



**This five-day overview program is based upon the National Security Agency's Directive for National Training Standard. This standard is issued by the Committee on National Security Systems (CNSS) as specified in CNSSI No. 4014; Information System Security Officer (ISSO).**

This course addresses the entry level standards which cover the fundamentals of Information Systems from a top-down approach. Various topics addressed in the course include IT Governance, certification and accreditation, public key infrastructures, configuration management, intrusion detection and incident response. Given a series of system security breaches, the ISSO will identify system vulnerabilities and recommend security solutions required to return the system to an operational level of assurance.

### **Audience**

This course is intended for officials in government or private industry working in the area of Information Security, wishing to become Information System Security Officer, or needing to advance their skills and knowledge in managing systems and organization security.

### **You will learn how to:**

- Explain the importance of IT governance as part of the role of the ISSO responsibility
- Define Confidentiality, Integrity and Availability for Information Systems Security
- Describe the certification and accreditation and explain their importance for an organization and the ISSO
- Describe the necessities in implementing a site Security Policy and its importance to the Department of National Defence and to other organizations
- Explain the importance of reporting the status of site security for the ISSO

**Setting the Foundation and Understanding your Role**

1. Security Concepts
2. Security Practices
3. Security Policies
4. ISSO Defined
5. Common Responsibilities
6. Types of ISSO
7. Type-specific Responsibilities

**Understanding, Implementing and Managing Site Security**

1. Confidentiality, Integrity and Availability for Sites
2. Site Security Principles
3. The Role of Site Security Policy
4. Site Security Policies
5. Plans and Procedures
6. Facility Approval
7. Operational Management
8. Access Control
9. Incident Response

**Understanding, Implementing and Managing System Security**

1. Confidentiality, Integrity and Availability for Systems
2. System Security Principles
3. The Role of System Security Policy
4. System Security Policies
5. Plans and Procedures
6. Media Handling
7. Security Tools and Methods
8. Operational Management
9. Incident Response

**Understanding and Developing Site and System Reporting**

1. Report Categories
2. Measurement
3. Reporting Roles and Responsibilities
4. Reporting Audiences
5. Report Planning
6. Reporting Formats and Conventions
7. Reporting to Management
8. Legal Considerations

**Achieving Security Certification and Accreditation**

1. Certification and Accreditation
2. Certification Practices
3. Certification Elements
4. Personnel Accreditation
5. Systems Accreditation (Type Accreditation)
6. Accreditation Activities