

€ TRAINING

Advanced Developing Field Leaders in
Industrial Security





Advanced Developing Field Leaders in Industrial Security

Introduction:

This Course provides an introduction to the Industrial Security Program as well as a thorough understanding of the DoD and National Industrial Security Program NISP rules, procedures, and requirements. The course also provides an in-depth review of the Certification and Accreditation C&A process. Upon completion of this Course, the candidates should have the knowledge to implement the basic industrial security requirements of the National Industrial Security Program Operating Manual NISPOM. These are the same requirements that every cleared contractor facility participating in the National Industrial Security Program NISP follows and on which any additional security requirements imposed by the government should be based. Upon completion of all courses in the curriculum and the passing of the individual course exams students will be issued a Basic Industrial Security for the Government Security Specialist eLearning Certificate. Industrial Security Program. The course presents the legal and regulatory basis for the program and how the program is implemented throughout DoD. This course includes an overview of DoD implementation of the National Industrial Security Program NISP and discussion of including in contracts security requirements that are outside the scope of NISP.

Course Objectives:

At the end of this course the participants will be able to:

- Become an effective information security manager
- Get up to speed quickly on information security issues and terminology
- Establish a minimum standard of security knowledge, skills, and abilities
- Speak the same language as technical security professionals
- Targeted Audience:
 - Security Managers
 - Security Professionals
 - Managers

Course Outlines:

Unit 1:

Document Security:

- Creation & Marking
- Storage & Accountability

- Transmission & Receipting
- Reproduction & Destruction
- End of Contract Actions
- Emergency Actions and Physical Protections
- Access Controls

Unit 2:

Information Systems Security:

- System Security Plans
- Accreditation
- Physical Protections
- Administrative & Procedural Controls
- Forensics
- Reporting & Records
- Destruction

Unit 3:

Physical Security:

- Theory: Graded & Layered Protection
- Locks & Security Containers
- Vaults & Vault-type Rooms
- Alarms
- CCTV
- Central Alarm Stations & Requirements
- Access Con

Unit 4:

Personnel Security:

- Forms
- Adjudication
- EPSQ/JPAS
- Clearances & Badges

Unit 5:

International Security:

- Export Control Regulations
- Foreign Visits & Assignments
- Foreign Ownership, Control, or Influence
- Controlling Access by Foreign Persons

Unit 6:

Classification:

- Identifying Critical Information
- Classification System & Guides
- Declassification

Unit 7:

Security Education:

- Requirements and Content
- Ideas & Techniques

Unit 8:

Audits & Self-Assessments:

- Audits
- Self-Assessments



Unit 9:

Electives:

- Intellectual Property
- COMSEC/TEMPEST
- Counterintelligence
- Operations Security OPSEC
- SAP1