Center for Development of Security Excellence

CI020.16 - Counterintelligence Concerns for National Security Adjudicators

This course provides an opportunity for students to practice recognition of counterintelligence (CI) concerns relevant to the performance of their job tasks and raises awareness of these issues and their importance in the context of the adjudication process.

CI102.16 - Supply Chain Threat Awareness

This course provides a detailed explanation of the importance of Supply Chain Threat Awareness, which encompasses and defines Supply Chain and Supply Chain Risk Management (SCRM). The reader will learn what potential threats are posed by Foreign Intelligence Entities (FIE), criminals, and strategic competitors, as well as various risk mitigation strategies/countermeasures.

CI112.16 - Counterintelligence Awareness and Security Brief

This course was developed primarily for employees at cleared defense contractor facilities. This eLearning training enables these employees to complete the training at any time, to fulfill their initial or annual security, counterintelligence, and Insider Threat awareness training requirement. This training emphasizes awareness of potential threats directed against U.S. technology. It also explains common suspicious activities, including Insider Threats that should be reported to the Facility Security Officer (FSO) in compliance with National Industrial Security Program Operating Manual (NISPOM). FSOs may use this training in conjunction with their company specific security protocols for duties applicable to the employee’s job, to meet the Counterintelligence and Threat Awareness training outlined in NISPOM 32 Code of Federal Regulation (CFR) Part 117.12.

CI116.16 - Counterintelligence Awareness and Reporting for DoD

This course explains the role everyone has in CI. CI Awareness and Reporting summarizes the potential threats and collection methods used by FIE, Potential Espionage Indicators (PIE), warning signs of terrorism, and reporting responsibilities. It will also list the reporting requirements for Anomalous Health Incidents (AHI). An AHI is when one or more individuals may experience an unexplained sensory event coupled with physical symptoms.

CI117.16 - Protecting Assets in the NISP

This course provides a detailed explanation of the importance of CI awareness to the NISP. Topics include the relationship between CI and security, CI and threat awareness policy for industry personnel, elements of an effective CI program, common types of threats and methods of operation, sources of threat information, threats related to U.S. Government sensitive/classified technologies, and CI/threat awareness reporting requirements and procedures.

CS200.16 - Continuous Monitoring

This course provides students with in-depth knowledge and understanding of the Risk Management Framework (RMF) Step 6. It also defines the role it plays in information system security and the overall risk management of an organization. It explores continuous monitoring processes and tasks required and addresses the roles and responsibilities for implementing continuous monitoring of information systems. This ongoing evaluation of the effectiveness of applied security controls will position organizations to better identify and mitigate vulnerabilities and threats to their information systems and information technology infrastructure.

ED504.10 (CDSE) - Understanding Adversaries and Threats to the United States and the DOD

This course specifically addresses the intentions and capabilities of the three to five most significant adversaries to the United States and DOD. It also examines the multifaceted concept of threat: Who presents a threat? What are internal and external threats? What is being threatened? Who can provide a threat assessment? The course addresses counterintelligence, counterterrorism, insider threats, and threats to critical information systems. In addition, this course covers such critical threats as embezzlement, physical sabotage, violence in the workplace by disgruntled employees, and others that must be addressed by the senior security manager. The course familiarizes students with Government and non-Government sources of reliable threat information.

ED520.10 (CDSE) - Foundations of Insider Threat Management

This course is designed to introduce students to the risks posed by trusted insiders, including the psychological motivations, predispositions, and behaviors associated with this group. Students will explore the historical context of insider threat and the counter insider threat mission, to include relevant law, policy, and regulation. Students will be challenged to apply critical thinking skills to address current issues surrounding this problem set, including privacy and civil liberties concerns, cyber insider threat, and active shooter/workplace violence. Students will contextualize these issues within their major area of study to identify the role of their discipline in preventing and countering the insider threat.

GS105.16 - Active Shooter Awareness

This short video helps to determine the most reasonable response to protect yourself and the lives of others around you, given a scenario about an active shooter incident.

IF130.16 - Unauthorized Disclosure (UD) of Classified Information and Controlled Unclassified Information (CUI)

This course provides an overview of what unauthorized disclosure is, including specific types of unauthorized disclosure and some common misconceptions about unauthorized disclosure. This course will also discuss the types of damage caused by unauthorized disclosure and the various sanctions one could face if caught engaging in unauthorized disclosure.

INT101.16 - Insider Threat Awareness

This course provides a thorough understanding of how Insider Threat Awareness is an essential component of a comprehensive security program. With a theme of "if you see something, say something," the course promotes the reporting of suspicious activities observed within the place of duty. Using a few case study scenarios, the course highlights the actions and behaviors that can signify an Insider Threat. The instruction promotes a proactive approach to reporting the suspicious activities.

INT122.16 - Establishing an Insider Threat Program for Your Organization

This course is designed for individuals designated as the organizational Insider Threat Program Manager. The instruction provides guidance for organizational Insider Threat Program Managers on how to organize and design their specific program. It covers the minimum standards outlined in the Executive Order 13587 that all programs must consider in their policy and plans. The course recommends which internal organizational disciplines should be included as integral members in the organization's Insider Threat team or "hub" to ensure all potential vulnerabilities are considered. The course instructs the Insider Threat Program Manager to ensure that everyone on the team receives fundamental training in the topics required by the National Policy.

INT200.10 - Insider Threat Detection Analysis Course (ITDAC)

This course was designed to meet the Minimum Standards for Executive Branch Insider Threat Programs identified by the National Insider Threat Task Force. This course provides entry level Counter-Insider Threat Analysts the ability to apply critical thinking skills and applicable structured analytic techniques to potential Insider Threat indicators. This course also allows learners to obtain and use holistic data in conjunction with the application of critical pathway theory.

INT201.16 - Developing a Multidisciplinary Insider Threat Capability

This course equips Insider Threat Program Management personnel with the knowledge, skills, and abilities required to assemble a multidisciplinary Insider Threat team of subject matter experts capable of monitoring, analyzing, reporting, and responding to Insider Threat incidents. The course includes an overview of security, law enforcement, human resource, behavioral science, counterintelligence, and cybersecurity disciplines and addresses requirements for establishing a collaborative environment and the benefits each group brings to an effective program. This training complies with DoD Directive 5205.16, The DoD Insider Threat Program, Enclosure 2 (Responsibilities).

INT210.16 - Insider Threat Mitigation Responses

This course was developed to equip Insider Threat Program Management and Operational personnel with the knowledge, skills, and abilities required to identify viable response options ranging from administrative actions, security violations or infractions, and referrals to Human Resources (HR), the Employee Assistance Program (EAP), law enforcement, and/or the appropriate supporting counterintelligence organization. Training is required to analyze and mitigate information to determine appropriate reporting as directed by Department of Defense Directive (DoDD) 5240.06, The DoD Insider Threat Program; SEAD-4, National Security Adjudicative

Guidelines; and other indicators that meet DITMAC thresholds or as determined by OUSD(I) and/or policy guidance.

INT220.16 - Preserving Investigative and Operational Viability in Insider Threat

This course equips Insider Threat Program Management and/or Operations personnel with the knowledge, skills, and abilities required to appropriately manage incident response and other Insider Threat Program actions within the scope of their authority; to properly handle evidence and apply chain of custody; to properly identify and report exculpatory information; to appropriately report and refer Insider Threat information; and to understand the consequences of poorly executed Insider Threat response.

INT230.16 - Insider Threat Records Checks

This course was developed to equip Insider Threat Program operational personnel with the knowledge, skills, and abilities required to conduct their duties under the data collection requirement of DoD Directive 5205.16, Insider Threat Program. Insider Threat operational personnel must identify Insider Threat Indicators in records, databases, and other electronic forms of information. Training is required to identify required reporting from DoD Directive 5240.06, Counterintelligence Awareness and Reporting (CIAR); DoD 5220.22-M, National Industrial Security Program Operating Manual; Security Executive Agent Directive 4 (SEAD-4); National Security Adjudicative Guidelines; and other indicators that meet DITMAC thresholds, or as determined by OUSD(I) and/or policy guidance.

INT240.16 - Insider Threat Basic HUB Operations

The Insider Threat Basic Hub Operations course provides Insider Threat Program Managers and operations personnel with an overview of Insider Threat Hub operations and breaks down proactive approaches to deter, detect, mitigate, and report the threats associated with trusted insiders. The course will explain the roles and purpose of an Insider Threat Hub and describe in detail the Insider Threat Hub management processes.

INT250.16 - Critical Thinking for Insider Threat Analysts

This course provides a high-level explanation of analytical and critical thinking as it relates to producing comprehensive analytic products for Insider Threat programs. Users will learn how critical thinking tools visually structure, facilitate, and empower thinking to help explain uncertainties, conclusions, and judgments. This course will give users the skills to help support your Insider Threat program in the deterrence, detection, and mitigation of insider risks while protecting the privacy and civil liberties of the workforce.

INT260.16 - Insider Threat Privacy and Civil Liberties

The Insider Threat Privacy and Civil Liberties course provides a high-level explanation of the importance that civil liberties, privacy laws, regulations, and policies have on conducting Insider Threat program actions. This course will identify what information is protected by law and how to employ safeguarding information. The user will be introduced to Insider Threat challenges that are impacted by socially charged matters regarding civil liberty laws and policies, unauthorized disclosure, whistleblowing, protected speech, and threats of violence.

INT270.16 - Maximizing Organizational Trust

Employees are an organization's first line of defense against threats to the mission or to the safety of the workforce. To motivate employees to actively participate in security and safety initiatives, organizational leaders must create an environment in which personnel trust leadership to be fair, honest, and transparent. In response to a tasking from the Office of the Under Secretary of Defense for Intelligence (OUSD[I]), the Defense Personnel and Security Research Center (PERSEREC) reviewed business, psychology, and communication literature to identify best practices for building and maintaining organizational trust. This guide is the result of that effort.

INT280.16 - Cyber Insider Threat

This course is designed to familiarize Department of Defense (DOD), Component, Industry, and Federal Agency Insider Threat Program Practitioners with cyber-Insider Threat and associated indicators. The instruction relates these concepts to efforts to counter the Insider Threat, to mitigate risks associated with trusted insiders, and to identify the role of cybersecurity within a multi-disciplinary threat management capability. These learning objectives support the conduct and integration of monitoring, analysis, reporting, and response to Insider Threats as required in the DoDD 5205.16, NISPOM Change 2, EO13587, and the President's Minimum Standards for Executive Branch Insider Threat Programs.

INT290.16 - Behavioral Science in Insider Threat

This course provides DOD component, industry, and federal agency Insider Threat Program personnel with an introduction to Behavioral Science. Relating Behavioral Science concepts to efforts to counter the Insider Threat; and identifies the role of Behavioral Science within a multi-disciplinary threat management capability to conduct and integrate the monitoring, analysis, reporting, and response to Insider Threats. This course is required by DoDD 5205.16, NISPOM Change 2, EO 13587 and the Minimum Standards for Executive Branch Insider Threat Programs.

PS113.16 - Introduction to Personnel Security

This course introduces the management practices and procedures required to administer the Department of Defense (DOD) Personnel Security Program (PSP) at the military base/installation level. The course provides an overview of the elements of the PSP to include designation of sensitive duties, investigative and adjudicative practices, security officer responsibilities under the PSP one-time access requirements, special security program requirements, and due process procedures. The course identifies the types of personnel security investigations (PSIs), the position sensitivity or duties associated, and the agency authorized to conduct PSIs.

FEMA Emergency Management Institute

IS-906 - Workplace Security Awareness

This course provides guidance to individuals and organizations on how to improve the security in their workplace. No workplace—be it an office building, construction site, factory floor, or retail store—is immune from security threats. Employees are often the target of these threats as well as the organization's first line of defense against them. Threats endanger the confidentiality, integrity, and security of your workplace, as well as your virtual workplace and computer systems. This course presents information on how employees can contribute to your organization's security.

IS-907 - Active Shooter: What You Can Do

Active shooter situations are unpredictable and evolve quickly. All employees can help prevent and prepare for potential active shooter situations. This course provides guidance to individuals, including managers and employees, so that they can prepare to respond to an active shooter situation. This course is not written for law enforcement officers, but for non-law enforcement employees. The material may provide law enforcement officers information on recommended actions for non-law enforcement employees to take should they be confronted with an active shooter situation.

IS-914 - Surveillance Awareness: What You Can Do

The purpose of this course is to make critical infrastructure employees and service providers aware of actions they can take to detect and report suspicious activities associated with adversarial surveillance. To achieve this goal, the course provides an overview of surveillance activities and the indicators associated with them, as well as the actions that employees and service providers can take to report potential surveillance incidents.

IS-915 - Protecting Critical Infrastructure Against Insider Threats

This course provides guidance to critical infrastructure employees and service providers on how to identify and act against Insider Threats to critical infrastructure. At the end of this course, participants will be able to describe the threat posed by malicious insiders, identify common characteristics of malicious insiders, and actions that can be taken against Insider Threats.

IS-916 - Critical Infrastructure Security: Theft and Diversion – What You Can Do

This course introduces critical infrastructure personnel to the information they need and the resources available to them to identify threats and vulnerabilities to critical infrastructure from the theft and diversion of critical resources, raw materials, and products that can be used for criminal or terrorist activities. The course also identifies actions that participants can take to reduce or prevent theft and diversion.

Carnegie Mellon University*

*<u>**Note**</u>: A fee may be required for Carnegie Mellon courses:

Building an Insider Threat Program

This course provides a thorough understanding of the organizational models for an Insider Threat program, the necessary components to have an effective program, the key stakeholders who need to be involved in the process, and basic education on the implementation and guidance of the program. This training is based upon the research of the CERT Insider Threat Center of the Software Engineering Institute.

Insider Threat Analyst

This three-day course presents strategies for collecting and analyzing data to prevent, detect, and respond to insider activity. It discusses various techniques and methods for designing, implementing, and measuring the effectiveness of various components of an Insider Threat data collection and analysis capability.

Insider Threat Awareness Training

This course provides a basic understanding of Insider Threats within an organization and what employees should be aware of in their responsibilities to protect an organization's critical assets. This course explains how your work can be affected and how you can be targeted by Insider Threats.

Insider Threat Program Evaluator (ITPE) Certificate

The ITPE program enables evaluators to help organizations gain a better understanding of the effectiveness of their established Insider Threat programs. Organizations will have the ability to license the CERT Insider Threat Program Evaluation methodology for internal use or to evaluate the effectiveness of other programs.

Insider Threat Program Manager: Implementation and Operation

This three-day course builds upon the initial concepts presented in the prerequisite courses Overview of Insider Threat Concepts and Activities and Building an Insider Threat Program. The course presents a process roadmap that can be followed to build the various parts of a robust Insider Threat Program. It discusses various techniques and methods to develop, implement, and operate program components.

Insider Threat Program Manager (ITPM) Certificate

The ITPM certificate program will assist insider threat program managers in developing a formal insider threat program. The certificate will cover areas such as insider threat planning, identification of internal and external stakeholders, components of an insider threat program, insider threat team development, strategies for effective communication of the program, and how to effectively implement and operate the program within the organization.

Insider Threat Vulnerability Assessor (ITVA) Certificate

The ITVA program enables assessors to help organizations gain a better understanding of their insider threat risk and an enhanced ability to identify and manage associated risks. The assessment methodology assists organizations by measuring how prepared they are to prevent, detect, and respond to the insider threat. Organizations will have the ability to license the CERT Insider Threat Vulnerability Assessment tool for internal use or to assess others for potential vulnerabilities.

Overview of Insider Threat Concepts and Activities

This course provides a thorough understanding of Insider Threat terminology, identifies different types of Insider Threats, teaches how to recognize both technical and behavioral indicators, and outlines mitigation strategies.

Cybersecurity and Infrastructure Security Agency (CISA)

Insider Threat Mitigation Workshop

This workshop provides public and private sector stakeholders with information regarding potential threats posed by insiders. The workshop also provides insights on consequences resulting from a successful attack or unintended action and suggests cost-effective measures to mitigate risk. CISA's Insider Threat Mitigation Workshop provides organizations with the tools to establish or improve their insider threat mitigation program through comprehensive guidance, interactive questions, and breakout sessions among participants.

National Counterintelligence and Security Center (NCSC)

Any Given Day – An Insider Threat Short

This eight-minute video was produced to enhance insider threat education and awareness. It highlights the balance between collecting information and privacy concerns and presents a side of insider threat programs that is not often considered: protecting national security at the human level. Executive Order 13587 focuses on safeguarding classified networks and classified information, but it's not just about information, it's also about protecting people.

Insider Threat Training

This training addresses a variety of insider threat matters such as leaks, spills, espionage, sabotage, and targeted violence.

Mental Wellness Training

This training was developed to explain challenges the workforce may endure if they are experiencing mental health issues. While there are times when behaviors of security concern overlap with mental disorders and require further review, the overwhelming reason for an employee to visit an agency's EAP is to have an objective, trained professional help sort out generally temporary and minor emotional problems.

Joint Knowledge Online (JKO)

DCPAS-001 - Preventing Workplace Violence for Employees

This course presents an introduction to the concepts of Workplace Violence (WPLV) at the employee level to include processes, personnel, and practices designed to address the threat of WPLV.

DCPAS-002 - Preventing Workplace Violence for Supervisors

This course presents an introduction to the concepts of WPLV at the supervisory level to include processes, personnel, and practices designed to address the threat of WPLV.

DEOMI-GEN-3000 - Organizational Socialization

This course is designed for DOD customers but is also open to the public. Upon completing this lesson, you should be able to Understand what Organizational Socialization is and how effectively leveraging the onboarding process contributes to mission success.

EUC-ECJ6-110-N - Operations Security (OPSEC) Annual Refresher Course

The purpose of this course is to provide in-depth OPSEC awareness training. The course will cover threat and potential adversaries. The OPSEC course will satisfy one of two requirements in OSPEC training.

PREV-001 - Violence: A Preventable Public Health Issue

This course will provide prevention personnel with a basic understanding of violence prevention concepts and approaches that can be applied to their environment. This course focuses on five forms of violence - child abuse, domestic abuse, harassment, sexual assault, and suicide.

Applied Research Laboratory for Intelligence and Security (ARLIS), University of Maryland

***For more information about these four courses provided by ARLIS, please visit the ARLIS homepage or UMD Academic Catalog.

BSST650 - Foundations of Insider Risk Management and Mitigation*

BSST651 (ARLIS) - The Psychology of Malicious Insiders*

BSST652 (ARLIS) - Managing Insider Threat Activities*

BSST653 (ARLIS) - Investigative Thinking, Analysis, and Decision-Making in Insider Risk Management and Mitigation*

MARYMOUNT UNIVERSITY

FLP 576 - Foundations of Insider Threat

The risks posed by trusted insiders to organizations in both the public and private sector are well documented. Past compromises of national security information have provided sensitive information to U.S. adversaries; theft or compromise of proprietary data and intellectual property has impacted businesses large and small; and incidents of workplace violence perpetrated by insiders are on the rise. This course provides context for the counter-insider threat mission and explores multi-disciplinary insider risk management concepts. The course addresses matter of policy, political and socio-economic impacts, psychological factors, and gives special consideration to issues of cyber insider threat, privacy and civil liberties, kinetic violence, and related social and behavioral science research.

Certification Programs

Certified Counter-Insider Threat Professional (CCITP)

In 2011, Executive Order 13587 established the requirement for all United States Government (USG) Executive Agencies to establish an Insider Threat Program. The Executive Order also established the National Insider Threat Task Force (NITTF), co-led by the Office of the Director of National Intelligence (ODNI) and the Department of Justice (DoJ), and the minimum standards by which a Counter-Insider Threat (C-InT) program would be deemed operational. The Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)), in partnership with the NITTF, focused on the people-related aspect of the C-InT capability and created two professional certifications: CCITP-F and CCITP-A.

Global Counter-Insider Threat Professional (GCITP) Certification Program

In 2021, a feasibility study regarding CCITP was conducted to identify the key similarities and differences between the USG and private industry. The study resulted in the establishment of a new essential body of work (EBW) and a new Essential Body of Knowledge (EBK), which were then validated through a Job Task Analysis (JTA) from among C-InT professionals from the USG and private industry to become the foundational standards for the development of the new Global Counter-Insider Threat Professional (GCITP) Program. The GCITP is the first C-InT certification program developed for a global audience and made available to both Government and private industry professionals.