Insider Threat Essential Body of Knowledge (EBK)

TECHNICAL COMPETENCIES AND AREAS OF EXPERTISE

Insider Threat COMMUNITY FUNDAMENTALS

C3. Policy and Directives
Complies with and stays current on relevant Insider Threat regulations, guidelines, laws, and directives.

	PD-AoE1	Insider Threat Policies
TCO 1	Scope	Executive Order 13587; National Insider Threat Policy and Minimum Standards; National Insider Threat Task Force (NITTF) Guidance; Department of Defense Directive (DoDD) 5205.16; Department of Defense Instruction (DoDI) 5205.83; National Defense Authorization Act (NDAA) FY17 Section 951; NDAA FY18; National Industrial Security Program Operating Manual (NISPOM); System of Records Notice (SORN); Prevention, Assistance, and Response (PAR) memo; DoD Performance and Accountability Report; Intelligence Community Directives; Insider Threat Reporting Standards; 811 referral process; DITMAC Reporting Thresholds

	PD-AoE2	Insider Threat Program
TCO 2	Scope	Goals and objectives; Concepts and terminologies (e.g., minimum standards, Multi-disciplinary Insider Threat Working Groups, Potential Risk Indicators, Threshold events); Insider Threat Hub and Spokes; Role of Hub Analyst vs. DoD Insider Threat Management and Analysis Center (DITMAC) Analyst; Insider Threat Case Management process; DITMAC; Office of the Under Secretary of Defense (Intelligence) (OUSD-I) Implementation Plan

	PD-AoE3	Protecting Civil Liberties
TCO 3	Scope	First Amendment Protections; Fourth Amendment Rights; DoDI 1325.06; DoD Military Whistleblower Act of 1988 (DoDD 7050.06); Whistleblower Act of 1989; Intelligence Community Whistleblower Act of 1998; DoD Privacy Program (DoD 5400.11-R); DoD Freedom of Information Act Program (FOIA/DoDD 5400.07); DoD Health Information Privacy Regulation (DoD 6025.18-R); Health Insurance Portability and Accountability Act (HIPAA); Executive Order 12333 (United States Intelligence Activities); Notice and Consent Banners; ADA; Privacy Act 1974; EEO

DISCIPLINE

C4. Social and Behavioral Science
Knowledge of and skill in recognizing Social and Behavioral Science (SBS) concepts, principles, theories, and methods to deter, detect, assess, and insider threat.

	SBS-AoE1	Psychology of Insider Threat
TCO 4	Scope	Terms of Reference, concepts, and principles (e.g., behavioral model of insider threat, potential risk indicator, critical pathways), predispositions, stressors, concerning behaviors, organizational responses to concerning behaviors); Role of SBS in production of Insider Threat products (e.g., consultation, assessment of behavior, influence mitigation, training and research); Holistic behavioral data; Potential Risk Indicators (PRIs; e.g., access attributes; professional lifecycle and performance; foreign considerations; security and compliance incidents; technical activity; criminal, violent, or abusive conduct; financial considerations; substance abuse and addictive behaviors; judgment, character, and psychological conditions); Psychological factors of the insider threat; Real-time case reviews; Case Studies

PROFESSIONAL TRADECRAFT

C5. Researching
Identifies a need for and knows where or how to gather information. Obtains, evaluates, organizes, and maintains information. Understand the Potential Risk Indicators (PRIs), DoD Insider Threat Management and Analysis Center (DITMAC) thresholds, and capabilities of each pillar.

	R-AoE1	Information Protection
TCO 5	Scope	Privacy and civil liberties; Protection of Personally identifiable information (PII); Information collection limitations; Insider Threat Security Classification Guide; Records Management; Classification, Derivative classification and aggregation; USD(I) Classification Guide; NITTF classification guide; DoD 5200.01; Freedom of Information Act (FOIA)

	R-AoE2	Investigative and Operational Viability
TCO 6	Scope	Preserving chain of custody and integrity of collected information; The investigative lifecycle

	R-AoE3	Counterintelligence (CI) Pillar
TCO 7	Scope	Terms of Reference, concepts, and principles (e.g., contact with foreign nationals, foreign visits, foreign travel, finances, adversarial tradecraft tactics, techniques, and procedures (TTPs), elicitation, polygraph results); Capabilities, authorities, and jurisdictions of CI organizations and/or elements; Role of CI data in Insider Threat assessments and mitigation; DoD 5240.1-R; DoDD 5240.06; Title 50, U.S. Code Section 402A; Foreign Intelligence Entity (FIE) collection priorities; CI National Intelligence Priorities Framework (NIPF) topics; FIE tactics, techniques, and procedures; Understand anomalous behaviors within the CI pillar

	R-AoE4	Cyber Pillar
TCO 8	Scope	Terms of Reference, concepts, and principles (e.g., enterprise audit monitoring tool audit logs, authentication of people, User activity monitoring (UAM) for data analysis, UAM trigger development – suicide/workplace theft/violence, profile data, printer log data, privileged user, trusted agents, download history); Role of Cyber data in Insider Threat assessments and mitigation; DoDI 8500.01; Committee on National Security Systems Directive (CNSSD) 504; Long term analysis of UAM data; Understand anomalous behaviors within the Cyber pillar; Identifying privileged users

	R-AoE5	Human Resources (HR) Pillar
TCO 9	Scope	Terms of Reference, concepts, and principles (e.g., Basic employment records; disciplinary actions, performance reviews, transfer applications, awards information, Timesheet data, leave approvals, travel card data, government purchase card data); Role of HR in Insider Threat assessments and mitigation (e.g., performance counseling, remedial training, compliance mandate, performance improvement plan, employee assistance referral, suspension of employment, termination of employment); Identifying minimum access potential insider threat needs to perform their job; Identify the field of work assigned to potential insider threat; Understand anomalous behaviors within the HR pillar; FMLA

	R-AoE6	Law Enforcement (LE) Pillar
TCO 10	Scope	Terms of Reference, concepts, and principles (e.g., arrest records, LE interactions, court records, public records); Role of LE in Insider Threat assessments and mitigation; Understand anomalous behaviors within the LE pillar

	R-AoE7	Legal Pillar
TCO 11	Scope	Terms of Reference, concepts, and principles (e.g., data integrity and support to inquiries); Role of Legal in Insider Threat assessments and mitigation; Understand anomalous behaviors within the Legal pillar

	R-AoE8	Behavioral Science Pillar
TCO 12	Scope	Terms of Reference, concepts, and principles; Role of Behavioral Science in Insider Threat assessments and mitigation; Knowing when and how to interact with a behavioral science professional; Mental Health data found in workforce vetting forms (e.g., SF-85 & SF-86); General understanding of what is included in behavioral considerations vs. health considerations; Understand anomalous behaviors within the Behavioral Science pillar

	R-AoE9	Security Pillar
TCO 13	Scope	Terms of Reference, concepts, and principles (Personnel Security – DoD 5200.02-M, Physical Security – DoD 5200.08-R; Information Security – DoD 5200.01, Volumes 1 through 4; contact with foreign nationals, foreign visits, foreign travel); Role of Security in Insider Threat assessments and mitigation; Title 32 Code of Federal Regulations Title 147; Adjudicative Guidelines vs. DITMAC Reporting Thresholds; Security-Based Mitigation (e.g., Access suspension, downgrades, etc.); Continuous Evaluation Process; Security Clearance Adjudicative Process; Use of Publicly Available Information (PAI); Security policies; Background investigation and workforce vetting/suitability questionnaires; Appeals documentation, Incident reports; Knowledge of who a Insider Threat analyst should leverage when an individual in question exhibits clearance related PRIs or other anomalous behavior (Security vs. Special Security Office (SSO), respectively); DoD 4105.21; Understand anomalous behaviors within the Security pillar

C6. Synthesis
Analyzes, interprets, and integrates data or other information; evaluates and prioritizes alternatives; and assesses similarities and differences in data to develop findings and conclusions.

	S-AoE1	All-Source Insider Threat Assessment
TCO 14	Scope	Concepts, principles, and standards for gathering, integrating, and analyzing CI, security, Cyber, HR, LE, and other relevant information to respond to potential insider threat indicators; Research strategy for an insider threat inquiry; Thresholds for reporting and action

	S-AoE2	All-Source Insider Threat Referral Triage
TCO 15	Scope	Compiles, reviews, interprets, correlates, and analyzes insider threat related data to identify behavior potentially indicative of a threat. Develops and recommends referral and analytic strategies.

	S-AoE3	All-Source Insider Threat Trend Analysis
TCO 16	Scope	Utilize various knowledge and skills to identify anomalous behavior/patterns of behavior indicative of an insider threat. Develop approach and actions required to produce timely, preventative, and relevant insider threat/trend analysis, indicators, referral, and mitigation strategies and advisement in direct support of senior leaders.

C7. Tools and Methods
Applies tools and methods to substantive discipline, domain, or area of work. Adapts existing tools and/or methods or employs new methodological approaches required for substantive discipline, domain, or area of work. A tool is a physical or virtual device (e.g., Analyst Notebook, Intelink, data extraction tools) used to perform work rather than something that is studied, exploited, or targeted. A method is a structured and repeatable process for carrying out work (e.g., analysis of competing hypotheses, modeling, and simulation).

	TM-AoE1	Analytic Communication
TCO 17	Scope	Criteria and standards for communicating all-source insider threat assessment results and mitigation recommendations (e.g., Analytic Standards for Analytic Products – Objective, Independent, Timely, Holistic, Descriptive; Intellectual Standards – Clarity, Accuracy, Precision, Relevance, Depth, Logical); Best practices and challenges of working with multidisciplinary teams; How to prevent group polarization, group think, and/or artificial consensus

	TM-AoE2	Critical Thinking Techniques
TCO 18	Scope	Critical thinking as a process; critical thinking techniques (e.g., Hypotheses/scenario generation; alternative analysis techniques; argument mapping); Biases (e.g. confirmation, hindsight, foresight, availability, overconfidence)

	TM-AoE3	Databases and Data Feeds
TCO 19	Scope	Function, capabilities, and accesses of local/national databases and data feeds; Government databases (e.g., military criminal investigations, security clearance and suitability investigations, security clearance incident reports, Defense Department family members eligibility for benefits, travel records, Financial Suspicious Activity Reports); Commercial databases (e.g., addresses, public records, court information including civil and criminal judgments, financial judgments and liens); Understand the difference between primary and secondary sources; Importance and "How to" for MOA (Memorandum of Agreement) and Special Leave Accrual (SLA) to ensure timely and dependable access

	TM-AoE4	DITMAC System-of-Systems (DSOS)
TCO 20	Scope	Function, capabilities, accesses, and strengths/weaknesses of DSOS; Request for Information; Analytic findings, Work flow process; DSOS Limited Distribution Node (LIMDIS)

	TM-AoE6	Structured Analytic Techniques
TCO 21	Scope	Occam's Razor; Diagnostic techniques (e.g., Key Assumptions, Quality of Information, Indicators or Signposts of Change, Analysis of Competing Hypothesis); Imaginative Thinking (e.g., Brainstorming, Outside-In Thinking, Red Team Analysis); Contrarian Techniques (e.g., Devil's Advocacy, Team A/Team B, High Impact/Low Probability Analysis); Ability to document analytic processes in a clear and understandable method

C8. Vulnerabilities Assessment and Management
Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations or enterprise or local policy, assesses the level of risk, and, if appropriate, identified potential mitigation countermeasures.

	VAM-AoE1	Insider Threat Mitigation: Individual
TCO 22	Scope	Individual mitigation response options – CI, Cyber, HR, LE, Legal, and Security (e.g., administrative actions, security violations or infractions, HR referrals, EAP, law enforcement, and/or the appropriate use of supporting CI organization); Recognize stressors and concerning behaviors on the critical pathway, discipline response options; response planning; risk assessing; mitigation impacts (positive & negative); response monitoring; reporting requirements

	VAM-AoE2	Insider Threat Mitigation: Organizational
TCO 23	Scope	Organizational mitigation response options (e.g., changes in policy or Standard Operating Procedures (SOPs), processes and procedures, education/training/awareness); mitigation impacts to the organization (positive & negative)