Department of Defense
DIRECTIVE

NUMBER 5205.16
September 30, 2014
Incorporating Change 1, Effective January 25, 2017

USD(I)

SUBJECT: The DoD Insider Threat Program

References: See Enclosure 1

1. PURPOSE. In accordance with sections 113 and 131 through 137, *and 2672* of Title 10, United States Code (U.S.C.) (Reference (a)); Presidential Memorandum (Reference (b)); Executive Orders (E.O.s) 12333, 13526, and 13587 (References (c), (d), and (e)); section 922 of Public Law 112-81 (Reference (f)); National Security Directive 42 (Reference (g)), and Committee on National Security Systems Directive 504 (Reference (h)), this directive:

a. Establishes policy and assigns responsibilities within DoD to develop and maintain an insider threat program to comply with the requirements and minimum standards to prevent, deter, detect, and mitigate the threat *insiders may pose to DoD and U.S. Government installations, facilities, personnel, missions, or resources*. This *threat* can include 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.

b. Identifies appropriate training, education, and awareness initiatives that may be made available to DoD personnel and contractors in accordance with Reference (b).

c. Ensures appropriate DoD policies, including but not limited to counterintelligence (CI), cybersecurity, security, civilian and military personnel management, workplace violence, emergency management, law enforcement (LE), and antiterrorism (AT) risk management, are evaluated and modified to effectively address insider threats to DoD.

d. Cancels Secretary of Defense Memorandum (Reference (i)).

e. Incorporates and cancels Deputy Secretary of Defense Memorandum (Reference (j)).

2. APPLICABILITY. This directive:

a. 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 the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within DoD (referred to collectively in this directive as the "DoD Components").

(2) Contractors and other non-DoD entities that have authorized access to DoD resources as required by their contract or agreement *and who meet the definition of insider as set forth in the definitions section of this directive*.

(3) Individuals who volunteer and donate their services to the DoD Components, including non-appropriated fund instrumentalities, pursuant to DoD Instruction (DoDI) 1100.21 (Reference (k)) *and who meet the definition of insider as set forth in the definitions section of this directive*.

b. Will not alter or supersede:

(1) The existing authorities and policies of the Director of National Intelligence regarding the protection of sensitive compartmented information and special access programs for intelligence as directed by Reference (c) and other laws and regulations.

(2) Existing statutes, E.O.s, and DoD policy issuances governing access to or dissemination of LE, LE sensitive, or classified LE information.

(3) Existing suspicious activity reporting and dissemination requirements as outlined in DoDI 2000.26 (Reference (l)).

3. POLICY. It is DoD policy that:

a. DoD will implement the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs in accordance with References (b), (e), (f), and (h).

b. The threat that an insider *may* do harm to the security of the United States requires the integration and synchronization of programs across the Department. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of resources or capabilities.

c. Through an integrated capability to monitor and audit information for insider threat detection and mitigation, the DoD Insider Threat Program will gather, integrate, review, assess, and respond to information derived from CI, security, cybersecurity, civilian and military personnel management, workplace violence, AT risk management, LE, the monitoring of user activity on DoD information networks, and other sources as necessary and appropriate to identify, mitigate, and counter insider threats.

d. Appropriate training, education, and awareness of the insider threat will be provided to DoD military and civilian personnel, DoD contractors, and volunteers who have access to DoD resources.

e. The collection, use, maintenance, and dissemination of information critical to the success of DoD efforts to counter insider threats must comply with all applicable laws and DoD policy issuances, including those regarding whistleblower, civil liberties, and privacy protections.

(1) Personally identifiable information (PII) for U.S. persons must be handled in accordance with section 552a of Title 5, U.S.C. (also known as "The Privacy Act of 1974" (Reference (m))), DoD Directive (DoDD) 5400.11 (Reference (n)), and DoD 5400.11-R (Reference (o)).

(2) Defense Intelligence Components will handle U.S. persons' PII in accordance with ~~DoD 5240.1-R~~ *DoD Manual 5240.01* (Reference (p)).

(3) Activities related to the insider threat program, including information sharing and collection, will comply with DoDI 1000.29 (Reference (q)).

(4) Information on individuals and organizations not affiliated with the DoD will not be collected unless allowed pursuant to DoDD 5200.27 (Reference (r)).

(5) Personally identifiable health information must be handled in accordance with Public Law 104-191 (Reference (s)), parts 160, 162, and 164 of Title 45, Code of Federal Regulations (Reference (t)), DoDI 6490.04 (Reference (u)), DoDI 6490.08 (Reference (v)), DoD 6025.18-R (Reference (w)), and DoD 8580.02-R (Reference (x)).

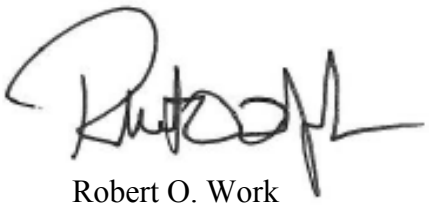
4. RESPONSIBILITIES. See Enclosure 2.

5. INFORMATION COLLECTIONS REQUIREMENTS. The DoD Insider Threat Program annual progress report and quarterly Key Information Sharing and Safeguarding Indicators questionnaire self-assessment compliance reports, referred to in paragraphs 1e, 5d, 5e, 6e, 6f, 8g, 11f and 11h of Enclosure 2 of this directive, have been assigned report control symbol DD-CIO(A,Q)2561 in accordance with the procedures in Volume 1 of DoD Manual 8910.01 (Reference (y)).

6. RELEASABILITY. **Cleared for public release**. This directive is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

7. EFFECTIVE DATE. This directive ~~: a. Is~~ *is* effective September 30, 2014.

~~b. Will expire effective September 30, 2024 if it hasn't been reissued or cancelled before this date in accordance with DoDI 5025.01 (Reference (z)).~~



Robert O. Work
Deputy Secretary of Defense

Enclosures
1. References
2. Responsibilities

Glossary

ENCLOSURE 1

REFERENCES

(a) Title 10, United States Code
(b) Presidential Memorandum, "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs," November 21, 2012
(c) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
(d) Executive Order 13526, "Classified National Security Information," December 29, 2009
(e) Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 7, 2011
(f) Section 922 of Public Law 112-81, "National Defense Authorization Act," December 31, 2011
(g) National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990[1]
(h) Committee on National Security Systems Directive (CNSSD) No. 504, "Directive on Protecting National Security Systems from Insider Threat," ~~January 2012~~ *February 4, 2014*
(i) Secretary of Defense Memorandum, "Information Security and Assurance Measures to Mitigate Unauthorized Removal of Information from Classified Networks," February 10, 2011 (hereby cancelled)
(j) Deputy Secretary of Defense Memorandum, "Appointment of the DoD Senior Official Charged with Overseeing Insider Threat Efforts," September 25, 2013 (hereby cancelled)
(k) DoD Instruction 1100.21, "Voluntary Services in the Department of Defense," March 11, 2002, as amended
(l) DoD Instruction 2000.26, "Suspicious Activity Reporting *(SAR)*," ~~November 1, 2011~~ *September 23, 2014*
(m) Section 552a of Title 5, United States Code (also known as "The Privacy Act of 1974")
(n) DoD Directive 5400.11, "DoD Privacy Program," ~~May 8, 2007, as amended~~ *October 29, 2014*
(o) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
(p) ~~DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 7, 1982~~ *DoD Manual 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities," August 8, 2016*
(q) DoD Instruction 1000.29 "DoD Civil Liberties Program," May 17, 2012, *as amended*
(r) DoD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense," January 7, 1980
(s) Public Law 104-191, "Health Insurance Portability and Accountability Act of 1996," August 21, 1996
(t) Title 45, Code of Federal Regulations
(u) DoD Instruction 6490.04, "Mental Health Evaluations of Members of the Military Services," March 4, 2013

[1] Document is available at http://bushlibrary.tamu.edu/research/pdfs/nsd/nsd42.pdf

(v) DoD Instruction 6490.08, "Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Service Members," August 17, 2011
(w) DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 1, 2003
(x) DoD *Instruction* 8580.02~~-R~~, "DoD Health Information Security Regulation," ~~July 12, 2007~~ *August 12, 2015*
(y) DoD Manual 8910.01, Volume 1, "DoD Information Collections Manual: Procedures for DoD Internal Information Collections," June 30, 2014
~~(z) DoD Instruction 5025.01, "DoD Issuances Program," June 6, 2014~~
(~~aa~~*z*) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," ~~November 23, 2005~~ *October 24, 2014, as amended*
(~~ab~~*aa*) DoD Directive 5240.06, "Counterintelligence Awareness and Reporting (CIAR)," May 17, 2011, as amended
(~~ac~~*ab*) DoD Instruction 5240.19, "Counterintelligence Support to the Defense Critical Infrastructure Program (DCIP)," January 31, 2014
(~~ad~~*ac*) DoD Instruction 5240.26, "Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat," May 4, 2012, as amended
(~~ae~~*ad*) DoD Directive ~~O~~ 5240.02, "Counterintelligence *(CI)*," ~~December 20, 2007, as amended~~ *March 17, 2015*
(~~af~~*ae*) DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended
(~~ag~~*af*) DoD Directive 5200.43, "Management of the Defense Security Enterprise," October 1, 2012, as amended
(~~ah~~*ag*) DoD 5200.2-R, "DoD Personnel Security Program," January 1, 1987, as amended
(~~ai~~*ah*) DoD Directive 5105.21, "Defense Intelligence Agency (DIA)," March 18, 2008
(~~aj~~*ai*) DoD Directive 5105.42, "Defense Security Service (DSS)," August 3, 2010, as amended
(~~ak~~*aj*) DoD Directive 5220.6, "Defense Industrial Personnel Security Clearance Review Program," January 2, 1992, as amended
(~~al~~*ak*) DoD Directive 5111.1, "Under Secretary of Defense for Policy (USD(P))," December 8, 1999
(~~am~~*al*) DoD Directive 5111.13, "Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD(HD&ASA))," January 16, 2009
(~~an~~*am*) DoD Directive 5124.02, "Under Secretary of Defense for Personnel and Readiness (USD(P&R))," June 23, 2008
(~~ao~~*an*) DoD Directive 1322.18, "Military Training," January 13, 2009
(~~ap~~*ao*) DoD Directive 5134.01, "Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L))," December 9, 2005, as amended
(~~aq~~*ap*) DoD Instruction 5210.42, "Nuclear Weapons Personnel Reliability Program (PRP)," July 16, 2012
(~~ar~~*aq*) DoD *Manual* 5210.42, "Nuclear Weapons Personnel Reliability Program (PRP) Regulation," ~~June 30, 2006, as amended~~ *January 13, 2015*
(~~as~~*ar*) DoD Directive 5210.41, "Security Policy for Protecting Nuclear Weapons," ~~November 1, 2004~~ *January 22, 2015*
(~~at~~*as*) DoD S-5210.41-M, "Nuclear Weapon Security Manual," July 13, 2009
(~~au~~*at*) DoD S-5210.92-M, "Physical Security Requirements for Nuclear Command and Control (NC2) Facilities, (U)" August 26, 2010

(~~av~~*au*) DoD Instruction O-5210.63, "DoD Procedures for Security of Nuclear Reactors and Special Nuclear Materials (SNM)," November 21, 2006
(~~aw~~*av*) Defense Federal Acquisition Regulation Supplement (DFARS) (current edition)
(~~ax~~*aw*) DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," ~~April 22, 2013~~ *November 21, 2014*
(~~ay~~*ax*) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
(~~az~~*ay*) Deputy Secretary of Defense Memorandum, "Appointment as the Senior Official Charged with Overseeing Classified Information Sharing and Safeguarding Efforts on Computer Networks," January 26, 2012
(~~ba~~*az*) DoD 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006, as amended
(~~bb~~*ba*) DoD Instruction 5505.17, "Collection, Maintenance, Use, and Dissemination of Personally Identifiable Information and Law Enforcement Information by DoD Law Enforcement Activities," December 19, 2012

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). In accordance with the responsibilities prescribed in DoDD 5143.01 (Reference (~~aa~~*z*)), DoDD 5240.06 (Reference (~~ab~~*aa*)), DoDI 5240.19 (Reference (~~ac~~*ab*)), DoDI 5240.26 (Reference (~~ad~~*ac*)), DoDD ~~O~~ 5240.02, (Reference (~~ae~~*ad*)), Volume 3 of DoD Manual 5200.01 (Reference (~~af~~*ae*)), and DoDD 5200.43 (Reference (~~ag~~*af*)), the USD(I):

a. Serves as the senior official and principal civilian advisor to the Secretary of Defense on the DoD Insider Threat Program. In this role, the USD(I):

(1) Provides management, accountability, and oversight of the DoD Insider Threat Program.

(2) Recommends improvements on DoD insider threat activities to the Secretary of Defense pursuant to Reference (b).

b. Develops and establishes policy, and oversees policy, strategy, plans, programs, required capabilities, and resources for DoD intelligence, CI, security, sensitive activities, and other intelligence and security-related matters as necessary to counter insider threats.

c. Ensures that personnel security policies for reinvestigations, post-adjudicative investigations, continuous evaluation, referrals for action, suspensions, and continuing security responsibilities address insider threats in accordance with DoD 5200.2-R (Reference (~~ah~~*ag*)).

d. Directs and facilitates the establishment of the DoD Insider Threat Management and Analysis Center (DITMAC) to perform the functions specified in paragraph 3.h. of this enclosure.

~~d~~*e*. In coordination with the Under Secretary of Defense for Policy (USD(P)), the DoD Chief Information Officer (DoD CIO), the Under Secretary of Defense for Personnel and Readiness (USD(P&R)), and other DoD Component heads as required:

(1) Develops guidelines and procedures to implement the requirements specified in References (b), (e), (f), and (h).

(2) Makes resource recommendations to the Secretary of Defense pursuant to References (b) and (~~aa~~*z*) in support of DoD insider threat activities.

(3) Within 150 days of the effective date of this directive, develops procedures to implement the Insider Threat Program (e.g., the use of social media and the application of adjudication guidelines).

~~e~~*f*. Monitors and reports progress on implementing the DoD Insider Threat Program to the Secretary of Defense in accordance with Reference (b).

~~f~~*g*. Identifies and oversees a DoD insider threat working group in accordance with Reference (~~ag~~*af*), to implement the requirements listed in Reference (b).

~~g~~*h*. Provides a representative to departmental and interagency insider threat forums or intelligence and security forums engaged in countering insider threats.

~~h~~*i*. Provides appropriate input to the DoD CIO for the report listed in paragraph 8e of this enclosure.

~~i~~*j*. Consults with the Office of the General Counsel of the Department of Defense in developing and implementing this program.

2. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). Under the authority, direction, and control of the USD(I), and in addition to the responsibilities in section 10 of this enclosure, the Director, DIA:

a. Develops and recommends processes, procedures, and tools, to include the use of commercial-off-the-shelf technologies, to enhance the quality of DoD CI capabilities and activities to counter insider threats.

b. Provides intelligence support to inform DoD civilian and military personnel management policy, as well as support to CI, cybersecurity, AT risk management, and security activities to counter insider threats, as authorized.

c. Ensures that the cybersecurity program associated with the Joint Worldwide Intelligence Communications System provides effective security against unauthorized disclosure and similar insider threats in accordance with DoDD 5105.21 (Reference (~~ai~~*ah*)).

3. DIRECTOR, DEFENSE SECURITY SERVICE (DSS). Under the authority, direction, and control of the USD(I), and in addition to the responsibilities in section 10 of this enclosure, the Director, DSS:

a. Conducts CI functional services for cleared defense industrial base (DIB) critical assets in coordination with the DoD Components; identifies intelligence gaps related to protecting DIB critical assets; and submits CI collection and production requirements to DIA and the intelligence sector Critical Infrastructure Assurance Officer (CIAO) in accordance with Reference (~~ac~~*ab*).

b. Develops requirements and requests for threat assessments for DIB critical assets. Provides industrial security threat information and CI-related information to CI organizations supporting the DIB pursuant to Reference (~~ac~~*ab*).

c. Monitors DIB security, threats, suspicious incidents, and countermeasures implementation in coordination with the ~~Assistant Secretary of Defense for Homeland Defense and America's Security Affairs (ASD(HD&ASA))~~ *Assistant Secretary of Defense for Homeland Defense and Global Security (ASD(HD&GS))*, *the Military Department Counterintelligence Operations*, and the Director, Defense Contract Management Agency (DCMA). As appropriate, notifies the Director, DCMA, the appropriate DoD Component head, ~~ASD(HD&ASA)~~ *ASD(HD&GS)*, supporting CI support official, intelligence sector CIAO, and the Director, DIA, when changing conditions could result in an increased risk to DoD resources.

d. Incorporates insider threat education and awareness material into DSS security education and training programs provided to DoD Components and *cleared* DoD contractors.

e. Provides oversight, training, and guidance in accordance with DoDD 5105.42 (Reference (~~aj~~*ai*)) to cleared contractors regarding insider threats.

f. Provides a representative to departmental and interagency forums engaged in countering insider threats.

g. In coordination with the DoD Consolidated Adjudications Facility (DoD CAF), ensures prompt actions are taken in accordance with DoDD 5220.6 (Reference (~~ak~~*aj*)) to suspend eligibility for access to classified information when DSS or DoD CAF receives information that there is a reasonable basis for concluding that continued access to classified information *by cleared contractor personnel poses a threat to national security*.

h. Establishes and oversees the operation of the DITMAC. The DITMAC will:

(1) Consistent with paragraph 1.a., oversee the mitigation of insider threats to DoD and U.S. Government installations, facilities, personnel, missions, or resources.

(2) Assess enterprise-level risks, refer recommendations for action, synchronize responses, and oversee resolution of identified issues on the insider threats listed in paragraph 3.h.(1).

(3) Develop enterprise-level risk reporting criteria (thresholds) to facilitate component reporting of potential threat information and assess the effectiveness of actions taken by reporting elements to address, mitigate, or resolve the threat posed to DoD missions and resources.

(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 the collaboration and sharing of insider threat information among DoD Components.

4. USD(P). The USD(P) facilitates staff assistance and necessary support to the USD(I), the DoD CIO, the USD(P&R), and other OSD Component heads to implement the standards of References (b) and (e) in accordance with DoDD 5111.1 (Reference (~~al~~*ak*)).

5. ~~ASD(HD&ASA)~~ *ASD(HD&GS)*. Under the authority, direction, and control of the USD(P) and in accordance with DoDD 5111.13 (Reference (~~am~~*al*)), the ~~ASD(HD&ASA)~~ *ASD(HD&GS)*:

a. Participates in departmental and interagency forums engaged in countering insider threats.

b. Evaluates and develops DoD AT and other applicable policies, including AT risk management, to ensure they fully address insider threats to DoD personnel and resources.

c. Collaborates with the USD(I), the USD(P&R), and the DoD CIO to develop guidelines and procedures for the implementation of requirements contained in References (b), (e), (f), and (h).

d. Provides appropriate input to the DoD CIO for the report listed in paragraph 8e of this enclosure.

e. Provides appropriate input to the USD(I) for the report listed in paragraph 1e of this enclosure.

6. USD(P&R). The USD(P&R):

a. Develops policy identifying the types of civilian and military personnel management information that will be shared with the DoD Insider Threat Program as it relates to countering insider threats in accordance with Reference (b) and DoDD 5124.02 (Reference (~~an~~*am*)).

b. Collaborates with the USD(I), the USD(P), and the DoD CIO to develop guidelines and procedures for the implementation of requirements contained in References (b) and (e).

c. Ensures the integration of insider threat education and awareness training efforts into overall military training and training transformation initiatives in accordance with DoDD 1322.18 (Reference (~~ao~~*an*)).

d. Provides a representative to departmental and interagency forums engaged in countering insider threats.

e. Provides input to the DoD CIO for the report listed in paragraph 8e of this enclosure.

f. Provides input to the USD(I) for the report listed in paragraph 1e of this enclosure.

7. UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS (USD(AT&L)). In accordance with DoDD 5134.01 (Reference (~~ap~~*ao*)), the USD(AT&L):

a. Advises the DoD Components on the requirements of insider threat policies as related to the nuclear enterprise and the Nuclear Weapons Personnel Reliability Program in accordance with DoDI 5210.42, DoD *Manual* 5210.42~~-R~~, DoDD 5210.41, DoD S-5210.41-M, DoD S-5210.92-M and DoDI O-5210.63 (References (~~aq~~*ap*) through (~~av~~*au*)).

b. Develops policy or amends the Defense Federal Acquisition Regulation Supplement (Reference (~~aw~~*av*)) and develops contract clauses to ensure DoD contracts impose uniform insider threat program requirements.

c. Provides research, development, test and evaluation support for potential material solutions.

8. DoD CIO. In accordance with DoDD 5144.02 (Reference (~~ax~~*aw*)) and DoDI 8500.01 (Reference (~~ay~~*ax*)), the DoD CIO:

a. Develops and implements policy and strategy, to include audit and user activity monitoring standards, to counter insider threats on DoD information networks in accordance with References (e) through (h).

b. Collaborates with the USD(I), USD(P), and USD(P&R) to develop guidelines and procedures for the implementation of the requirements contained in References (b), (e), (f), and (h).

c. Incorporates insider threat education and awareness into annual cybersecurity training.

d. Provides a representative to departmental and interagency forums engaged in countering insider threats.

e. Oversees DoD Component self-assessments on DoD compliance with policies and standards issued pursuant to Reference (e) and reports the results of these self-assessments to the Senior Information Sharing and Safeguarding Steering Committee in accordance with Deputy Secretary of Defense memorandum (Reference (~~az~~*ay*)).

f. Facilitates independent assessments of the implementation of DoD Insider Threat Program in accordance with References (b) and (e).

g. Provides appropriate input to the USD(I) for the report listed in paragraph 1e of this enclosure, pursuant to the requirements specified in Reference (b).

9. DEPUTY CHIEF MANAGEMENT OFFICER (DCMO) OF THE DEPARTMENT OF DEFENSE. The DCMO:

a. Establishes policy and oversees its implementation to ensure compliance with all laws and regulations regarding privacy and civil liberties, in accordance with References (m) through (o).

b. Establishes policy and operating procedures regarding appropriate protections for privacy and civil liberties for use by the OSD and DoD Component heads in the execution of their responsibilities under the DoD Insider Threat Program.

c. Ensures that the DoD CAF provides actionable information regarding insider threats to the USD(I) and promptly initiates actions to review eligibility for access to classified information or eligibility for a sensitive National Security position. Pursuant to Reference (~~ak~~*aj*), DoD CAF will also ensure prompt action, in coordination with DSS, to suspend eligibility for access to classified information when DSS or DoD CAF receives information that ~~a cleared contractor's~~ continued access to classified information ~~poses an imminent threat to the national interest~~ *by cleared contractor personnel poses a threat to national security*.

d. Advises the DoD Components on the requirements of Reference (p) for the handling of PII derived from intelligence sources in the establishment and implementation activities of the DoD Insider Threat Program.

10. DoD COMPONENT HEADS. The DoD Component heads:

a. Implement the minimum standards for Executive Branch insider threat programs listed in Reference (b) in accordance with the DoD implementation plan prescribed in paragraph 1e(1) of this enclosure.

b. Establish or maintain a multi-disciplinary threat management capability to conduct and integrate the monitoring, analysis, reporting, and response to insider threats. Establish procedures for a multi-disciplinary threat management capability that:

(1) Complies with References (m) and (s), and all other applicable laws and DoD policies.

(2) Includes the ability to share relevant LE, civilian and military personnel management, mental health, cybersecurity, security, and CI information with commanders (or civilian equivalents) Component-wide.

c. Facilitate timely, informed decision-making by ensuring the following subject matter expertise and multi-disciplinary capabilities are readily available to all commanders (or civilian equivalents):

(1) LE.

(2) CI.

(3) Mental health.

(4) Security.

(5) Civilian and military personnel management.

(6) Legal.

(7) Cybersecurity.

d. Establish Component insider threat management forums to monitor implementation of this directive.

e. Verify insider threat program implementation and policy conformance by contractors and other non-DoD entities that have authorized access to DoD resources as required by contract or agreement pursuant to DoD 5220.22-M (Reference (~~ba~~*az*)).

f. Incorporate insider threat education and awareness into annual CIAR training in accordance with References (~~ab~~*aa*) and (~~ac~~*ad*).

g. Provide a representative to departmental and interagency forums engaged in countering insider threats.

h. Provide information to the USD(I) for the report listed in paragraph 1f of this enclosure.

i. Provide input to the DoD CIO for the report listed in paragraph 8e of this enclosure.

11. SECRETARIES OF THE MILITARY DEPARTMENTS. In addition to the responsibilities in section 10 of this enclosure, the Secretaries of the Military Departments evaluate their LE policies and operating procedures to ensure they address the information sharing requirements prescribed in DoDI 5505.17 (Reference (~~bb~~*ba*)).

12. COMMANDER, UNITED STATES STRATEGIC COMMAND (CDRUSSTRATCOM). In addition to the responsibilities in section 10 of this enclosure, and in coordination with the Commander, United States Cyber Command, the CDRUSSTRATCOM coordinates with the DoD CIO through the Chairman of the Joint Chiefs of Staff concerning actions to counter insider threats on DoD information networks.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AT	Antiterrorism
~~ASD(HD&ASA)~~	~~Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs~~
ASD(HD&GS)	*Assistant Secretary of Defense for Homeland Defense and Global Security*
CDRUSSTRATCOM	Commander, United States Strategic Command
CI	Counterintelligence
DCMA	Defense Contract Management Agency
DCMO	Deputy Chief Management Officer
DIA	Defense Intelligence Agency
DIB	defense industrial base
DITMAC	*DoD Insider Threat Management and Analysis Center*
DoD CAF	DoD Consolidated Adjudications Facility
DoD CIO	DoD Chief Information Officer
DoDD	DoD Directive
DoDI	DoD Instruction
DSS	Defense Security Service
E.O.	Executive order
PII	personally identifiable information
U.S.C.	United States Code
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
USD(P&R)	Under Secretary of Defense for Personnel and Readiness

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purposes of this directive.

CI. Defined in Reference (~~a~~*fae*).

DoD policy issuances. Issuances published by the DoD that establish DoD policy, designate authority, assign responsibilities, or provide procedures. Issuances include DoD directives, instructions, and directive-type memoranda.

insider. ~~Any person with authorized access to DoD resources by virtue of employment, volunteer activities, or contractual relationship with DoD.~~ *A person who has or had been granted eligibility for access to classified information or eligibility to hold a sensitive position. These individuals include Active and Reserve Component (including National Guard) military personnel, civilian employees (including non-appropriated fund employees), and DoD contractor personnel; this includes officials or employees from federal, State, local, tribal and private sector entities affiliated with or working with DoD who have been granted access to classified information by DoD based on an eligibility determination made by DoD or by another federal agency authorized to do so.*

insider threat. The threat ~~an insider will use her or his authorized access, wittingly or unwittingly, to do harm to the security of the United States~~ *insiders may pose to DoD and U.S. Government installations, facilities, personnel, missions, or resources*. This *threat* can include 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.

senior official. The DoD official, designated by a DoD Component head, that is responsible for the direction, management, and oversight of the component's insider threat program.

social media. Web-based tools, websites, applications, and media that connect users and allow them to engage in dialogue, share information, collaborate, and interact.

Social media websites are oriented primarily to create a rich and engaging user experience.

In social media, users add value to the content and data online; their interactions with the information (e.g., both collectively and individually) can significantly alter the experiences of subsequent users.