve on and advise the InT Program Hub and the TMT.

c. Provide legal advice to management officials in actions involving actual or suspected InT activities and/or matters.

2.4. EXECUTIVE DIRECTOR, CORPORATE OPERATIONS Directorate. In addition to the requirements established in Paragraph 2.14., the Executive Director, Corporate Operations will provide staff oversight to the DCMA Security Division serving as the InT Program Office.

2.5. EXECUTIVE DIRECTOR, INFORMATION TECHNOLOGY (IT) DIRECTORATE. In addition to the requirements established in Paragraph 2.14., the Executive Director, IT will:

a. Serve as the Agency lead for establishing, resourcing, implementing, and maintaining IT-related requirements established in DoDD 5205.16, and other applicable policies.

b. Establish and support information sharing and reporting processes and requirements ensuring IT related information necessary to support InT identification, inquiries, analysis, and response actions is promptly provided to the InT Hub and/or inquiry and/or investigative officials.

c. Establish procedures that ensure the prompt reporting of InT-related anomalous activities and/or behaviors derived from user activity monitoring (UAM) and audit processes to the InT Hub.

d. Support InT related reporting and assessment requirements.

e. Report InT resource expenditures and requirements to the InT Program Manager (PM) for consolidation and further reporting.

2.6. EXECUTIVE DIRECTOR, HUMAN CAPITAL (HC) DIRECTORATE. In addition to the requirements established in Paragraph 2.14., the Executive Director, HC will:

a. Establish and support information sharing and reporting requirements ensuring HC related information necessary to support InT identification, inquiries, analysis, and response actions is promptly provided to the InT Hub and/or investigators.

b. Support InT related reporting and assessment requirements.

c. Report InT resource expenditures and requirements to the InT PM for consolidation and further reporting.

2.7. EXECUTIVE DIRECTOR, SPECIAL PROGRAMS DIRECTORATE. In addition to the requirements established in Paragraph 2.14., the Executive Director, Special Programs will:

a. Appoint a representative to serve on the InT Hub, as needed.

b. In consultation with the SO, the DoD Special Access Program (SAP) Coordinating Office and responsible program office officials, coordinate and address InT activities specifically involving SAP and sensitive compartmented information (SCI) programs under the cognizance of the Special Programs Directorate.

c. Support InT related reporting and assessment requirements.

d. Serve as the Agency lead for policies involving SAP and/or SCI systems under the cognizance of the Special Programs Directorate.

e. Establish, resource, implement, and maintain IT-related requirements established in DoDD 5205.16 and promptly report InT indicators derived from UAM and audit processes to the InT Hub consistent with security clearance and program access requirements.

g. Report InT resource expenditures and requirements to the InT PM for consolidation and further reporting.

2.8. EXECUTIVE DIRECTOR, INTERNAL AUDIT AND INSPECTOR GENERAL (IG). In addition to the requirements established in Paragraph 2.14., Executive Director, Internal Audit and IG will:

a. Establish and maintain an investigative capability that provides advice, guidance, training, and other related support to the InT Program and to management officials in response to actual or potential InT matters.

b. Designate a component representative to serve as part of the InT Program Hub, and TMT.

c. Promptly report to the InT Hub information received and the results of investigative activities conducted revealing anomalous activities and/or behaviors indicative of an InT.

d. Conduct and document investigations and inquiries in support of the InT Program.

e. Share relevant information with the InT Hub necessary to support InT inquiries, analysis, and response activities.

f. Report InT resource expenditures and requirements to the InT PM for consolidation and further reporting.

g. Conduct program assessments in accordance with the guidance in Section 3, Paragraph 3.6.b.

2.9. DIRECTOR OF SECURITY. In addition to the requirements established in Paragraph 2.14., the Director of Security will:

a. Appoint a PM to manage and lead the InT Program.

b. Designate members from the AT, CI, and personnel, information and physical security programs to serve as members of the InT Hub.

c. In conjunction with the Office of the Under Secretary of Defense (Intelligence) (OUSD(I)) and the DoD Consolidated Adjudication Facility (CAF), maintain a comprehensive continuous evaluation (CE) program that assesses personnel reliability and trustworthiness for continued access to national security information and/or assignment to sensitive positions. Promptly report to the InT Hub tentative and final decisions by the DoD CAF to deny eligibility for access to national security information or assignment to a sensitive position.

d. Establish procedures to promptly report to the InT Hub identified or reported anomalous activities and/or behaviors indicative of InT activity derived through security channels.

e. Share relevant information with the InT Hub and/or investigators necessary to support InT inquiries, analysis, and response activities.

f. Ensure DCMA personnel granted access to classified national security information and/or systems have completed nondisclosure agreements (NDA) and these agreements are readily available for inspection and/or investigative purposes.

g. Prior to granting DCMA personnel access to classified national security information and/or systems, validate completion of InT awareness training and document validation in the Electronic Personnel Security File for inspection and/or investigation purposes.

h. Designate knowledgeable personnel to assist the Director of IA/Cybersecurity in establishing InT Program-specific triggers to support UAM efforts.

i. Lead Agency-level coordination in support of reporting and assessment requirements.

j. Annually conduct, document, and report the results of an Agency-level InT Program Review to the SO and the OUSD(I).

k. Provide advice and guidance to management officials in actions involving actual or suspected InT activities.

l. Allocate and report resource requirements in support of the InT Program.

2.10. DIRECTOR, LABOR AND EMPLOYEE RELATIONS (LER). In addition to the requirements established in Paragraph 2.14., the Director of LER will:

a. Appoint a representative(s) to serve as a member of the InT Hub.

b. Serve as a member of the TMT and complete required training.

c. Provide LER advice, guidance, training, and other related support to the InT Program.

d. Promptly report to the InT Hub identified or reported anomalous activities and/or behaviors indicative of InT activity.

e. Share relevant information with the InT Hub and/or inquiry and/or investigative officials necessary to support InT inquiries, analysis, and response activities.

f. Provide advice and guidance to management officials in actions involving actual or suspected InT activities.

2.11. DIRECTOR OF IA/CYBERSECURITY. In addition to the requirements established in Paragraph 2.14., the Director of IA/Cybersecurity will:

a. Appoint a representative to serve as a member of the InT Hub.

b. Serve as a member of the TMT and complete required training.

c. Provide IA/Cybersecurity and UAM advice, guidance, training, and other related support to the InT Program.

d. Promptly report to the InT Hub identified or reported anomalous activities and/or behaviors indicative of InT activity.

e. Share relevant information with the InT Hub and/or inquiry/investigative officials necessary to support InT inquiries, analysis, and response activities.

f. In coordination with the InT PM and other designated security representatives, establish InT Program-specific triggers to support network UAM efforts.

g. Establish and maintain procedures to safeguard UAM activities and related information from unauthorized disclosure.

2.12. PM, InT PROGRAM. Under the authority, direction, and control of the Director of Security, the PM, InT Program will:

a. Serve as a member of the InT Program Hub and TMT and complete required training.

b. Establish and maintain InT policy, procedures, practices, and tools that comply with applicable laws, policies, and guidance.

c. Establish and maintain a comprehensive InT DCMA 360 site, accessible by all DCMA personnel, which meet the requirements of DoDD 5205.16 and other governing policies and guidance.

d. Establish, document, and maintain internal InT Hub specific processes and procedures for acquiring, safeguarding, integration, review, analysis, and when appropriate, refer information and reports indicating insider threats. Ensure the GC and the Component Senior Official for Privacy (CSOP) and the Chief Civil Liberties Officer (CCLO) review processes and procedures to ensure compliance with laws and DoD policies.

e. Coordinate and/or conduct InT related inquiries.

f. In coordination with the SO, establish and maintain training requirements for personnel assigned InT roles and responsibilities and track training to validate completion.

g. Schedule, coordinate, lead, and document the results of TMT meetings.

h. Represent the Agency at departmental and interagency forums engaged in countering the insider threat.

i. Annually conduct and document the results of an InT Program self-assessment.

j. In coordination with the Director of IA/Cybersecurity and designated security representatives, assist in establishing InT Program-specific triggers to support network UAM efforts.

k. Maintain close and recurring liaison and connectivity with the Defense InT Management and Analysis Center (DITMAC); and, ensure timely accomplishment of DITMAC reporting requirements.

2.13. CSOP AND CCLO. The CSOP and CCLO will:

a. Serve as a member of the InTP Hub, and TMT and complete required training.

b. Provide privacy and civil liberties advice, guidance, training, and other related support to the InT Program and to management officials responding to actual or potential InT matters.

c. Provide privacy and civil liberties training annually to designated InT personnel and TMT members.

d. Provide privacy and civil liberties support to program reviews and the annual InT Report.

2.14. COMMANDERS, DIRECTORS, AND OTHER MANAGEMENT OFFICIALS. Commanders, Directors, and other management officials will:

a. Promptly report anomalous activities and/or behaviors potentially indicative of InT activities using existing AT, CI, security, HC, or IA/cybersecurity reporting channels.

b. Leverage the unique training, expertise, and capabilities of the Agency's GC, HC, IG, InT, security, IA/Cybersecurity, and privacy and civil liberties staffs when responding to actual or suspected InT matters.

c. Ensure assigned personnel complete InT awareness training in accordance with Section 6 of this Manual.

2.15. DCMA PERSONNEL. All personnel assigned duties with DCMA will:

a. Promptly report anomalous activities and/or behaviors potentially indicative of an insider threat through existing management, AT, CI, security, HC, IG, or IA/cybersecurity reporting channels.

b. Complete InT training as directed.

SECTION 3: PROGRAM GOVERNANCE AND OVERSIGHT

3.1. GENERAL.

a. The DCMA InT Program is designed to prevent and/or deter personnel from becoming InTs, detect potential insiders who pose a threat to DoD or DCMA resources, and mitigate insider threat risk through appropriate and authorized measures.

b. The InT Program will consist of the following focus areas: network UAM and auditing, information sharing, security (to include but not limited to personnel, physical, and information security), training and awareness, and InT reporting and response.

3.2. InT SO.

a. The DCMA SO is appointed by the DCMA Director and is responsible for providing executive management, accountability, and oversight to the InT Program thereby ensuring compliance with applicable higher-level policies and standards.

b. The SO will, through recurring updates, ensure the DCMA Director maintains an appropriate level of InT Program situational awareness and provide resource recommendations in support of the program.

c. To ensure seamless integration of various functions required to implement a comprehensive InT Program, the SO serves as the senior advisor to the TMT. Through these forums, the SO will ensure policy development and update, information sharing, and other program requirements are met and internal conflicts are resolved.

3.3. TMT.

a. The TMT will consist of a select group of senior multifunctional subject matter experts specifically cleared to review and analyze actual or suspected InT reports and then make recommendations to management on actions to take to prevent and/or mitigate the impacts of the threat.

b. The TMT is an event driven forum responding to actual or suspected InT reports requiring senior level involvement and will convene quarterly to review InT reports, activities, and to identify trends to support deterrence efforts.

(1) Any member of the TMT may convene an emergency meeting of the forum based on the identification of an actual or suspected threat. Under such conditions, the TMT may be convened with all members or select members based on the situation and member availability.

(2) The InT PM will schedule, coordinate, and document the results of recurring quarterly meetings.

c. Listed below is the primary membership of the TMT. TMT members will retain eligibility for access to at least SECRET information and sign an InT Program specific NDA. The InT PM will retain the members NDA for record.

- Senior Official - Senior Advisor to the TMT
- Director of Security and CI - Chairperson
- InT PM - Alternate Chairperson
- GC Representative
- Director of LER
- IG Representative
- Director of IA/Cybersecurity
- CSOP and CCLO
- Other management officials as directed by the SO or Chairperson

3.4. InT PROGRAM MANAGEMENT OFFICE.

a. The Security Division will serve as the Agency's program office for the InT Program. The Director of Security will appoint, in writing, an InT PM who will have responsibility for establishing and implementing a DCMA specific InT Program that complies with applicable laws and DoD policies.

b. The InT PM will coordinate and integrate the activities of the various functions (security, investigations, CI, HC, AT, IA/Cybersecurity, GC, CSOP/CCLO, etc.) supporting the InT Program. In addition, the InT PM will support assessment and reporting requirements in accordance with higher-level guidance and Paragraph 3.7.

3.5. I nT HUB.

a. The InT Hub, operating under the direction of the Director of Security and/or the InT PM, is not a physical location or organization but a multifunctional virtual team designed to consolidate, integrate, analyze, coordinate, document, and refer information and/or reports indicating InT activities for action. The InT Hub is formed with designated membership from security enterprise programs, investigations, CI, LER, AT, IA/Cybersecurity, GC, CSOP/CCLO, and others as deemed necessary. The InT PM and the CI PM will serve as the primary members forming the nucleus of the InT Hub with other members serving in an ancillary role providing subject matter expertise and support on an as needed basis.

b. InT Hub activities will be compartmentalized to safeguard the integrity of InT information (both classified and unclassified) and to ensure privacy and civil liberties protections. InT information and records will be safeguarded and retained in accordance with Section 5 of this Manual.

3.6. ASSESSMENTS.

a. Program Review. Every July, the InT PM will conduct a self-assessment of the InT Program to measure the effectiveness of the program and to determine compliance with established policy and guidance.

(1) The InT PM will conduct the self-assessment using approved benchmarks, document the assessment in a formal report, and maintain the assessment on file with a copy provided to the Director of Security.

(2) The InT PM will ensure self-assessment reports are marked, transmitted, safeguarded, and destroyed in accordance with the appropriate classification level and retained in accordance with this Manual and DCMA records management guidance.

b. Annual Oversight Review. Annually, not later than December 15, the DCMA IG will conduct an overarching review of the InT Program and report the results to the DCMA Director, through the SO, in the form of an annual report.

(1) The annual oversight review will evaluate the status of the program in meeting the requirements of DoDD 5205.16 and will include progress made to enhance program effectiveness, accomplishments made to improve the program, resources allocated, risks, goals, resource recommendations, and challenges.

(2) To facilitate this review, the IG will establish or adopt a common assessment strategy that ensures assessment processes remain consistent across assessment periods.

3.7. SUPPORT TO ASSESSMENT AND REPORTING REQUIREMENTS. The Security Division, as the Agency's InT Program Office, will serve as the central point of entry for coordination, support, and response to InT-related taskings, assessments, and reporting requirements. This will ensure the Agency speaks as "one team, one voice" on all InT related matters and will ensure compliance with the requirements of DoDD 5205.16.

SECTION 4: DETECTION, REPORTING, ANALYSIS, AND RESPONSE

4.1. GENERAL GUIDANCE. InT actors typically exhibit observable concerning behaviors that can be detected, reported, investigated, and analyzed to determine the severity of a threat. These actions can lead to the development of appropriate response options to prevent and/or mitigate damage to national security or to DoD personnel and/or resources while preserving privacy and civil liberties. This Section contains baseline guidance for the detection, reporting, analysis, and response actions to potential and/or actual insider threat activities.

4.2. DETECTING AND REPORTING InT ACTIVITIES/BEHAVIORS.

a. An effective InT Program relies on the timely identification and reporting of anomalous activities and/or behaviors (also referred to as indicators) that could indicate an InT. To detect InT indicators, DCMA will use information derived from management and employee reporting as well as information and reporting derived from CI, security, investigative, UAM and auditing, and HC channels.

b. Personnel detecting InT indicators will promptly report such activity through management and/or other established reporting channels (CI, AT, HC, security, investigative, and/or network UAM). Personnel assigned to the Special Programs Directorate will report such activity through their management and/or security channels. To assist in the identification of these indicators DCMA will adopt DoD established indicator criterion and supplement these with Agency-specific indicators, where necessary. A list of potential indicators and reporting tools/procedures is posted to the DCMA webpage 360 InT site and to the Resource Page for this Manual. When there is a question as to whether a particular indicator or set of indicators warrant reporting, personnel will promptly report the indicator(s).

c. Management officials responsible for implementing CI, AT, HC, security, investigative, and/or network UAM functions will promptly share InT indicators reported or detected with the InT Hub in accordance with Paragraph 4.2.b.

4.3. ANALYSIS, REFERRAL AND RESPONSE.

a. Upon receipt of a report of potential InT activity, InT Hub personnel will immediately initiate a review to establish a path forward. If reported information reveals an imminent threat, the situation will be immediately relayed by the most expeditious means possible to the responsible Commander/Director, the Director of Security, the SO, and/or local law enforcement or security force authorities, as appropriate, to address the urgency of the threat. An emergency TMT meeting may be called to address the situation.

(1) When the initial review determines the reported information does not constitute an insider threat, the information will be referred to an appropriate organization(s) for action. For example, information reported of a strictly criminal matter may not represent an insider threat and as such would be referred to the DCMA IG for action.

(2) When it is determined reported activity potentially constitutes an InT, InT Hub personnel will initiate a preliminary inquiry to determine if probable cause exists to believe the reported activity, and the person(s) allegedly conducting the activity, represent a threat to the Department and/or DCMA. When the initial inquiry fails to result in the establishment of probable cause, InT Hub personnel will document the results of the inquiry and refer the report for action in accordance with Paragraph 4.3.a.(1) and/or close the report unless directed otherwise by the GC, the SO, or the Agency Director. The TMT will review all initial inquiries and their results and/or status at quarterly TMT meeting to ensure situational awareness by team members.

(3) If inquiry results establish probable cause, the inquiry will be referred to the DCMA IG to conduct a detailed investigation and/or referral/coordination with other applicable investigative organizations (Defense Criminal Investigative Service (DCIS), Federal Bureau of Investigations (FBI), etc.). In addition, InT PM will alert the TMT membership to the referral to ensure situational awareness. In these circumstances, the DCMA IG will lead the investigative activity and will ensure the TMT membership maintains situational awareness on the progress of the case. When required, an emergency TMT meeting may be called to address emergent issues or concerns discovered during the course of the investigation.

(4) If reported information or the results of an investigative action reach the level of a "Section 811 referral," as established by United States Code, Title 50, Section 3381 the InT PM or the DCMA IG will immediately refer the matter to the FBI and take no further action unless otherwise directed by the FBI.

b. When conducting either an InT inquiry or a detailed investigation, DCMA organizations must provide any information necessary to support the successful conclusion of the investigative action. Questions regarding the legality of sharing information in support of an inquiry or investigative action must be referred to the GC for advice.

c. If investigative efforts conclude InT activity exists or there is insufficient information to rule out such activity, the case will be referred to the TMT for further analysis and to the responsible management official for action, as appropriate. The InT PM will monitor, coordinate, and track referred actions through closure. In all cases, InT related inquiries and investigations will be documented in a written report that is retained and safeguarded in accordance with Section 5 of this Manual.

d. When information meets DoD reporting thresholds established by the DITMAC, the InT PM will promptly report the information in accordance with established DITMAC reporting guidance.

SECTION 5: INFORMATION/RECORDS SAFEGUARDING AND RETENTION

5.1. GENERAL.

a. Due to the nature of the information contained in InT related reports, inquiries, and other records, special handling, safeguarding, and retention guidance is appropriate. Additionally, the November 21, 2012 Presidential Memorandum, "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs," requires the establishment of component specific InT information and records handling guidance. As such, this section meets these requirements.

b. DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)," and associated manuals establish DoD overarching guidance for safeguarding classified and controlled unclassified information (CUI). For the purposes of this Manual, all information, materials, and records related to the InT Program will comply with the requirements of these and any supplemental policy documents.

5.2. SAFEGUARDING InT INFORMATION AND RECORDS.

a. Access to InT Information and Records. Access to InT information and records must be limited to personnel meeting access requirements under DoD and DCMA information security policies and can demonstrate a valid InT related mission requirement for access. When personnel meet the general requirements under this paragraph, access must be limited to that required to meet mission objectives and need to know. Due to the nature of their assigned duties, personnel specifically assigned InT Hub and TMT duties may be authorized access to the full range of information required to perform assigned duties and responsibilities consistent with security clearance and NDA requirements.

b. Classifying, Marking, Handling, Transmitting, and Safeguarding InT Information and Records.

(1) Classified Information and Records. InT information and records must be classified, marked, handled, transmitted, and safeguarded in accordance with DoD Manual (DoDM) 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification;" DoDM 5200.01, Volume 2, "DoD Information Security Program: Marking of Classified Information;" DoDM, Volume 3, "DoD Information Security Program: Protection of Classified Information;" and applicable DCMA guidance. The DCMA Director is the only original classification authority within DCMA. As such, all classification decisions not rendered by the DCMA Director will be based on approved derivative classification authorities and processes.

(2) Unclassified Information and Records. InT information and records not classified under the guidance of Paragraph 5.2.b.(1) will be designated CUI and marked, transmitted, and safeguarded in accordance with DoDM 5200.1, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)," and other applicable policies.

(3) Personally Identifiable Information (PII). PII for U.S. persons will be marked, transmitted, and safeguarded in accordance with DoDD 5400.11, "DoD Privacy Program," DoD 5400.11-R, "Department of Defense Privacy Program" and Paragraph 5.2.b(2) of this Manual.

(4) Personally Identifiable Health Information. Personally identifiable health information will be marked, handled, transmitted, and safeguarded in accordance with DoDI 6490.04, "Mental Health Evaluations of Members of the Military Services," DoDI 6490.08, "Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Service Members," DoD Instruction 8580.02, "Security of Individually Identifiable Health Information in DoD Health Care Programs," and Paragraph 5.2.b(2) of this Manual.

5.3. RETENTION REQUIREMENTS AND LIMITATIONS.

a. The guidance established under this paragraph applies specifically to InT information and records. Separate AT, CI, security, HC, IA/Cybersecurity, investigative, and/or intelligence-specific information and records will be handled, stored, and retained in accordance with applicable DoD and DCMA retention guidance.

b. Existing DCMA records management guidance serves as the basis for InT records management operations. InT records will be labelled in accordance with established DCMA records management guidance but stored separate from other records to ensure their integrity and to enhance privacy and civil liberties protections.

SECTION 6: TRAINING AND AWARENESS

6.1. GENERAL. The DoDD 5205.16 requires DoD components to establish InT specific training requirements for both the workforce and InT personnel. This section addresses these requirements.

6.2. TRAINING.

a. InT Personnel Training. In order to be effective, personnel serving in InT roles (InT Hub, TMT, etc.) must possess the InT Program specific skills necessary to perform their assigned duties. The InT PM will identify and document minimum training requirements for personnel serving in InT roles. The SO will serve as the approving authority for InT training requirements. The InT PM and SO will review and update training requirements annually to ensure requirements remain current.

b. Workforce Training. All assigned DCMA personnel will complete approved InT Awareness Training within 30 days of assignment and annually thereafter. Existing training that incorporates InT awareness meets the spirit and intent of this requirement. In addition, appropriate training, education, and awareness of the insider threat will be provided to all DCMA contractors, and volunteers who have access to DCMA resources.

6.3. AWARENESS.

a. To maximize opportunities to deter and/or prevent potential threats, InT training and awareness must be a continuous effort, not just a one-time or annual event. The InT awareness topics must be integrated into briefings, meetings, lectures, electronic media, etc., at all levels to compliment formal training courses.

b. Listed below are the types of activities used to maintain a high state of InT awareness throughout the workforce:

(1) DCMA Sharepoint 360 InT Program Site. The InT PM will establish and maintain a comprehensive DCMA Sharepoint 360 InT site, accessible by the workforce, containing policy, training and awareness information, a listing of potential anomalous activities, reporting requirements, etc.

(2) Meetings. Commanders, Directors, and Managers are encouraged to include InT related topics in meetings such as staff and all-hands meetings. The InT and CI PMs can support this effort by providing training and awareness materials as well as information briefings.

(3) The Sentinel Newsletter. Periodically, the InT PM will include InT awareness information into articles published via the DCMA security newsletter "The Sentinel."

GLOSSARY

G.1. DEFINITIONS

Counterintelligence (CI). See DoDD 5240.02, "Counterintelligence"

Classified Information. See DoDM 5200.01, Volume 1

Cybersecurity. See DoDI 8500.01, "Cybersecurity"

Employee. See Federal Register, Vol 60., No. 151, (August 7, 1995)

IA. See DCMA-INST 815, "Cybersecurity/Information Assurance"

Insider. See DoDD 5205.16

InT. See DoDD 5205.16

Senior Official. See DoDD 5205.16

GLOSSARY

G.2. ACRONYMS

AT	Antiterrorism
CAF	Consolidated Adjudication Facility
CCLO	Chief Civil Liberties Officer
CI	Counterintelligence
CSOP	Chief Senior Official for Privacy
CUI	Controlled Unclassified Information
DITMAC	Defense Insider Threat Management and Analysis Center
DoD	Department of Defense
DoDD	DoD Directive
DoDI	DoD Instruction
DoDM	DoD Manual
EO	Executive Order
FBI	Federal Bureau of Investigations
GC	General Counsel
HC	Human Capital
IA	Information Assurance
IG	Inspector General
InT	Insider Threat
IT	Information Technology
LER	Labor and Employee Relations
NDA	Non-disclosure Agreement
OUSD(I)	Office of the Under Secretary of Defense (Intelligence)
PII	Personally Identification Information
PM	Program Manager
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SO	Senior Official
TMT	Threat Management Team
UAM	User Activity Monitoring

REFERENCES

DCMA Instruction 710, "Managers' Internal Control Program," April 21, 2014
DCMA Instruction 815, "Cybersecurity/Information Assurance," July 10, 2014
DCMA Manual 3301-08, "Information Security," TBD
DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
DoD Directive 5105.64, "Defense Contract Management Agency (DCMA)," January 10, 2013
DoD Directive 5205.16, "The DoD Insider Threat Program," September 30, 2014, as amended
DoD Directive 5240.02, "Counterintelligence (CI)," March 17, 2015, as amended
DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014
DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)," April 21, 2016, as amended
DoD Instruction 6490.04, "Mental Health Evaluations of Members of the Military Services," March 4, 2013
DoD Instruction 6490.08, "Command Notification Requirements To Dispel Stigma In Providing Mental Health Care to Service Members," August 17, 2011
DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
DoD Instruction 8580.02, "Security of Individually Identifiable Health Information In DoD Health Care Programs," August 12, 2015
DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012, as amended
DoD Manual 5200.01, Volume 2, "DoD Information Security Program: Marking of Classified Information," February 24, 2012, as amended
DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended
DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)," February 24, 2012, as amended
Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and Responsible Sharing and Safeguarding of Classified Information," October 7, 2011
Presidential Memorandum, "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs," November 21, 2012
United States Code, Title 50, Section 3381 Regulatory Relief Task Force," October 15, 2006
United States Code, Title 10, Section 801
Committee on National Security Systems (CNSSD), Directive on Protecting National Security Systems From Insider Threat, Per E.O