COURSE SYLLABUS

Counterintelligence for Information Security Assessment and Protection for Investigators Course

Gain an introduction to today’s threats (criminals, foreign intelligence services, terrorists, malicious code writers, hackers/hacktivists, and disgruntled employees) to sensitive and classified information, your employees, and your resources. Learn about the multifaceted threat of intrusion and exfiltration that companies and agencies face today, as well as tactics you can employ to combat it. Clearly understand the multifaceted threat to sensitive and classified information, resources, and personnel. Effectively articulate this threat to employees as part of your security and risk prevention education and training effort.

> Group classes in Live Online and onsite training is available for this course. For more information, email onsite@graduateschool.edu or visit: https://sdfm.graduateschool.edu/courses/counterintelligence-for-information-security-assessment-and-protection-for-investigators

CustomerRelations@graduateschool.edu •

(888) 744-4723

Course Outline

Module 1: Counterintelligence

- Define counterintelligence, espionage, and leakage, and why the threat is multi-faceted (external and internal).
- Identify U.S. critical infrastructure sectors and apply the “five D’s” (deter, deceive, disrupt, deny, defeat).
- Review roles, responsibilities, and reporting expectations for security professionals and cleared employees.
- Discuss case studies to recognize tactics, techniques, and procedures used by foreign intelligence entities.

Module 2: Who Is the Threat and What Do They Want?

- Survey significant nation-state collectors and the top targeted technologies (e.g., electronics, C4, software).
- Map common methods of operation: resume submissions, business exploitation, insider access, and cyber operations.
- Analyze notable cases and “hall of shame” examples to connect motives, methods, and impacts.
- Differentiate economic vs. traditional espionage and assess risk to cleared industry and government operations.

Module 3: Domestic Terrorism and Domestic Violent Extremist (DVE) Groups

- Define domestic terrorism and DVE; understand constitutional guardrails around protected speech and activity.
- Examine the five U.S. DT threat categories (RMVE, anti-government/authority, animal/environmental, abortion-related, other).
- Review current assessment and data trends on lone offenders and small-cell threats.
- Apply definitions and categories to investigative triage and information sharing.

Module 4: Classified Information and Foreign Travel as a Clearance Holder

- Explain classification levels (C, S, TS), handling rules, and CUI/NOFORN protections.
- Clarify SCI/SAP handling and SCIF requirements; recognize Five Eyes access considerations.
- Apply SEAD-3 reporting requirements for unofficial foreign travel and pre-travel threat briefings.
- Practice need-to-know, dissemination controls, and safeguarding measures.

Module 5: The Cyber Threat and the Criminal/Terrorism Connection

- Define cyber threats and review trends in intrusions, attempted intrusions, and social-media targeting.
- Identify nation-state and criminal actors, their collaboration, and why attackers hold the advantage.
- Assess geo-tagging, mobile devices, and cloud risks; recognize common exfiltration vectors.
- Review U.S. response and coordination guidance for significant cyber incidents.

Module 6: Insider Threats

- Define insider threat and examine primary motivations: divided loyalties, disgruntlement, money, and ingratiation.
- Interpret historical and modern cases; connect personal risk indicators to adjudicative guidelines.
- Review NISPOM insider-threat program requirements and continuous evaluation practices.
- Implement early-warning, reporting, and mitigation strategies in partnership with HR, IT, and leadership.

Module 7: Tools to Use in Counterintelligence

- Leverage enterprise risk management, OPSEC, training, and awareness programs to reduce exposure.
- Use reporting channels, adverse-information submissions, and referral pathways to act on indicators.
- Apply access controls, monitoring, and incident response playbooks to protect people, data, and facilities.
- Integrate multi-discipline collaboration (CI, HR, IT, management, vendors) for holistic threat mitigation.