COURSE SYLLABUS

Insider Threat Awareness Course

A half-day live session on insider threat: what the indicators really look like, where to report them, and how insider threat reporting differs from a protected whistleblower disclosure.

Group classes (Live Online) and onsite training are available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/insider-threat-awareness



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

Course Outline

Module 1

- Understanding Insider Threats
- What counts as an insider, including current and former employees, contractors, and trusted business partners
- The malicious, negligent, or exploited categories
- Composite scenarios illustrating each
- The national security, safety, financial, and mission-continuity consequences

Module 2

- The Legal and Policy Framework
- Executive Order 13587
- The National Insider Threat Policy and Minimum Standards
- The role of the National Insider Threat Task Force
- The initial and annual training requirement for cleared personnel
- How agency policy takes precedence

Module 3

- Recognizing Behavioral and Technical Indicators
- What a potential risk indicator is and why one indicator proves nothing
- Behavioral indicators including unexplained financial distress, disgruntlement, and interest beyond need-to-know
- Technical indicators including after-hours access, unusual data volume, unauthorized removable media, and control bypass attempts
- Handling personal-stressor indicators with care

Module 4

Reporting: Your Responsibilities and Protections (30 min): reporting channels; what happens after a report and why the employee's role ends there; reporting promptly rather than waiting for certainty; the distinction between insider threat reporting and protected whistleblower disclosure; anti-retaliation protections for good-faith reports

Module 5

- Prevention, Mitigation, and Your Role

- Individual best practices covering credentials, need-to-know, removable media, social engineering, and offboarding
- The multidisciplinary nature of a mature program spanning security, HR, legal, IT, counterintelligence, and employee assistance
- Lessons-learned vignette and course recap