

NATIONAL TRAINING STANDARD FOR INFORMATION SYSTEMS SECURITY (INFOSEC) PROFESSIONALS

NSTISSI No. 4011 20 June 1994



Comp 6370 – NSTISS Basics – Awareness Level



Performance Levels

- **Awareness Level.** Creates a sensitivity to the threats and vulnerabilities of national security information systems, and a recognition of the need to protect data, information and the means of processing them; and builds a working knowledge of principles and practices in INFOSEC.
- **Performance Level.** Provides the employee with the skill or ability to design, execute, or evaluate agency INFOSEC security procedures and practices. This level of understanding will ensure that employees are able to apply security concepts while performing their tasks.



Comp 6370 – NSTISS Basics – Awareness Level



Legal Elements

- **evidence collection and preservation**
 - intrusion detection and monitoring
 - case study, NSA
- **fraud, waste and abuse**
 - hotlines
 - signs of computer intrusion
 - case study, Lawrence Livermore break-in
- **investigative authorities**
 - Federal
 - DOJ
 - DOD
 - State



Comp 6370 – NSTISS Basics – Awareness Level



Countermeasures

- **Cover and deception**
- **Technical surveillance countermeasures**
- **Threat and Vulnerability Assessment**



Comp 6370 – NSTISS Basics – Awareness Level



Concepts of Trust

- **Assurance**
- **Policy**



Comp 6370 – NSTISS Basics – Awareness Level



Modes of Operation

- **Compartmented/Partitioned**
- **Dedicated**
- **System-high**



Comp 6370 – NSTISS Basics – Awareness Level



Roles of Various Organizational Personnel

- Audit office *
- COMSEC custodian
- end users information resources management staff
- INFOSEC Officer
- OPSEC managers
- program or functional managers
- security office
- senior management
- system manager
- system staff
- telecommunications office and staff



Comp 6370 – NSTISS Basics – Awareness Level



7

What is OPSEC?

- Operations security (OPSEC) is an analytic process used to deny an adversary information - generally unclassified
- Trains people on the handling of information
- We can apply OPSEC in our daily lives
 - “What could an adversary glean from the knowledge of this activity?”



Comp 6370 – NSTISS Basics – Awareness Level



8

Facets of NSTISS

- protection of areas
- protection of data communications
- protection of equipment
- protection of keying material protection of magnetic storage media
- protection of voice communications reporting security violations
- transmission security countermeasures (e.g., call signs, frequency, and pattern forewarning protection)



Comp 6370 – NSTISS Basics – Awareness Level



9

Agency Specific Security Policies

- guidance
- points of contact
- roles and responsibilities



Comp 6370 – NSTISS Basics – Awareness Level



10

Risk Management

- information identification
- risk analysis and/or vulnerability assessment components
- risk analysis results evaluation
- roles and responsibilities of all the players in the risk analysis process



Comp 6370 – NSTISS Basics – Awareness Level



11

Security Planning

- directives and procedures for NSTISS policy
- NSTISS program budget
- NSTISS program evaluation
- NSTISS training (content and audience definition)



Comp 6370 – NSTISS Basics – Awareness Level



12

Contingency Planning/Disaster Recovery

- agency response procedures and continuity of operations
- development of plans for recovery actions after a disruptive event
- development of procedures for off-site processing
- emergency destruction procedures
- team member responsibilities in responding to an emergency situation



Comp 6370 – NSTISS Basics – Awareness Level



13

Physical Security Measures

- alarms
- building construction
- cabling
- communications centers
- environmental controls (humidity and air conditioning)
- filtered power
- fire safety controls
- information systems centers
- physical access control systems (key cards, locks and alarms)
- power controls (regulator, uninterruptible power service (UPS), and emergency power-off switch)
- protected distributed systems
- shielding
- stand-alone systems and peripherals
- storage area controls



Comp 6370 – NSTISS Basics – Awareness Level



14

Software Security

- assurance
- configuration management (documentation)
- configuration management (programming standards and controls)
- software security mechanisms to protect information (identification and authentication)
- software security mechanisms to protect information (internal labeling)
- software security mechanisms to protect information (need-to-know controls)
- software security mechanisms to protect information (segregation of duties)



Comp 6370 – NSTISS Basics – Awareness Level



15

Administrative Security Procedural Controls

- destruction of media
- documentation, logs and journals
- emergency destruction
- external marking of media
- media downgrade and declassification
- preparation of security plans
- reporting of computer misuse or abuse
- sanitization of media
- transportation of media



Comp 6370 – NSTISS Basics – Awareness Level



16

Auditing and Monitoring

- conducting security reviews
- effectiveness of security programs
- investigation of security breaches
- review of accountability controls
- verification, validation, testing, and evaluation processes



Comp 6370 – NSTISS Basics – Awareness Level



17

Key Management

- Access, control and storage of COMSEC material
- destruction procedures for COMSEC material
- identify and inventory COMSEC material
- key management protocols (bundling, electronic key, over-the-air rekeying)
- report COMSEC incidents



Comp 6370 – NSTISS Basics – Awareness Level



18

Transmission Security

- burst transmission
- directional signals
- jamming
- line-of-sight
- line authentication
- low power
- masking
- optical systems
- protected wireline
- screening



Comp 6370 – NSTISS Basics – Awareness Level



19

TEMPEST Security

- attenuation
- banding
- cabling
- filtered power
- grounding
- shielding
- TEMPEST separation
- zone of control/zoning



Comp 6370 – NSTISS Basics – Awareness Level



20

Legal Issues

- (1) explain the legal responsibilities of the DAA;
- (2) discuss the Computer Fraud and Abuse Act, P.L. 99-474, 18 U.S. Code 1030;
- (3) discuss Copyright Protection and License, Copyright Act of 1976, Title 17 U.S. Code, P.L. 102- 307, amended the Copyright Act of 1976, 1990;
- (4) discuss the Freedom of Information Act;
- (5) discuss the purpose and history of NSD 42;
- (6) discuss implications of the Privacy Act;
- (7) list and discuss the issues of Computer Security Act of 1987(P.L. 100-235); and
- (8) list international legal issues which can affect INFOSEC.



Comp 6370 – NSTISS Basics – Awareness Level



21

Liabilities

- (1) state the importance of annual loss expectancy;
- (2) list the damage which can occur when anti-virus programs are not used;
- (3) determine the responsibilities associated with the business aspects of INFOSEC; and
- (4) explain the legal responsibilities of the data owner.



Comp 6370 – NSTISS Basics – Awareness Level



22

Crime

- (1) explain how audit analysis tools can be useful in crime analysis;
- (2) explain the importance of written procedures for evidence collection and preservation;
- (3) illustrate the importance of written procedures for investigation of security breaches;
- (4) describe how collection methods can affect evidence acceptability;
- (5) list the ways logs/journals can be important evidence in a suspected criminal investigation; and
- (6) describe the DAA role in witness interview and interrogation.



Comp 6370 – NSTISS Basics – Awareness Level



23

Issues

- (1) explain the dangers of not using your agency's Computer Emergency Response Team (CERT);
- (2) discuss the effects of disregarding COMSEC policy and guidance;
- (3) illustrate the ramifications of improper disposition of classified information;
- (4) determine the effects of threats to electronic data interchange to systems in your agency;
- (5) explain the consequences of damage occurring to electronic funds transfer to systems in your agency;
- (6) explain how unauthorized modifications to electronic mail affect your agency;
- (7) outline the vulnerabilities associated with electronic records management;
- (8) describe the liabilities associated with electronic monitoring;
- (9) illustrate how fraud, waste, and abuse of computer resources can affect your agency's system security;
- (10) define the term "Information Warfare" (INFOWAR);
- (11) explain the DAA's role in information warfare through the use of INFOSEC;
- (12) describe ways in which connecting to the National Information Infrastructure can create risks to your systems;
- (13) define the term "national security information";
- (14) explain the DAA's role in the security violations reporting process;
- (15) discuss the importance of separation of duties;
- (16) explain software piracy; and
- (17) explain DAA responsibility for preventing unauthorized disclosure of information.



Comp 6370 – NSTISS Basics – Awareness Level



24

C&A Keys to Success

- Sponsorship (requirements analysis)
- Documentation (network architecture)
- Vulnerabilities (network/component)
- Self Diagnosed Risk
- Adequate Physical/Administrative Controls
- Conceptual Risk Assessment (CA endorsement)
- DAA Accreditation (IATO/ATO)



Comp 6370 – NSTISS Basics – Awareness Level



31

System Security Authorization Agreement

- Key to Success in the DITSCAP Process
- Initiated at Phase 1, used to evaluate the entire process
- Updated as necessary



Comp 6370 – NSTISS Basics – Awareness Level



32

SSAA Outline, Section 1

- 1 Mission Description and System Identification
 - 1.1 System Name and Identification
 - 1.2 System Description
 - 1.3 Functional Description
 - 1.3.1 System Capabilities
 - 1.3.2 System Criticality
 - 1.3.3 Classification and Sensitivity of Data Processed
 - 1.3.4 System User Description and Clearance Levels
 - 1.3.5 Life Cycle of the System



Comp 6370 – NSTISS Basics – Awareness Level



33

SSAA Outline, Section 2

- 2 Environment Description
 - 2.1 Operating Environment
 - 2.1.1 Facility Description
 - 2.1.2 Physical Security
 - 2.1.3 Administrative Issues
 - 2.1.4 Personnel
 - 2.1.5 COMSEC
 - 2.1.6 TEMPEST
 - 2.1.7 Maintenance Procedures
 - 2.1.8 Training Plans
 - 2.2 Software Development and Maintenance Environment
 - 2.3 Threat Description



Comp 6370 – NSTISS Basics – Awareness Level



34

SSAA Outline, Sections 3 & 4

- 3 System Architectural Description
 - 3.1 System Architecture Description
 - 3.2 System Interfaces and External Connections
 - 3.3 Data Flow
 - 3.4 Accreditation Boundary
- 4 System Security Requirement
 - 4.1 National and DoD Security Requirements
 - 4.2 Governing Security Requisites
 - 4.3 Data Security Requirements
 - 4.4 Security CONOPS
 - 4.5 Network Connection Rules
 - 4.6 Configuration Management Requirements
 - 4.7 Reaccreditation Requirements



Comp 6370 – NSTISS Basics – Awareness Level



35

SSAA Outline, Sections 5 & 6

- 5 Organizations and Resources
 - 5.1 Organizations
 - 5.2 Resources
 - 5.3 Training
 - 5.4 Other Supporting Organizations
- 6 DITSCAP Plan
 - 6.1 Tailoring Factors
 - 6.1.1 Programmatic Considerations
 - 6.1.2 Security Environment
 - 6.1.3 IS Characteristics
 - 6.1.4 Reuse of Previously Approved Solutions
 - 6.2 Tasks and Milestones
 - 6.3 Schedule Summary
 - 6.4 Level of Effort
 - 6.5 Roles and Responsibilities



Comp 6370 – NSTISS Basics – Awareness Level



36

SSAA Outline, Appendices

- Appendix A - Acronyms
- Appendix B - Definitions
- Appendix C - References
- Appendix D - System Concept of Operations
- Appendix E - Information System Security Policy
- Appendix F - Security Requirements and/or Requirements Traceability Matrix
- Appendix G - Certification Test and Evaluation Plan and Procedures (Type only)
- Appendix H - Security Test and Evaluation Plan and Procedures
- Appendix I - Applicable System Development Artifacts or System Documentation
- Appendix J - System Rules of Behavior
- Appendix K - Incident Response Plan
- Appendix L - Contingency Plans
- Appendix M - Personnel Controls and Technical Security Controls
- Appendix N - Memorandums of Agreement – System Interconnect Agreements
- Appendix O - Security Education, Training, and Awareness Plan
- Appendix P - Test and Evaluation Report
- Appendix Q - Residual Risk Assessment Results
- Appendix R - Certification and Accreditation Statement



Comp 6370 – NSTISS Basics – Awareness Level



37

C & A References

- NSTISSI 4009 - National Information Systems Security (INFOSEC) Glossary, January 1999
- NSTISSI No 4011 - National Training Standard for Information Systems Security (INFOSEC) Professionals
- NSTISSP Fact Sheet 11 – National Information Assurance Acquisition Policy, January 2000
- Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 6-8519 "Department of Defense Global Information Grid Information Assurance, June 2000
- DODInst 5200.40 Department of Defense Information Technology Security Certification and Accreditation Process



Comp 6370 – NSTISS Basics – Awareness Level



38