DoD Instruction 5205.16

The DoD Insider Threat Program

Originating Component:	Office of the Under Secretary of Defense for Intelligence and Security
Effective:	December 20, 2024
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Directive 5205.16, "The DoD Insider Threat Program," September 30, 2014, as amended
Incorporates and Cancels:	See Paragraph 1.3.
Approved by:	Milancy D. Harris, Acting Under Secretary of Defense for Intelligence and Security

Purpose: In accordance with the authority in DoD Directive (DoDD) 5143.01, this issuance establishes policy, assigns responsibilities, and prescribes procedures and requirements to develop and maintain an insider threat program (InTP) pursuant to the November 21, 2012 Presidential Memorandum; Executive Order (E.O.) 13587; Section 2224 of Title 10, United States Code (U.S.C.); Section 922 of Public Law (PL) 112-81; Section 951 of PL 114-328; Section 1090 of PL 116-283; and the Committee on National Security Systems Directive Number 504.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

a. This issuance applies to:

(1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense (OIG DoD), 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").

(2) Any person who has, or once had, authorized access to information, a facility, a network, or a resource of the DoD.

(3) Foreign nationals including international military students and their accompanying family members who have authorized access to information, a facility, a network, or a resource of the DoD, in accordance with Section 1090 of PL 116-283 and the November 18, 2021 Secretary of Defense Memorandum.

b. This issuance does not supersede restrictions and does not otherwise affect:

(1) The authorities, policies, and responsibilities of the Director of National Intelligence regarding the protection of intelligence sources, methods, and activities, including the standards for access to sensitive compartmented information and special access programs.

(2) The authority or independence of the OIG DoD.

(3) DoD policy governing access to or dissemination of sensitive or classified law enforcement (LE) information, counterintelligence (CI), and intelligence operations information.

(4) The use of the Federal Bureau of Investigation eGuardian System as the exclusive unclassified means for reporting suspicious activity, in accordance with DoD Instruction (DoDI) 2000.26.

(5) DoD personnel security and personnel vetting authorities and responsibilities.

(6) Other restrictions as directed in other issuances related to intelligence, CI, LE, or OIG DoD functions of the DoD and the DoD Components.

1.2. POLICY.

a. The DoD will establish a comprehensive InTP in accordance with Federal laws, E.O.s, and national-level policies.

b. The DoD InTP will comply with applicable laws, whistleblower protections, and privacy and civil liberties policies in accordance with PL 104-191; Parts 160, 162, and 164 of Title 45, Code of Federal Regulations; Section 552(a) of Title 5, U.S.C., also known and referred to in this issuance as the "Privacy Act of 1974"; DoDIs 5400.11, 6025.18, 6490.04, 6490.08, and 8580.02, and Volume 2 of DoD Manual (DoDM) 5400.11.

c. The November 21, 2012 Presidential Memorandum transmitted the National Insider Threat Policy and Minimum Standards for InTP including access, sharing, and analysis of information and data; InTP personnel; monitoring user activity on classified networks; and workforce training and awareness. DoD Components may establish additional standards, provided they are consistent with the requirements contained in this issuance and national policy.

d. The DoD InTP, an element of the Defense Security Enterprise, is established to deter, detect, and mitigate insider threats to national security and DoD information, resources, facilities, personnel, and readiness, in collaboration with CI, LE, human resources (HR), cybersecurity, and other relevant functions and security programs, to include personnel vetting, information security, physical security, and operations security.

e. Direction set forth in this issuance will serve as minimum requirements for the DoD InTP. Nothing in this issuance will be construed to supersede existing or future Intelligence Community or DoD policy, which may impose commensurate or more stringent requirements beyond these minimum standards for the InTP.

1.3. INCORPORATES AND CANCELS.

This issuance incorporates and cancels these documents:

a. Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) Memorandum, "Stand-down of the Non-Secure Internet Protocol Router User Activity Monitoring Program," August 29, 2023.

b. Office of the Under Secretary of Defense for Intelligence Memorandums:

(1) "Insider Threat Mission Requirements," March 28, 2016.

(2) "Establishment of an Insider Threat Enterprise Program Management Office," March 9, 2017.

(3) "Reaching Department of Defense Counter Insider Threat Program Milestones," March 28, 2019.

(4) "Department of Defense Counter-Insider Threat Program Strategic Plan," August 1, 2019.

(5) "Reporting Investigative Information to Department of Defense Component Insider Threat Hubs and the Department of Defense Insider Threat Management and Analysis Center," April 22, 2019.

(6) "Department of Defense Counter-Insider Threat Program Requirements," January 9, 2020.

c. Under Secretary of Defense for Intelligence and Security (USD(I&S)) Memorandum, "Implementation of Countering Extremist Activity Working Group recommendations," June 6, 2022.

d. Under Secretary of Defense for Intelligence Memorandums:

(1) "Reporting Information to the Department of Defense Management and Analysis Center," December 29, 2016.

(2) "Reaching Department of Defense Counter Insider Threat Program Milestones," August 10, 2018.

e. DoD Instruction 5205.83, "DoD Insider Threat Management and Analysis Center (DITMAC)," March 30, 2017, as amended.

SECTION 2: RESPONSIBILITIES

2.1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY (USD(I&S)).

In accordance with DoDDs 3115.18, 5200.43, 5240.02, and 5240.06; and DoDIs 5240.19 and 5240.26, the USD(I&S):

a. Serves as the DoD senior official for the InTP; establishes policy, prescribes guidance, and oversees implementation of the DoD InTP; and makes resource recommendations to implement requirements, in accordance with E.O. 13587, the November 21, 2012 Presidential Memorandum, and Section 951 of PL 114-328.

b. Conducts oversight activities for program efficacy and appropriate resourcing of DoD insider threat activities, as defined in this issuance, and reports status to the Secretary of Defense.

c. Coordinates with the DoD Chief Information Officer (DoD CIO) on user activity monitoring (UAM) oversight and improves threat monitoring across all DoD networks and computer environments as technology and operating environments evolve.

d. Ensures InTP policies and procedures are aligned with other DoD policies and facilitates coordination of other DoD policies for InTP equities, as appropriate.

e. Ensures that personnel security policies for reinvestigations, post-adjudicative investigations, continuous vetting, referrals for action, suspensions, and continuing security responsibilities address insider threats in accordance with DoDM 5200.02.

f. Oversees the Defense Counterintelligence and Security Agency (DCSA), which provides DoD enterprise-level services to support InTP analyses, assessments, data management, and information technology systems that support and advance the DoD InTP.

g. Coordinates with the General Counsel of the Department of Defense in developing DoD insider threat policy and overseeing the DoD InTP.

h. Supports DoD training and awareness efforts to inform the workforce about the InTP.

i. Represents the DoD at departmental and interagency intelligence and security forums related to insider threat.

j. Coordinates with the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) on DoD prevention programs to facilitate information sharing, in accordance with DoDI 6400.11.

k. Coordinates with the DoD Component heads to develop policy and guidance on the DoD's access to and use of publicly available information (PAI) for matters related to USD(I&S) responsibilities and functions.

l. Maintains program management and governance board responsibilities for the nationally accredited Certified Insider Threat Professional (CITP) Program or its successors for personnel conducting DoD InT activities and the DoD InTP.

2.2. DIRECTOR FOR DEFENSE INTELLIGENCE (COUNTERINTELLIGENCE, LAW ENFORCEMENT, AND SECURITY).

Under the authority, direction, and control of the USD(I&S), the Director for Defense Intelligence (Counterintelligence, Law Enforcement, and Security):

a. Conducts oversight activities of the DoD InTP on behalf of the USD(I&S), to include establishing performance measurement criteria and providing guidance and support to the DoD Components to resolve operational matters.

b. Interprets and provides implementing guidance on insider threat policy and procedures to ensure compliance by DoD Components.

c. Coordinates with DoD Component heads to synchronize and oversee all DoD InTP research initiatives and activities, as needed.

d. Approves updates to the DoD InTP reporting thresholds and timelines for DoD Component reporting of potential insider threats to the Director, DCSA.

e. Maintains a single DoD system of records notice for the repository for DoD insider threat related information.

f. Serves as the sponsor for the DoD InTP information technology systems and cyber capabilities.

2.3. DIRECTOR, DCSA.

Under the authority, direction, and control of the USD(I&S), and in addition to the responsibilities in Paragraph 2.11., the Director, DCSA:

a. In coordination with the USD(I&S), provides DoD enterprise-level services to support InTP analyses, assessments, information integration, and information sharing. Determines appropriate agency and DoD elements for the cost, schedule, and delivery of insider threat related services.

b. Incorporates OUSD(I&S) and Component requirements into insider threat-related services and provides periodic performance metrics as prescribed by the OUSD(I&S).

c. Provides insider threat analytic services to Component insider threat hubs, to include behavioral threat analysis center consultations, responses to requests for information, and reviews of PAI, as requested.

d. Conducts insider threat activities with the support of subject matter experts in CI, LE, HR, identity intelligence, network monitoring, cybersecurity, privacy and civil liberties, behavioral threat assessment, and other relevant functions and security programs, to include personnel vetting, information security, physical security, and operations security.

e. Ensures efficient access to necessary data using an enterprise and shared data management capability, pursuant to Paragraph 3.4. of this issuance.

f. Establishes procedures and leverages technology to facilitate sharing of agency-specific information among DCSA and DoD Components to facilitate insider threat risk mitigation and personnel vetting activities, including continuous vetting activities as defined by national-level and DoD policy and Trusted Workforce 2.0 initiatives.

g. Recommends updates to the DoD InTP reporting thresholds and timelines to the OUSD(I&S), and leverages technology to the greatest extent possible to facilitate Component reports of potential insider threats.

h. Conducts assessments of DoD Component InTP elements for efficiency and effectiveness and provides assessment reports to the OUSD(I&S). Receives and tracks submissions of DoD Component annual reports and self-assessments.

i. Provides performance measurement data on output, efficacy, and reporting trends through Advana, or a successor platform, to the OUSD(I&S) to improve performance, inform research, training, and resourcing requirements, as necessary.

j. Assesses cleared contractors under DoD cognizance in the National Industrial Security Program, in accordance with insider threat requirements established by Part 117 of Title 32, Code of Federal Regulations.

k. Establishes and administers education, training, and certification programs for insider threat and the designated enterprise information technology system. Conducts annual assessments of education, training, and certification products for efficacy and policy compliance.

l. Implements a DoD-wide insider threat hotline to support reporting and information sharing requirements and provides the OUSD(I&S) performance measurement data on hotline output, efficacy, and reporting trends through Advana, or a successor platform.

m. Supports the DoD Components in implementing the information sharing and reporting requirements related to their respective prevention, assistance, and response (PAR) capability and other prevention activities, when requested, and in accordance with agreements with the DoD Components. Provides performance measurement data on output, efficacy, and reporting trends through Advana, or a successor platform, to the OUSD(I&S) and the respective DoD Components who have an agreement with the DCSA to use this service.

n. In coordination with the USD(I&S) and the DoD Component heads, evaluates research needs for the DoD InTP, makes recommendations, and facilitates research projects, as necessary.

2.4. UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT.

The Under Secretary of Defense for Acquisition and Sustainment:

a. Advises the DoD Components on the requirements of insider threat policies with respect to the nuclear enterprise and the Nuclear Weapons Personnel Reliability Program, pursuant to DoDD 5210.41; DoDIs 5210.42 and O-5210.63; and DoDMs 5210.42, S-5210.41, and S-5210.92.

b. Develops policy, amends the Defense Federal Acquisition Regulation Supplement, as appropriate, and develops contract clauses to ensure that DoD contracts impose uniform program requirements to InTPs.

2.5. UNDER SECRETARY OF DEFENSE FOR POLICY.

In accordance with DoDI 3020.45, the Under Secretary of Defense for Policy evaluates DoD Component InTP elements and provides mission assurance assessments to the OUSD(I&S).

2.6. USD(P&R).

The USD(P&R):

a. Establishes policy and prescribes practices and procedures to enable the sharing of civilian and military personnel information with the Component InTP elements. Relevant information includes, but is not limited to:

(1) Personnel files.

(2) Payroll and voucher files.

(3) Outside work and activities requests.

(4) Disciplinary files.

(5) Suspensions.

(6) Administrative leave.

b. Ensures timely reporting of insider threat related information to DoD Component InTP elements.

c. Provides policy for the implementation of military training and civilian leadership training aspects of the DoD InTP, in accordance with DoD Directive 1322.18 and Volume 410 of DoD Instruction 1400.25.

2.7. INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE (IG DOD).

In addition to the responsibilities in Paragraph 2.11., and pursuant to the authority in DoDD 5106.01, the IG DoD:

a. Prescribes procedures for access requests by the InTP involving particularly sensitive or protected information held by the IG DoD.

b. Conducts periodic evaluations of the DoD InTP as the IG DoD determines appropriate.

2.8. DOD CIO.

In accordance with DoDI 8500.01, the DoD CIO:

a. Establishes policies and develops strategies, including audit and UAM standards and capabilities, on DoD classified and unclassified information networks. In coordination with the Director of National Intelligence, ensures consistent UAM coverage between DoD systems and those systems subject to the authorities and policies of the Director of National Intelligence.

b. Coordinates with the USD(I&S) to develop guidelines and procedures to:

(1) Support and integrate cyber capabilities, including UAM, with InTP activities.

(2) Implement the requirements transmitted with the November 21, 2012 Presidential Memorandum; E.O. 13587; Section 2224 of Title 10, U.S.C.; and the Committee on National Security Systems Directive Number 504.

c. Provides oversight and guidance for the DoD Components to use or employ cyber capabilities through the ability to collect, observe, record, store, process, and share with the DoD InTP any data generated by any user of any DoD network.

d. Coordinates UAM oversight with the USD(I&S) and improves threat monitoring across all DoD networks and computer environments as technology and operating environments evolve.

e. Incorporates insider threat awareness into annual cybersecurity training for all DoD-affiliated personnel.

2.9. ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS.

In accordance with DoDI 5400.13, the Assistant to the Secretary of Defense for Public Affairs develops and employs DoD public affairs activities and capabilities to support command operations and awareness activities to deter insiders from conducting malicious activity and promotes the reporting of concerning activity to DoD Component InTP elements.

2.10. ASSISTANT TO THE SECRETARY OF DEFENSE FOR PRIVACY, CIVIL LIBERTIES, AND TRANSPARENCY.

The Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency:

a. Establishes policy and prescribes practices and procedures regarding appropriate protections for privacy and civil liberties for use by the DoD Components in the execution of their responsibilities in accordance with the DoD InTP.

b. Executes independent oversight of all intelligence and intelligence-related support provided to the DoD InTP.

2.11. DOD COMPONENT HEADS.

The DoD Component heads:

a. Establish, maintain, and provide management, accountability, and oversight of their Component's InTP that complies with all applicable laws, orders, regulations, and policy, including those regarding whistleblowers, civil liberties, and privacy protections.

b. Designate a senior official with the authority to provide management, accountability, and oversight of their Component's InTP, and make resource recommendations to the appropriate agency official.

c. Establish and maintain an insider threat hub to conduct and integrate the monitoring, analysis, reporting, and response to address insider threats through the fusion of disparate data sources.

d. Establish procedures to submit information meeting a DoD InTP reporting threshold through the enterprise capability for insider threat information management, in accordance with established reporting timelines.

e. Request DCSA analytic capabilities, to include case consultation by the Behavioral Threat Analysis Center, when needed.

f. Ensure their InTP elements cover all individuals assigned to their theater or function and promptly report information indicative of an insider threat to the individual's parent InTP hub.

g. Establish processes for access to and use of, as permitted by law and policy, commercially available information, PAI, and Component data, including but not limited to LE, intelligence and CI information and analytic products, and agency-specific information, by their insider threat hub.

h. Ensure procedures and accountability measures are in place for PAR functional subject matter experts, prevention workforce, commanders, or equivalent civilian leaders, security management personnel, InTP personnel, and other Component-designated command elements, as

appropriate, to share relevant information and report behaviors of concern by DoD personnel to the respective DoD Component InTP hub.

i. Ensure classified systems, including those authorized pursuant to the National Industrial Security Program, are monitored by UAM capabilities in accordance with the Committee on National Security Systems Directive Number 504. Ensure InTP elements use cyber monitoring capabilities on unclassified information systems in accordance with DoDM 8530.01 and based on Component priorities and risk assessment. The Component InTP, in consultation with the Component chief information officer, will have operational control and validation authority over the tool(s), requirements, configuration, use, and any new acquisitions of cyber capabilities in support of insider threat, including UAM.

j. Integrate appropriate insider threat awareness training and Component-specific reporting procedures into professional military education, commanders' courses, civilian courses, and courses for DoD contractors and volunteers who have access to DoD resources, in accordance with this issuance.

k. Implement training for the professionalization of Component InTP personnel in accordance with the November 21, 2012 Presidential Memorandum and Paragraph 3.3. of this issuance.

l. Support DoD training and awareness efforts to inform the workforce about the InTP, including participation in the annual National Insider Threat Awareness Month.

m. Refer criminal allegations or suspected criminal activities to the appropriate defense criminal investigative organization or LE organization as soon as possible in accordance with DoDI 5505.03.

n. Refer any information derived from Component threat reporting that indicates an individual has an affiliation with foreign entities, including organizations, persons, or agents, or international terrorist organizations or activities to the supporting Military Department counterintelligence organization as soon as possible in accordance with DoDI O-5240.10 and the DoD Component's CI element in accordance with DoDD 5240.06 and DoDI 5240.26.

o. Ensure Component inspector general and mission assurance programs establish requirements to assess Component InTP compliance and efficacy, including training and reporting requirements at all command levels.

p. Perform annual self-assessments for compliance and provide performance measurement and data on output, efficacy, and reporting trends through Advana, or a successor platform, to the OUSD(I&S) to improve performance, inform research, training, and resourcing requirements, as necessary.

q. Provide assessment information to the DCSA or the Office of the Director of National Intelligence National Insider Threat Task Force to independently assess Component InTP compliance.

r. Ensure the respective insider threat hub is notified of mitigation measures taken in response to a referral to facilitate performance measurement and trend analysis.

s. Comply with applicable record maintenance requirements in accordance with the Privacy Act of 1974, DoDI 5400.11, Volume 2 of DoDM 5400.11, and DoDM 5240.01.

t. Maintain and manage all records in accordance with National Archives and Records Administration-approved schedules to ensure proper maintenance, use, accessibility, and preservation, regardless of format or medium.

u. Designate and retain a record of Component-level, non-intelligence entities that are authorized to conduct InTP activities.

v. Provide a representative to departmental and interagency forums and working groups engaged in detecting, deterring, and mitigating insider threats, as appropriate.

w. Provide a Component representative to the CITP Certification Governance Council, or successor, as appropriate.

x. Ensure Component InTP hubs and arming authorities maintain communication to identify behaviors of concern that might result in arming authority-directed disarming or voluntary disarming, in accordance with DoDD 5210.56.

2.12. CHIEF, NATIONAL GUARD BUREAU.

In addition to the responsibilities in Paragraph 2.11., the Chief, National Guard Bureau develops procedures that implement DoD insider threat policy for National Guard personnel and organizations, in accordance with DoDD 5105.77 and Title 32, U.S.C.

SECTION 3: PROCEDURES

3.1. DOD INTP.

a. DoD Component InTP activities will be executed in a staff element with an analytic and behavioral threat management capability (referred to in this issuance as "hub"). The hub will manually and electronically gather, integrate, review, assess, and respond to information derived from government and commercial data sources, as necessary and appropriate, to examine concerning behaviors.

b. The DoD InTP focuses on deterring insiders from becoming threats; detecting insiders who pose a risk to personnel, installations, information, resources, or mission; and mitigating risk by informing administrative, investigative, security, or other response actions as required.

3.2. INSIDER THREAT AWARENESS TRAINING.

The DoD Components will:

a. Provide DoD employees insider threat awareness training within 30 working days of initial employment, entry on duty, and annually thereafter. All training requirements may be met by insider threat specific training or by training associated with other mission areas provided the training addresses potential threats in the workplace, and includes these topics at a minimum:

(1) The importance of detecting and reporting potentially concerning behaviors to insider threat personnel or other designated officials, including training on Component-specific reporting procedures.

(2) Methodologies of adversaries to recruit insiders and collect classified information.

(3) Indicators of insider threat behavior and procedures to report such behavior.

(4) Other mission reporting requirements, as applicable.

b. Verify that employees have completed the required insider threat awareness training contained in these standards.

c. Conduct strategic engagement and outreach activities to supplement annual training requirements to enhance insider threat reporting to identify, mitigate, and counter insider threats.

3.3. INSIDER THREAT PERSONNEL TRAINING, EDUCATION, AND PROFESSIONALIZATION.

The DoD Component heads will ensure that InTP personnel training and professionalization plans are established, implemented, and measured for efficacy for all military, civilian, and DoD contractor personnel performing InTP functions. At a minimum, the plan will:

a. Require that all military, civilian, and DoD contractor personnel assigned InTP responsibilities receive training commensurate with their responsibilities.

b. Ensure that InTP capabilities training aligns with national and DoD policy.

c. Leverage the CITP program or its successor to professionalize InTP personnel through the CITP-fundamentals and CITP-analysis certifications.

d. Require assigned insider threat hub analytic personnel to achieve both CITP-fundamentals and CITP-analysis certifications or designated successor certifications within 2 years of entry on duty.

e. Integrate CITP achievement and maintenance as one of the decision criteria in hiring, selection, and promotion for InTP personnel.

f. Be regularly refined and adapted to evolving threats or concerns posed to the DoD.

g. Be regularly reviewed by the DoD Component InTP for compliance with this issuance and report any potential deficiencies to the OUSD(I&S).

3.4. COLLECTION, STORAGE, AND RETENTION OF INFORMATION.

Through an integrated capability to share, collect, analyze, monitor, and audit information, the DoD Component insider threat hubs will, consistent with law and policy, assemble data; integrate, review, and assess risks and threats; and recommend mitigating measures using relevant behavior-based data derived from various sources, including:

a. Agency-specific information.

b. Cybersecurity.

c. CI

d. Command climate assessments pursuant to DoDI 6400.11.

e. Enterprise asset management.

f. HR, including civilian and military personnel management.

g. Information assurance.

h. Integrated primary prevention.

i. LE

j. OIG DoD and DoD Component inspector generals.

k. PAI.

l. Reports concerning workplace violence.

m. Security-related information, including administrative inquiries or investigations, and polygraph.

n. Other commercial and government data sources as the DoD Component senior official or their designee considers necessary and appropriate to identify, mitigate, and counter insider threats.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
CI	counterintelligence
CITP	certified insider threat professional
DCSA	Defense Counterintelligence and Security Agency
DoD CIO	DoD Chief Information Officer
DoDD	DoD directive
DoDI	DoD instruction
DoDM	DoD manual
E.O.	Executive order
HR	human resources
IG DoD	Inspector General of the Department of Defense
InTP	insider threat program
LE	law enforcement
OIG DoD	Office of Inspector General of the Department of Defense
OUSD(I&S)	Office of the Under Secretary of Defense for Intelligence and Security
PAI	publicly available information
PAR	prevention, assistance, and response
PL	public law
UAM	user activity monitoring
U.S.C.	United States Code
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(P&R)	Under Secretary of Defense for Personnel and Readiness

G.2. DEFINITIONS.

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

TERM	DEFINITION
agency-specific information	Information from the following DoD data sources and categories: Insider threat. Identity matching engine for security and analysis. UAM. Internal misconduct investigations and disciplinary action. Civilian disciplinary actions (conduct-related). Security incidents and violations. Information technology. Self-reporting. Third-party reporting.
authorized access	Maintaining an active DoD common access card, DoD identification card, pass, or credential by a DoD organization that can be used as proof of identity to gain physical or logical (system or network) access to a DoD facility, network, system, or resource.
concerning behaviors	Observable behaviors or actions that suggest an insider may be planning or carrying out an act that may constitute an insider threat.
defense criminal investigative organization	Defined in DoDI 5505.03.
DoD Component InTP	The required elements of a DoD Component head's responsibilities as required by this issuance and directed to agency heads by E.O. 13587, the November 21, 2012 Presidential Memorandum, and Section 951 of PL 114-328.
enterprise information technology system	The primary insider threat case management system with advanced analytic tools for capturing, consolidating, storing, analyzing, managing, sharing, and reporting insider threat-related data.

TERM	DEFINITION
foreign national	Defined in DoDD 5230.20.
insider	Any person who has, or once had, authorized access to information, a facility, network, a person, or a resource of the DoD.
insider threat	A threat presented by a person who has, or once had, authorized access to information, a facility, network, a person, or a resource of the DoD and wittingly or unwittingly commits an act in contravention of law or policy that resulted in or might result in harm through the loss or degradation of government or company information, resources, or capabilities, or a destructive act, which may include physical harm to oneself or another.
insider threat hub	The InTP staff element with an analytic and behavioral threat management capability that manually and electronically gathers, integrates, reviews, assesses, and responds to information derived from CI, security, HR, LE, the monitoring of network user activity, and other available sources, as necessary and appropriate, to examine concerning behaviors to deter, detect, and mitigate risk by informing administrative, investigative, or other response actions as required.
integrated primary prevention	Defined in DoDI 6400.09.
publicly available information	Defined in DoDD 3115.18.
senior official	A DoD official who has been designated by the DoD Component head to provide direction, management, and oversight of that DoD Component's InTP.
serious threat	A threat that presents a reasonable risk to life or limb or has the potential to degrade or destroy a critical intelligence or operational capability of DoD.
system of records notice	Defined in Office of Management and Budget Circular Number A- 108.
terrorism	The unlawful use of violence or threat of violence, often motivated by religious, political, or other ideological beliefs, to instill fear and coerce governments or societies in pursuit of goals that are usually political.

TERM	DEFINITION
threat management	Managing a subject's behavior through interventions and strategies to disrupt or prevent an act of targeted violence.
UAM	Defined in Committee on National Security Systems Directive Number 504.
violent behavior	Defined in DoDI 1438.06.
workplace violence	Defined in DoDI 1438.06.

REFERENCES

Code of Federal Regulations, Title 32

Code of Federal Regulations, Title 45

Committee on National Security Systems Directive Number 504, "Directive on Protecting National Security Systems from Insider Threat," September 27, 2021

Defense Federal Acquisition Regulation Supplement, current edition

DoD Directive 1322.18, "Military Training," October 3, 2019

DoD Directive 3115.18, "DoD Access to and of Publicly Available Information (PAI)," June 11, 2019, as amended

DoD Directive 5105.77, "National Guard Bureau (NGB)," October 30, 2015, as amended

DoD Directive 5106.01, "Inspector General of the Department of Defense (IG DoD)," April 20, 2012, as amended

DoD Directive 5143.01, "Under Secretary of Defense for Intelligence and Security (USD(I&S))," October 24, 2014, as amended

DoD Directive 5200.43, "Management of the Defense Security Enterprise," October 1, 2012, as amended

DoD Directive 5210.41, "Security Policy for Protecting Nuclear Weapons," January 22, 2015, as amended

DoD Directive 5210.56, "Arming and the Use of Force," November 18, 2016, as amended

DoD Directive 5230.20, Visits and Assignments of Foreign Nationals," June 22, 2005, as amended

DoD Directive 5240.02, "Counterintelligence (CI)," March 17, 2015, as amended

DoD Directive 5240.06, "Counterintelligence Awareness and Reporting (CIAR)," May 17, 2011, as amended

DoD Instruction 1400.25, Volume 410, "DoD Civilian Personnel Management System: Training, Education, and Professional Development," September 25, 2013, as amended

DoD Instruction 1438.06, "DoD Workplace Violence Prevention and Response Policy," January 16, 2014, as amended

DoD Instruction 2000.26, "DoD Use of the Federal Bureau of Investigation (FBI) eGuardian System," December 4, 2019

DoD Instruction 3020.45, "Mission Assurance Construct," August 14, 2018, as amended

DoD Instruction 5210.42, "DoD Nuclear Weapons Personnel Reliability Assurance," April 27, 2016, as amended

DoD Instruction O-5210.63, "DoD Procedures for Security of Nuclear Reactors and Special Nuclear Materials (SNM)," November 21, 2006, as amended

DoD Instruction O-5240.10, "Counterintelligence (CI) in the DoD Components," April 27, 2020

DoD Instruction 5240.19, "Counterintelligence Support to the Defense Critical Infrastructure Program (DCIP)," January 31, 2014, as amended

DoD Instruction 5240.26, "Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat," May 4, 2012, as amended

DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019, as amended

DoD Instruction 5400.13, "Public Affairs (PA) Operations," October 15, 2008

DoD Instruction 5505.03, "Initiation of Investigations by Defense Criminal Investigative Organizations," August 2, 2023

DoD Instruction 6025.18, "Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care Programs," March 13, 2019

DoD Instruction 6400.09, "DoD Policy on Integrated Primary Prevention of Self-Directed Harm and Prohibited Abuse or Harm," September 11, 2020

DoD Instruction 6400.11, "DoD Integrated Primary Prevention Policy for Prevention Workforce and Leaders," December 22, 2022, as amended

DoD Instruction 6490.04, "Mental Health Evaluations of Members of the Military Services," March 4, 2013, as amended

DoD Instruction 6490.08, "Command Notification Requirements to Dispel Stigmas in Providing Mental Health Care to Service Members," September 6, 2023

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended

DoD Instruction 8580.02, "Security of Individually Identifiable Health Information in DoD Health Care Programs," August 12, 2015

DoD Manual 5200.02, "Procedures for the DoD Personnel Security Program (PSP)," April 3, 2017, as amended

DoD Manual S-5210.41, "(U) Nuclear Weapon Security Manual," May 4, 2022

DoD Manual 5210.42, "Nuclear Weapons Personnel Reliability Program," January 13, 2015, as amended

DoD Manual S-5210.92, "Physical Security Requirements for Nuclear Command and Control (NC2) Facilities (U)," August 26, 2010, as amended

DoD Manual 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities," August 8, 2016

DoD Manual 5400.11, Volume 2, "DoD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan" May 6, 2021

DoD Manual 8530.01, "Cybersecurity Activities Support Procedures," May 31, 2023

Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the 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

Public Law 104-191, "Health Insurance Portability and Accountability Act of 1996," August 21, 1996

Public Law 112-81, Section 922, "National Defense Authorization Act for Fiscal Year 2012," December 31, 2011

Public Law 114-328, Section 951, "National Defense Authorization Act for Fiscal Year 2017," December 23, 2016

Public Law 116-283, Section 1090, "William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021," January 1, 2021

Secretary of Defense Memorandum, "Implementation of Section 1090 of the National Defense Authorization Act for Fiscal Year 2021," November 18, 2021

United States Code, Title 5

United States Code, Title 10, Section 2224

United States Code, Title 32