Insider Threat Essential Body of Knowledge

Deskside Reference

COUNTER-INSIDER THREAT TECHNICAL COMPETENCIES AND AREAS OF EXPERTISE MAPPED TO TRAINING RESOURCES

CDSE Center for Development of Security Excellence

LEARN.
PERFORM.
PROTECT.

COUNTER-INSIDER THREAT (C-InT) TECHNICAL COMPETENCIES (TCO) AND AREAS OF EXPERTISE (AOE) MAPPED TO TRAINING RESOURCES

Table of Contents

DISCLAIMER: **The CDSE Insider Threat Deskside Reference is designed to support Insider Threat Program Managers, Insider Threat Program Analyst and Operations Personnel, and Insider Threat Senior Leaders in DoD, Federal government, and cleared industry. The courseware is available at https://www.cdse.edu/catalog/insider-threat.html. The courseware was designed to meet requirements under EO 13587, the National Minimum Standards, DoDD 5205.16, and the NISPOM. Learning objectives were developed in coordination with OUSD(I) and the NITTF, and have been mapped to the Essential Body of Knowledge tested in the Counter Insider Threat Certification Exams. Matriculation through these courses does NOT guarantee the student will pass the exam(s). These materials have been recognized as potential preparatory resources and as acceptable sources of professional development units for those maintaining certification.**

Counter Insider Threat Essential Body of Knowledge (C-InT EBK)

Policy and Directives (PD)
Complies with and stays current on relevant C-InT regulations, guidelines, laws, and directives.

	PD-AoE1	Insider Threat Policies	Relevant CDSE Courses/Training
TCO 1	Scope	Executive Order 13587;	• INT122 Establishing an Insider Threat Program for Your Organization • INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT220 Preserving Investigative and Operational Viability in Insider Threat • INT230 Insider Threat Records Checks • INT240 Insider Threat Basic Hub Operations • INT250 Critical Thinking for Insider Threat Analysts • INT260 Privacy and Civil Liberties for Insider Threat • DoD Component Insider Threat Training Requirements and Resources Job Aid • Insider Threat for Senior Leaders Video • Insider Threat for DoD Security Professionals Webinar
		National Insider Threat Policy and Minimum Standards;	• INT122 Establishing an Insider Threat Program for Your Organization • INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT220 Preserving Investigative and Operational Viability in Insider Threat • INT230 Insider Threat Records Checks • INT240 Insider Threat Basic Hub Operations • INT250 Critical Thinking for Insider Threat Analysts • INT260 Privacy and Civil Liberties for Insider Threat • DoD Component Insider Threat Training Requirements and Resources Job Aid • Insider Threat Indicators in UAM Job Aid • Insider Threat Toolkit • Insider Threat for Senior Leaders Video • Insider Threat for DoD Security Professionals Webinar • UAM in Insider Threat Programs Webinar
		National Insider Threat Task Force (NITTF) Guidance;	• INT122 Establishing an Insider Threat Program for Your Organization • INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT220 Preserving Investigative and Operational Viability in Insider Threat • INT230 Insider Threat Records Checks • INT240 Insider Threat Basic Hub Operations • INT250 Critical Thinking for Insider Threat Analysts • INT260 Privacy and Civil Liberties for Insider Threat, • DoD Component Insider Threat Training Requirements and Resources Job Aid • Insider Threat Toolkit • Insider Threat for Senior Leaders Video • Insider Threat for DoD Security Professionals Webinar

		Department of Defense Directive (DoDD) 5205.16;	• INT122 Establishing an Insider Threat Program for Your Organization • INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT220 Preserving Investigative and Operational Viability in Insider Threat • INT230 Insider Threat Records Checks • INT240 Insider Threat Basic Hub Operations • INT250 Critical Thinking for Insider Threat Analysts • INT260 Privacy and Civil Liberties for Insider Threat • Customizable DoD Command Brief for Insider Threat Awareness Job Aid (pptx) • DoD Component Insider Threat Training Requirements and Resources Job Aid • Insider Threat Indicators in UAM Job Aid • DITMAC Short • Insider Threat Toolkit • Insider Threat for Senior Leaders Video • DITMAC Update Webinar • Insider Threat for DoD Security Professionals Webinar • UAM in Insider Threat Programs Webinar
		Department of Defense Instruction (DoDI) 5205.83;	• DITMAC Short • DITMAC Update Webinar
		National Defense Authorization Act (NDAA) FY17 Section 951;	• Personnel Security Toolkit, Policy and Training Tabs
		National Industrial Security Program Operating Manual (NISPOM);	• INT122 Establishing an Insider Threat Program for Your Organization • INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT220 Preserving Investigative and Operational Viability in Insider Threat • INT230 Insider Threat Records Checks • INT240 Insider Threat Basic Hub Operations • INT250 Critical Thinking for Insider Threat Analysts • INT260 Privacy and Civil Liberties for Insider Threat • Insider Threat Programs for the Critical Manufacturing Sector Implementation Guide Job Aid • Insider Threat Programs (ITP) for Industry Job Aid • Sample Insider Threat Program Plan for Industry Job Aid • Insider Threat Resources for Industry Senior Officials Job Aid • Insider Threat for Senior Leaders Video • Industry and Insider Threat Webinar • Virtual Insider Threat Symposium for Industry Webinar
		System of Records Notice (SORN);	• INT260 Privacy and Civil Liberties for Insider Threat
		Prevention, Assistance, and Response (PAR) memo;	• PAR Short
		DoD Performance and Accountability Report;	
		Intelligence Community Directives;	• INT250 Critical Thinking for Insider Threat Analysts • Personnel Security Toolkit, Policy and Training Tabs

		Insider Threat Reporting Standards;	• INT122 Establishing an Insider Threat Program for Your Organization • INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT220 Preserving Investigative and Operational Viability in Insider Threat • INT240 Insider Threat Basic Hub Operations • IS150 NISP Reporting Requirements • Insider Threat Program (ITP) for Industry Job Aid • Insider Threat Reporting Procedures Job Aid • Insider Threat Indicators in UAM Job Aid • Insider Threat Tool Kit • Adverse Information Reporting Short • DITMAC Short • Security Incidents Reporting Requirements Short • Insider Threat for Senior Leaders Video • Virtual Insider Threat Symposium for Industry Webinar • DITMAC Update Webinar • Insider Threat for DoD Professionals Webinar • UAM in Insider Threat Programs Webinar
		811 referral process;	• INT220 Preserving Investigative and Operational Viability in Insider Threat • Insider Threat Reporting Procedures Job Aid • What's the 411 on the 811? Job Aid • Insider Threat Reporting Toolkit
		DITMAC Reporting Thresholds;	• INT220 Preserving Investigative and Operational Viability in Insider Threat • DITMAC Short • DITMAC Update Webinar

	PD-AoE2	**Counter Insider Threat Program**	**Relevant CDSE Courses/Training**
TCO 2	Scope	Goals and objectives;	• INT122 Establishing an Insider Threat Program for Your Organization • INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT240 Insider Threat Basic Hub Operations • Insider Threat Program (ITP) for Industry Job Aid • Sample Insider Threat Program Plan for Industry Job Aid
		Concepts and terminologies (e.g., minimum standards, Multi-disciplinary Insider Threat Working Groups, Potential Risk Indicators, Threshold events);	• INT122 Establishing an Insider Threat Program for Your Organization • INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT220 Preserving Investigative and Operational Viability in Insider Threat • INT240 Insider Threat Basic Hub Operations • INT260 Privacy and Civil Liberties for Insider Threat • Insider Threat Definitions Job Aid • Potential Risk Indicators: Kinetic Violence Job Aid • Potential Risk Indicators: Insider Threat Job Aid • Insider Threat for DoD Security Professionals Webinar

		Insider Threat Hub and Spokes;	• INT122 Establishing an Insider Threat Program for Your Organization • INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT220 Preserving Investigative and Operational Viability in Insider Threat • INT240 Insider Threat Basic Hub Operations
		Role of Hub Analyst vs. DoD Insider Threat Management and Analysis Center (DITMAC) Analyst;	• INT250 Critical Thinking for Insider Threat Analyst • DITMAC Short • DITMAC Update Webinar
		Insider Threat Case Management process;	• INT240 Insider Threat Basic Hub Operations
		DITMAC;	• INT220 Preserving Investigative and Operational Viability in Insider Threat • DITMAC Short • DITMAC Update Webinar
		Office of the Under Secretary of Defense (Intelligence) (OUSD-I) Implementation Plan;	

	PD-AoE3	Protecting Civil Liberties	Relevant CDSE Courses/Training
TCO 3	Scope	First Amendment Protections;	• INT260 Privacy and Civil Liberties for Insider Threat • Privacy and Civil Liberties Case Law Examples Job Aid • Why Threats of Violence are Not Protected Job Aid • Privacy and Civil Liberties in Insider Threat Webinar
		Fourth Amendment Rights;	• Privacy and Civil Liberties in Insider Threat Webinar
		DoDI 1325.06; DoD Military Whistleblower Act of 1988 (DoDD 7050.06);	• INT260 Privacy and Civil Liberties for Insider Threat • Whistleblower Protection Policies and FAQs Job Aid • Unauthorized Disclosure Toolkit
		Whistleblower Act of 1989;	• INT260 Privacy and Civil Liberties for Insider Threat • Whistleblower Protection Policies and FAQs Job Aid • Unauthorized Disclosure Toolkit • Privacy and Civil Liberties in Insider Threat Webinar
		Intelligence Community Whistleblower Act of 1998;	• INT260 Privacy and Civil Liberties for Insider Threat • Whistleblower Protection Policies and FAQs Job Aid • Unauthorized Disclosure Toolkit • Privacy and Civil Liberties in Insider Threat Webinar
		DoD Privacy Program (DoD 5400.11-R)	• DS-IF101 Identifying and Safeguarding PII • INT260 Privacy and Civil Liberties for Insider Threat • Information Security Toolkit • Privacy and Civil Liberties in Insider Threat Webinar
		DoD Freedom of Information Act Program (FOIA/DoDD 5400.07);	• INT260 Privacy and Civil Liberties for Insider Threat • Freedom of Information Act (FOIA) Exemptions Job Aid
		DoD Health Information Privacy Regulation (DoD 6025.18-R);	• INT260 Privacy and Civil Liberties for Insider Threat • DS-IF101 Identifying and Safeguarding PII • Information Security Toolkit
		Health Insurance Portability and Accountability Act (HIPAA); Executive Order 12333 (United States Intelligence Activities);	• DS-IF101 Identifying and Safeguarding PII • INT230 Insider Threat Records Check • INT260 Privacy and Civil Liberties for Insider Threat • Information Security Toolkit
		Notice and Consent Banners;	• INT220 Preserving Investigative and Operational Viability in Insider Threat • INT260 Privacy and Civil Liberties for Insider Threat • Insider Threat Indicators in UAM Job Aid • UAM in Insider Threat Programs Webinar

		ADA;	• INT260 Privacy and Civil Liberties for Insider Threat • The Principle of Confidentiality Job Aid
		Privacy Act 1974;	• INT260 Privacy and Civil Liberties for Insider Threat • Privacy Act Consent Rule Exceptions Job Aid • The Principle of Confidentiality Job Aid • Privacy and Civil Liberties in Insider Threat Webinar
		EEO;	• INT260 Privacy and Civil Liberties for Insider Threat • Workplace Environment and Organizational Justice Job Aid

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

	SBS-AoE1	**Psychology of Insider Threat**	**Relevant CDSE Courses/Training**
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);	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT240 Insider Threat Basic Hub Operations • INT290 Behavioral Science in Insider Threat • Insider Threat Toolkit • Behavioral Indicators of an Active Shoot Video • Behavioral Analysis in Insider Threat Webinar (Security Chat with Dr. Gallagher) • Applied Research on Mental Health Conditions and Security Webinar • Kinetic Violence Insider Threat Toolkit • PERSEREC Support to Insider Threat Programs Webinar
		Role of SBS in production of Insider Threat products (e.g., consultation, assessment of behavior, influence mitigation, training and research);	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT240 Insider Threat Basic Hub Operations • INT290 Behavioral Science in Insider Threat • Insider Threat Toolkit • Behavioral Indicators of an Active Shooter Video • Behavioral Analysis in Insider Threat Webinar (Security Chat with Dr. Gallagher) • Kinetic Violence Insider Threat Toolkit • Applied Research on Mental Health Conditions and Security Webinar • PERSEREC Support to Insider Threat Programs Webinar
		Holistic behavioral data;	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT240 Insider Threat Basic Hub Operations • INT290 Behavioral Science in Insider Threat • Insider Threat Toolkit • Behavioral Indicators of an Active Shooter Video • Behavioral Analysis in Insider Threat Webinar (Security Chat with Dr. Gallagher) • Kinetic Violence Insider Threat Toolkit • Applied Research on Mental Health Conditions and Security Webinar • PERSEREC Support to Insider Threat Programs Webinar

		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);	• INT101 Insider Threat Awareness Course • INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT230 Insider Threat Records Checks • Insider Threat Case Studies (21 total) • Customizable DoD Command Brief for Insider Threat Awareness Job Aid (pptx) • Foreign Intelligence Entity (FIE) Targeting Recruitment Methodology Job Aid • DITMAC Short • Mishandling Classified Information, Micro Learning Video Lesson • Mozaffar Khazaee, Micro Learning Video Lesson • Insider Threats to Cybersecurity Video • Adverse Information Reporting Webinar • Cyber Insider Threat Webinar • DITMAC Update Webinar
		Psychological factors of the insider threat;	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT240 Insider Threat Basic Hub Operations • INT290 Behavioral Science in Insider Threat • Behavioral Indicators of an Active Shooter Video • Behavioral Analysis in Insider Threat Webinar (Security Chat with Dr. Gallagher) • Kinetic Violence Insider Threat Toolkit • Applied Research on Mental Health Conditions and Security Webinar • PERSEREC Support to Insider Threat Programs Webinar
		Real-time case reviews;	• INT240 Insider Threat Basic Hub Operations
		Case Studies;	• CDSE Insider Threat Case Studies • CDSE Counterintelligence Case Studies

Researching (R)
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**	**Relevant CDSE Courses/Training**
TCO 5	Scope	Privacy and civil liberties;	• INT122 Establishing an Insider Threat Program for Your Organization • INT201 Developing a Multidisciplinary Insider Threat Capability • INT230 Insider Threat Records Checks • INT240 Insider Threat Basic Hub Operations • INT260 Privacy and Civil Liberties for Insider Threat • Insider Threat for Senior Leaders Video
		Protection of Personally identifiable information (PII);	• DS-IF101 Identifying and Safeguarding PII • INT260 Privacy and Civil Liberties for Insider Threat • Information Security Toolkit
		Information collection limitations;	• INT220 Preserving Investigative and Operational Viability in Insider Threat • INT230 Insider Threat Records Checks
		Insider Threat Security Classification Guide;	• INT220 Preserving Investigative and Operational Viability in Insider Threat • INT260 Privacy and Civil Liberties for Insider Threat

		Records Management;	• INT230 Insider Threat Records Checks • INT240 Insider Threat Basic Hub Operations
		Classification, Derivative classification and aggregation;	• IF101 Security Classification Guidance • IF102 Original Classification • IF103 Derivative Classification • IF105 Marking Classified Information • IF110 Classification Conflicts and Evaluations • Derivative Classification Training Job Aid • Downgrading and Declassification Short • Marking in the Electronic Environment Short
		USD(I) Classification Guide;	
		NITTF classification guide;	
		DoD 5200.01;	• IF130 Unauthorized Disclosure of Classified Information for DoD and Industry • Unauthorized Disclosure Toolkit • DoD Unauthorized Disclosure Program Manager Webinar
		Freedom of Information Act (FOIA);	• INT260 Privacy and Civil Liberties for Insider Threat • Freedom of Information Act (FOIA) Exemptions Job Aid

	R-AoE2	**Investigative and Operational Viability**	**Relevant CDSE Courses/Training**
TCO 6	Scope	Preserving chain of custody and integrity of collected information;	• INT220 Preserving Investigative and Operational Viability in Insider Threat • INT230 Insider Threat Records Checks • INT240 Insider Threat Basic Hub Operations
		The investigative lifecycle	• INT220 Preserving Investigative and Operational Viability in Insider Threat

	R-AoE3	**Counterintelligence (CI) Pillar**	**Relevant CDSE Courses/Training**
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);	• CI112 Counterintelligence Awareness and Security Brief • CI116 Counterintelligence Awareness and Reporting for DoD • CI Case Studies • Foreign Collection Methods: Indicators and Countermeasures Job Aid • Foreign Intelligence Entity (FIE) Targeting Recruitment Methodology Job Aid • CI Concerns for National Security Adjudicators Short • CI Foreign Travel Briefing Short • CI Awareness Toolkit
		Capabilities, authorities, and jurisdictions of CI organizations and/or elements;	• CI Toolkit, Policy Tab
		Role of CI data in C-InT assessments and mitigation;	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT220 Preserving Investigative and Operational Viability in Insider Threat • INT240 Insider Threat Basic Hub Operations
		DoD 5240.1-R;	• CI Intelligence Oversight Toolkit
		DoDD 5240.06;	• CI116 Counterintelligence Awareness and Reporting for DoD • CI117 Protecting Assets in the NISP

			• CI Case Studies • CI Toolkit • CI Trivia Twirl
		Title 50, U.S. Code Section 402A;	
		Foreign Intelligence Entity (FIE) collection priorities;	• CI Toolkit • Industrial Base Technology List (ITBL) Job Aid • DSS 2017 Targeting US Technologies Webinar
		CI National Intelligence Priorities Framework (NIPF) topics;	• CI Toolkit • DSS 2017 Targeting U.S. Technologies Webinar
		FIE tactics, techniques, and procedures;	• CI112 Counterintelligence Awareness and Security Brief • CI116 Counterintelligence Awareness and Reporting for DoD • CI117 Protecting Assets in the NISP • CI Case Studies • Foreign Intelligence Entity (FIE) Targeting Recruitment Methodology Job Aid • Understanding Espionage and National Security Crimes Job Aid • Critical Program Information (CPI) Short • CI Toolkit • Critical Technology Protection: Foreign Visits and Academic Solicitation Webinar • The Classified Foreign Visit Process Webinar
		Understand anomalous behaviors within the CI pillar;	• CI112 Counterintelligence Awareness and Security Brief • CI116 Counterintelligence Awareness and Reporting for DoD • CI117 Protecting Assets in the NISP • CI Case Studies • Foreign Intelligence Entity (FIE) Targeting Recruitment Methodology Job Aid • Understanding Espionage and National Security Crimes Job Aid • Critical Program Information (CPI) Short • CI Toolkit • Critical Technology Protection: Foreign Visits and Academic Solicitation Webinar • The Classified Foreign Visit Process Webinar

	R-AoE4	Cyber Pillar	Relevant CDSE Courses/Training
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);	• CS130 Cybersecurity Awareness • CS200 Continuous Monitoring • INT122 Establishing an Insider Threat Program for Your Organization • INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT240 Insider Threat Basic Hub Operations • INT280 Cyber Insider Threat • Potential Risk Indicators: Insider Threat • Insider Threat Indicators in UAM Job Aid • Insider Threat Toolkit • Insider Threats to Cybersecurity Video Lesson • Cyber Insider Threat Webinar • UAM in Insider Threat Programs Webinar

		Role of Cyber data in C-InT assessments and mitigation;	• CS160 Cybersecurity for Security Personnel • INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT240 Insider Threat Basic Hub Operations • INT280 Cyber Insider Threat • Insider Threat Indicators in UAM Job Aid • Insider Threat Toolkit • Insider Threats to Cybersecurity Video Lesson • Cyber Insider Threat Webinar • UAM in Insider Threat Programs Webinar
		DoDI 8500.01;	• CS160 Cybersecurity for Security Personnel
		Committee on National Security Systems Directive (CNSSD) 504;	
		Long term analysis of UAM data;	• CS200 Continuous Monitoring • INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT240 Insider Threat Basic Hub Operations • Insider Threat Indicators in UAM Job Aid • UAM in Insider Threat Programs Webinar
		Understand anomalous behaviors within the Cyber pillar;	• Potential Risk Indicators: Insider Threat • Insider Threat Indicators in UAM Job Aid • Insider Threats to Cybersecurity Video Lesson • Cyber Insider Threat Webinar • UAM in Insider Threat Programs Webinar
		Identifying privileged users;	• CS160 Cybersecurity for Security Personnel • DS-IA112 Privileged User Cybersecurity Responsibilities • Cyber Insider Threat Webinar

	R-AoE5	Human Resources (HR) Pillar	Relevant CDSE Courses/Training
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);	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT230 Insider Threat Records Checks • INT240 Insider Threat Basic Hub Operations
		Role of HR in C-InT assessments and mitigation (e.g., performance counseling, remedial training, compliance mandate, performance improvement plan, employee assistance referral, suspension of employment, termination of employment);	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT230 Insider Threat Records Checks • INT240 Insider Threat Basic Hub Operations • INT270 Maximizing Organizational Trust • Human Resources Webinar • Maximizing Organizational Trust Webinar
		Identifying minimum access potential insider threat needs to perform their job;	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT230 Insider Threat Records Checks • INT240 Insider Threat Basic Hub Operations
		Identify the field of work assigned to potential insider threat;	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT230 Insider Threat Records Checks • INT240 Insider Threat Basic Hub Operations

		Understand anomalous behaviors within the HR pillar; FMLA;	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT230 Insider Threat Records Checks • INT240 Insider Threat Basic Hub Operations

	R-AoE6	Law Enforcement (LE) Pillar	Relevant CDSE Courses/Training
TCO 10	Scope	Terms of Reference, concepts, and principles (e.g., arrest records, LE interactions, court records, public records);	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT220 Preserving Investigative and Operational Viability in Insider Threat • INT230 Insider Threat Records Checks • INT240 Insider Threat Basic Hub Operations
		Role of LE in C-InT assessments and mitigation;	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT220 Preserving Investigative and Operational Viability in Insider Threat • INT230 Insider Threat Records Checks • INT240 Insider Threat Basic Hub Operations
		Understand anomalous behaviors within the LE pillar;	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT220 Preserving Investigative and Operational Viability in Insider Threat • INT230 Insider Threat Records Checks • INT240 Insider Threat Basic Hub Operations

	R-AoE7	Legal Pillar	Relevant CDSE Courses/Training
TCO 11	Scope	Terms of Reference, concepts, and principles (e.g., data integrity and support to inquiries);	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT220 Preserving Investigative and Operational Viability in Insider Threat • INT240 Insider Threat Basic Hub Operations
		Role of Legal in C-InT assessments and mitigation;	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT220 Preserving Investigative and Operational Viability in Insider Threat • INT240 Insider Threat Basic Hub Operations
		Understand anomalous behaviors within the Legal pillar;	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT220 Preserving Investigative and Operational Viability in Insider Threat • INT240 Insider Threat Basic Hub Operations

	R-AoE8	Behavioral Science Pillar	Relevant CDSE Courses/Training
TCO 12	Scope	Terms of Reference, concepts, and principles;	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT240 Insider Threat Basic Hub Operations • INT290 Behavioral Science in Insider Threat • Insider Threat Toolkit • Behavioral Indicators of an Active Shooter Video

			• Behavioral Analysis in Insider Threat Webinar (Security Chat with Dr. Gallagher) • Kinetic Violence Insider Threat Toolkit • Applied Research on Mental Health Conditions and Security Webinar • PERSEREC Support to Insider Threat Programs Webinar
		Role of Behavioral Science in C-InT assessments and mitigation;	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT240 Insider Threat Basic Hub Operations • Insider Threat Toolkit • Behavioral Indicators of an Active Shooter Video • Behavioral Analysis in Insider Threat Webinar (Security Chat with Dr. Gallagher) • Kinetic Violence Insider Threat Toolkit • Applied Research on Mental Health Conditions and Security Webinar • PERSEREC Support to Insider Threat Programs Webinar
		Knowing when and how to interact with a behavioral science professional;	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT240 Insider Threat Basic Hub Operations • INT290 Behavioral Science in Insider Threat • Insider Threat Toolkit • Behavioral Indicators of an Active Shooter Video • Behavioral Analysis in Insider Threat Webinar (Security Chat with Dr. Gallagher) • Kinetic Violence Insider Threat Toolkit • Applied Research on Mental Health Conditions and Security Webinar • PERSEREC Support to Insider Threat Programs Webinar
		Mental Health data found in workforce vetting forms (e.g., SF-85 & SF-86);	• Personnel Security Toolkit • Adjudicative Guideline I: Psychological Conditions Short
		General of what is included in behavioral considerations vs. health considerations;	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT240 Insider Threat Basic Hub Operations • INT290 Behavioral Science in Insider Threat • Insider Threat Toolkit • Behavioral Indicators of an Active Shooter Video • Behavioral Analysis in Insider Threat Webinar (Security Chat with Dr. Gallagher) • Kinetic Violence Insider Threat Toolkit • Applied Research on Mental Health Conditions and Security Webinar • PERSEREC Support to Insider Threat Programs Webinar
		Understand anomalous behaviors within the Behavioral Science pillar;	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT240 Insider Threat Basic Hub Operations • INT290 Behavioral Science in Insider Threat • Insider Threat Toolkit • Behavioral Indicators of an Active Shooter Video • Behavioral Analysis in Insider Threat Webinar (Security Chat with Dr. Gallagher)

			• Kinetic Violence Insider Threat Toolkit • Applied Research on Mental Health Conditions and Security Webinar • PERSEREC Support to Insider Threat Programs Webinar

	R-AoE9	Security Pillar	Relevant CDSE Courses/Training
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);	• IF130 Unauthorized Disclosure of Classified Information for DoD and Industry • INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT240 Insider Threat Basic Hub Operations • GS101 DoD Security Specialist Course • Information Security Toolkit • Personnel Security Toolkit • Physical Security Toolkit • Security Assistant Toolkit • Security Education and Training Awareness (SETA) Toolkit
		Role of Security in C-InT assessments and mitigation;	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT240 Insider Threat Basic Hub Operations
		Title 32 Code of Federal Regulations Title 147;	• Adjudicative Guidelines A-M Shorts • Revised Federal Investigative Standards Short • Personnel Security Toolkit
		Adjudicative Guidelines vs. DITMAC Reporting Thresholds;	• Adjudicative Guidelines A-M Shorts • DITMAC Short • Revised Federal Investigative Standards Short • DITMAC Update Webinar
		Security-Based Mitigation (e.g., Access suspension, downgrades, etc.);	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses
		Continuous Evaluation Process;	• CS200 Continuous Monitoring • Personnel Security Toolkit: Continuous Evaluation Tab

		Security Clearance Adjudicative Process;	• 13 Adjudicative Guidelines Shorts:
			  • A: Allegiance to the United States Short
			  • B: Foreign Influence Short
			  • C: Foreign Preference Short
			  • D: Sexual Behavior Short
			  • E: Personal Conduct Short
			  • F: Financial Considerations Short
			  • G: Alcohol Consumption Short
			  • H: Drug Involvement and Substance Misuse Short
			  • I: Psychological Conditions Short
			  • J: Criminal Conduct Short
			  • K: Handling Protected Information Short
			  • L: Outside Activities Short
			  • M: Use of Information Technology Short

		Use of Publicly Available Information (PAI);	• Personnel Security Toolkit • Incorporating Social Media into Background Investigations Video Lesson • Applied Research on Social Media and Security Webinar

		Security policies;	• GS101 DoD Security Specialist Course • Information Security Toolkit • Personnel Security Toolkit • Physical Security Toolkit • Security Assistant Toolkit • Security Education and Training Awareness (SETA) Toolkit
		Background investigation and workforce vetting/suitability questionnaires;	• PS001 Introduction to DoD Personnel Security Adjudication • PS010 Introduction to Suitability Adjudications for the DoD • PS112 Introduction to DoD HSPD-12 CAC Credentialing • PS113 Introduction to Personnel Security • PS170 Introduction to National Security Adjudications • PS181 JCAVS User Level 7 & 8 • PS182 JCAVS User Level 10 • PS183 JCAVS User Levels 2-6
		Appeals documentation, Incident reports;	• PS001 Introduction to DoD Personnel Security Adjudication • PS010 Introduction to Suitability Adjudications for the DoD • PS112 Introduction to DoD HSPD-12 CAC Credentialing • PS113 Introduction to Personnel Security • PS170 Introduction to National Security Adjudications
		Knowledge of who a C-InT analyst should leverage when an individual in question exhibits clearance related PRIs or other anomalous behavior (Security vs. Special Security Office (SSO), respectively);	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT240 Insider Threat Basic Hub Operations • Insider Threat and the DoD CAF Webinar
		DoD 4105.21; Understand anomalous behaviors within the Security pillar;	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT240 Insider Threat Basic Hub Operations • Insider Threat Case Studies • Unauthorized Disclosure Case Studies • National Security Adjudicative Guidelines Job Aid • Potential Risk Indicators: Insider Threat • Potential Risk Indicators: Kinetic Violence Job Aid • DITMAC Short • DITMAC Update Webinar

Synthesis (S)
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	Relevant CDSE Courses/Training
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;	• INT122 Establishing an Insider Threat Program for Your Organization • INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT230 Insider Threat Records Checks • INT240 Insider Threat Basic Hub Operations • INT250 Critical Thinking for Insider Threat Analysts
		Research strategy for an insider threat inquiry;	• INT230 Insider Threat Records Checks • INT240 Insider Threat Basic Hub Operations • INT250 Critical Thinking for Insider Threat Analysts
		Thresholds for reporting and action;	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT220 Preserving Investigative and Operational Viability in Insider Threat • INT240 Insider Threat Basic Hub Operations • Insider Threat Program (ITP) for Industry Job Aid • DITMAC Short • Virtual Insider Threat Symposium for Industry Webinar • DITMAC Update Webinar

	S-AoE2	All-Source Insider Threat Referral Triage	Relevant CDSE Courses/Training
TCO 15	Scope	Compiles, reviews, interprets, correlates, and analyzes insider threat related data to identify behavior potentially indicative of a threat;	• INT122 Establishing an Insider Threat Program for Your Organization • INT240 Insider Threat Basic Hub Operations • INT250 Critical Thinking for Insider Threat Analysts
		Develops and recommends referral and analytic strategies;	• INT210 Insider Threat Mitigation Responses • INT240 Insider Threat Basic Hub Operations • INT250 Critical Thinking for Insider Threat Analysts

	S-AoE3	All-Source Insider Threat Trend Analysis	Relevant CDSE Courses/Training
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;	• INT210 Insider Threat Mitigation Responses • INT240 Insider Threat Basic Hub Operations • INT250 Critical Thinking for Insider Threat Analysts

Tools and Methods (TM)
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	Relevant CDSE Courses/Training
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);	• INT250 Critical Thinking for Insider Threat Analysts
		Best practices and challenges of working with multidisciplinary teams; How to prevent group polarization, group think, and/or artificial consensus;	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT220 Preserving Investigative and Operational Viability in Insider Threat • INT250 Critical Thinking for Insider Threat Analysts

	TM-AoE2	Critical Thinking Techniques	Relevant CDSE Courses/Training
TCO 18	Scope	Critical thinking as a process;	• INT250 Critical Thinking for Insider Threat Analysts
		critical thinking techniques (e.g., Hypotheses/scenario generation; alternative analysis techniques; argument mapping);	• INT250 Critical Thinking for Insider Threat Analysts • Checklist for Reasoning for Insider Threat Analysts Resource • Critical Thinking Techniques for Insider Threat Analysts Job Aid • Critical Thinking Tools for Insider Threat Analysts Job Aid
		Biases (e.g. confirmation, hindsight, foresight, availability, overconfidence);	• INT250 Critical Thinking for Insider Threat Analysts

	TM-AoE3	Databases and Data Feeds	Relevant CDSE Courses/Training
TCO 19	Scope	Function, capabilities, and accesses of local/national databases and data feeds;	• INT230 Insider Threat Records Checks
		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);	• INT230 Insider Threat Records Checks
		Commercial databases (e.g., addresses, public records, court information including civil and criminal judgments, financial judgments and liens);	• INT230 Insider Threat Records Checks
		Understand the difference between primary and secondary sources;	• INT230 Insider Threat Records Checks

		Importance and "How to" for MOA (Memorandum of Agreement) and Special Leave Accrual (SLA) to ensure timely and dependable access;	• INT230 Insider Threat Records Checks (reference is to One Time Advisements to custodians and associated MOA for frequent access of records)

	TM-AoE4	DITMAC System-of-Systems (DSOS)	Relevant CDSE Courses/Training
TCO 20	Scope	Function, capabilities, accesses, and strengths/weaknesses of DSOS;	• Insider Threat Toolkit • DITMAC Short • DITMAC Update Webinar
		Request for Information;	• Insider Threat Toolkit • DITMAC Short • DITMAC Update Webinar
		Analytic findings, Work flow process;	• Insider Threat Toolkit • DITMAC Short • DITMAC Update Webinar
		DSOS Limited Distribution Node (LIMDIS);	• Insider Threat Toolkit • DITMAC Short • DITMAC Update Webinar

	TM-AoE6	Structured Analytic Techniques	Relevant CDSE Courses/Training
TCO 21	Scope	Occam's Razor;	• INT250 Critical Thinking for Insider Threat analysts • Checklist for Reasoning for Insider Threat Analysts Resource • Critical Thinking Techniques for Insider Threat Analysts Job Aid • Critical Thinking Tools for Insider Threat Analysts Job Aid
		Diagnostic techniques (e.g., Key Assumptions, Quality of Information, Indicators or Signposts of Change, Analysis of Competing Hypothesis);	• INT250 Critical Thinking for Insider Threat Analysts • Checklist for Reasoning for Insider Threat Analysts Resource • Critical Thinking Techniques for Insider Threat Analysts Job Aid • Critical Thinking Tools for Insider Threat Analysts Job Aid
		Imaginative Thinking (e.g., Brainstorming, Outside-In Thinking, Red Team Analysis);	• INT250 Critical Thinking for Insider Threat Analysts • Checklist for Reasoning for Insider Threat Analysts Resource • Critical Thinking Techniques for Insider Threat Analysts Job Aid • Critical Thinking Tools for Insider Threat Analysts Job Aid
		Contrarian Techniques (e.g., Devil's Advocacy, Team A/Team B, High Impact/Low Probability Analysis);	• INT250 Critical Thinking for Insider Threat Analysts • Checklist for Reasoning for Insider Threat Analysts Resource • Critical Thinking Techniques for Insider Threat Analysts Job Aid • Critical Thinking Tools for Insider Threat Analysts Job Aid
		Ability to document analytic processes in a clear and understandable method;	• INT250 Critical Thinking for Insider Threat Analysts

Vulnerabilities Assessment and Management (VAM)
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	Relevant CDSE Courses/Training
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);	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT240 Insider Threat Basic Hub Operations
		Recognize stressors and concerning behaviors on the critical pathway, discipline response options; response planning;	• INT101 Insider Threat Awareness Course • INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT290 Behavioral Science in Insider Threat • Potential Risk Indicators: Insider Threat • Potential Risk Indicators: Kinetic Violence Job Aid • DITMAC Short • Behavioral Indicators of an Active Shooter Video • Behavioral Analysis in Insider Threat Webinar (Security Chat with Dr. Gallagher) • DITMAC Update Webinar
		Risk assessing; mitigation impacts (positive & negative); response monitoring; reporting requirements;	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT240 Insider Threat Basic Hub Operations • INT270 Maximizing Organizational Trust • Maximizing Organizational Trust Webinar

	VAM-AoE2	Insider Threat Mitigation: Organizational	Relevant CDSE Courses/Training
TCO 23	Scope	Organizational mitigation response options (e.g., changes in policy or Standard Operating Procedures (SOPs), processes and procedures, education/training/awareness);	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT270 Maximizing Organizational Trust • Maximizing Organizational Trust Webinar • Positive Outcomes Webinar
		Mitigation impacts to the organization (positive & negative);	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT270 Maximizing Organizational Trust • Maximizing Organizational Trust Webinar • Positive Outcomes Webinar

C-InT Certification Minimally Acceptable Candidate (MAC) Descriptions

	MAC Description	Relevant CDSE Courses/Training
Tier 1	Describe the structure, mission, capability, and resource requirements of a C-InT Hub as well as the policies that govern them. Describe the capabilities and reporting streams of each of the pillars, all local and DITMAC Reporting thresholds, and the proper procedures for information sharing. Be able to monitor and track data feeds (e.g., UAM) as well as review referrals/reports of anomalous behavior(s) and validate whether they meet local and/or DITMAC reporting thresholds. Access, search, query, and/or monitor relevant data feeds for additional relevant information or to review Insider threat events which already occurred but were not previous identified or tracked. Validate and analyze data from multiple sources (e.g., security, CI, UAM, etc.) in order to ensure quality and applicability to the inquiry, compile the relevant data, and document any information gaps. Use the RFI process to gain additional relevant information from the DITMAC or other external functional SMEs about anomalous behavior(s)/events or to address information gaps within an open inquiry.	• INT201 Developing a Multidisciplinary Insider Threat Capability • INT210 Insider Threat Mitigation Responses • INT220 Preserving Investigative and Operational Viability in Insider Threat • INT230 Insider Threat Records Checks • INT240 Insider Threat Basic Hub Operations • INT260 Privacy and Civil Liberties for Insider Threat • Insider Threat Program (ITP) for Industry Job Aid • Insider Threat Indicators in UAM Job Aid • DITMAC Short • UAM in Insider Threat Programs Webinar

	MAC Description	Relevant CDSE Courses/Training
Tier 2	Perform all of the tasks described in Level 1, as well as evaluate, integrate, analyze, and interpret all collected data against local and/or DITMAC reporting threshold(s). Provide mentorship/training to basic C-InT analysts and ensure tradecraft standards are met by Quality Assurance/Quality Control of analytic products. Generate report(s) of assessment results and review them with legal, the appropriate senior leaders, and stakeholders as required. Support the C-InT Hub in facilitating and monitoring an appropriate mitigation strategy with all relevant stakeholders as required. Participate in local and external reviews/lessons learned (e.g., audits, after action reports (AARs), insider threat working groups (InT-WGs), and analysis and mitigation community of practice (AMCOP), etc.) in order to assess triggers, redress policies, and follow up. Support the development of agency policies and/or procedures.	• Above plus • INT250 Critical Thinking for Insider Threat Analysts • Critical Thinking Tools for Insider Threat Analyst Job Aid • Critical Thinking Techniques for Insider Threat Analyst Job Aid

DISCLAIMER: **The CDSE Insider Threat Deskside Reference is designed to support Insider Threat Program Managers, Insider Threat Program Analyst and Operations Personnel, and Insider Threat Senior Leaders in DoD, Federal government, and cleared industry. The courseware is available at https://www.cdse.edu/catalog/insider-threat.html. The courseware was designed to meet requirements under EO 13587, the National Minimum Standards, DoDD 5205.16, and the NISPOM. Learning objectives were developed in coordination with OUSD(I) and the NITTF, and have been mapped to the Essential Body of Knowledge tested in the Counter Insider Threat Certification Exams. Matriculation through these courses does NOT guarantee the student will pass the exam(s). These materials have been recognized as potential preparatory resources and as acceptable sources of professional development units for those maintaining certification.**