COURSE SYLLABUS

Security Specialist Course

Acquire foundational knowledge in personnel, physical, information, and cybersecurity program components relevant to federal security responsibilities.

Group classes in Live Online and onsite training is available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/security-specialist-course

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

Course Outline

Module 1: Physical Security: Design and Assessment

- Understanding the layers of defense that protect personnel, assets, and classified information, and the roles of HR, senior management, supervisors, and security staff.
- Applying the four D's — deter, delay, detect, and deny — and Crime Prevention Through Environmental Design (CPTED) to assess a facility.
- Conducting a site survey and building the physical security plan and its supporting standard operating procedure.
- Recognizing everyday vulnerabilities including tailgating, vendor and visitor access, shared copy machines, unsecured laptops, discarded trash, and elicitation attempts.

Module 2: Physical Security: Threats and Incident Response

- Developing a bomb incident plan covering notification, evacuation, search procedures, and standoff distance.
- Preparing employees for workplace violence and active shooter incidents using the Avoid, Deny, Defend response model.
- Establishing a Critical Incident Response Team (CIRT) and continuity of operations (COOP) planning.
- Assessing emerging threats from unmanned aircraft systems (UAS), and safeguarding classified material in the workspace.

Module 3: The Cyber Threat and the Criminal/Terrorism Connection

- Understanding how cyber espionage, criminal intrusion, and social engineering intersect with physical and personnel security.
- Advising cleared employees on device preparation, geolocation exposure, and cyber precautions before, during, and after foreign travel.
- Recognizing social media deception and deepfakes, and the unintentional insider threat they create.

Module 4: Insider Threat Program

- Tracing the origins of federal insider threat programs and the authorities that require an agency program.
- Recognizing the behavioral and technical indicators of a potential insider threat.
- Analyzing documented espionage and insider threat cases to identify the indicators that were present and the reporting opportunities that were missed.
- Understanding the security specialist's role in the program, including what to report and to whom.

Module 5: Personnel Security: Investigations and Eligibility

- Defining national security eligibility and the requirements for access to classified information.

- Matching a position's risk and sensitivity to the correct investigative tier under the Federal Investigative Standards.
- Understanding citizenship requirements, Limited Access Authorization (LAA), and how a clearance is justified.
- Working through the investigation from initiation to subject interview, and what the security specialist can do to improve its speed and quality.

Module 6: Personnel Security: Adjudication and Due Process

- Applying the whole-person concept and the additional factors that shape an eligibility determination.
- Working through all 13 adjudicative guidelines of Security Executive Agent Directive (SEAD) 4, each with supporting case studies.
- Identifying disqualifying and mitigating conditions, and applying Bond Amendment restrictions.
- Understanding the due process afforded when eligibility is denied or revoked.

Module 7: Security Education, Briefings, and Continuous Evaluation

- Meeting the security education and training requirements of Executive Order 13526 and ISOO Directive 1, and documenting delivery.
- Delivering the initial security briefing and administering the SF-312 Nondisclosure Agreement.
- Distinguishing the initial, refresher, special, foreign travel, and termination briefings, and when each is required.
- Applying SEAD 6 continuous evaluation requirements, including adverse information and how employees report it.

Module 8: Classification Management and Marking

- Tracing classification authority through the executive orders culminating in Executive Order 13526.
- Distinguishing original from derivative classification and identifying who may perform each.
- Applying the automatic, systematic, and mandatory declassification programs and the exemption codes.
- Marking classified documents with banner lines, portion markings, and dissemination controls, and handling Controlled Unclassified Information (CUI).