COURSE SYLLABUS

Counterintelligence for Information Security Assessment and Protection Course

Learn how to assess information systems for counterintelligence threats and apply protective measures aligned with federal guidelines.

Group classes (Live Online) and onsite training are 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



CustomerRelations@graduateschool.edu • (888) 744-4723

Course Outline

Module 1: Counterintelligence

- Define counterintelligence and explain its role in information security
- Identify internal and external threats to cleared industries
- Discuss the 16 U.S. critical infrastructure sectors
- Apply the “Five D’s” of counterintelligence: deter, deceive, disrupt, deny, and defeat

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

- Identify nation-states and technologies targeted for espionage
- Understand methods used to steal economic and defense secrets
- Explore real-world espionage cases and motivations
- Examine foreign intelligence services and their operations

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

- Define domestic terrorism and categorize violent extremist groups
- Understand threat trends from racially motivated and anti-government actors
- Analyze legal definitions and reporting structures for DT threats

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

- Explain classification levels and handling protocols
- Describe SEAD 3 reporting requirements for foreign travel
- Understand Controlled Unclassified Information (CUI) and Five Eyes alliance

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

- Identify cyber threats and the actors behind them
- Discuss emerging cyber espionage tactics and attack vectors

- Analyze the exploitation of mobile and social technologies

Module 6: Insider Threats

- Define insider threats and understand their motivations
- Review historical and recent insider espionage cases
- Learn indicators of espionage, financial distress, and misuse of IT resources

Module 7: Tools to Use in Counterintelligence

- Administer SF-312 agreements and conduct security training
- Use physical and IT security measures to detect threats
- Apply insider threat indicators and conduct risk assessments