

Security Specialist Course (Self-Paced)

Acquire foundational knowledge in personnel, physical, information, and cyber security 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-self-paced>



support@graduateschool.edu •

[\(888\) 744-4723](tel:(888)744-4723)

Course Outline

Module 1: Introduction to Physical Security

- Understanding the first layers of defense in protecting personnel, assets, and classified information.
- Overview of physical and personnel security, including the role of HR, senior management, and security staff in the program.
- Examining the supervisors' role in identifying threats and ensuring adherence to security measures.

Module 2: Physical Security Site Planning

- Creating a physical security site plan to safeguard personnel and assets against threats such as espionage, terrorism, and theft.
- Exploring various security measures such as video monitoring, intrusion detection, and access control to enhance protection.
- Planning security with crime prevention through environmental design (CPTED) strategies and effective site assessments.

Module 3: A Common-sense Approach to Physical Security

- Implementing risk management strategies to prioritize vulnerabilities and mitigate potential threats effectively.
- Assessing threats such as tailgating, hackers, and unauthorized access, and implementing appropriate countermeasures.
- Training employees to recognize and respond to security threats, including safeguarding sensitive data and information.

Module 4: Other Physical Threats

- Understanding and preparing for bomb threats, workplace violence, and other physical threats to the security of personnel and facilities.
- Developing and executing a bomb incident plan, including evacuation, search, and disposal procedures.
- Identifying critical incident response teams (CIRT) and ensuring proper response to potential threats.

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

- Understanding the intersection between cybersecurity threats and physical security, including the rise of cyber espionage and terrorism.
- Exploring the threats posed by cybercriminals, including social engineering tactics like phishing, and the importance of cybersecurity in physical security.
- Educating employees about risks related to mobile device security, password protection, and social media deception.