A. COMMUNICATIONS BASICS (Awareness Level)

Instructional Content
Describe vehicles of transmission III
Introduce the evolution of modern communications systems I

(1) Topical Content
(a) Historical vs. Current Methodology I
(b) Capabilities and limitations of various communications systems III, b
Asynchronous vs. synchronous III, b
Dedicated line III, e
Digital vs. analog III, e
Line of sight III, c
Microwave III, c
Public switched network III, e
Radio frequency (e.g., bandwidth) III, c
Satellite III, d

B. AUTOMATED INFORMATION SYSTEMS (AIS) BASICS (Awareness Level)

Instructional Content
Describe an AIS environment I
Provide language of an AIS I
Providing an overview of hardware, software, firmware components of an AIS to integrate into information systems security aspects/beaviors discussed later I

(1) Topical Content
(a) Historical vs. Current Methodology I
(b) Hardware I, a
Components (e.g., I/O, CPU) I, a
Distributed vs. stand alone I, f
Micro, mini, mainframe processors I, a
Storage devices I, c
(c) Software I, b
Applications I, b
Operating system I, b
(d) Memory I, c
Random I, c
Sequential I, c
Volatile vs. nonvolatile I, c
(e) Media I, d
Magnetic remanence I, d
Optical remanence I, d
(f) Networks I, b
Asynchronous vs. synchronous III, b
File servers I, b
Modems III, g
Sharing of data I
Sharing of devices I
Switching I, b, I, c
Topology I, c

C. SECURITY BASICS (Awareness Level)

Instructional Content
Using the Comprehensible Model of Information Systems Security, (contained in the Annex to this instruction), introduce a comprehensive model of information systems security that addresses:

Critical characteristics of information I, I, H
Information states I, I, H
Security measures I, I, H

(1) Topical Content
(a) INFOSEC Overview
Critical information characteristics - availability I, I

(b) Operations Security (OPSEC)
INFOSEC and OPSEC interdependency
OPSEC process
OPSEC surveys/OPSEC planning
Unclassified indicators

(c) Information Security
Application dependent guidance
Policy
Roles and responsibilities

(d) INFOSEC
Computer security - access control
Cryptography - encryption (e.g., point-to-point, network, link)
Computer security - audit
Computer security - identification and authentication
Computer security - object reuse
Cryptography - key management
Cryptography - strength (e.g., complexity, secrecy, characteristics of the key)
Emanations security
Physical, personnel and administrative security
Transmission security

D. NSTISS BASICS (Awareness Level)

Instructional Content
Describe components of NSTISS (with examples to include: national policy, threats and vulnerabilities, countermeasures, risk management, systems lifecycle management, trust, modes of operation, roles of organizational units, facets of NSTISS).

(1) Topical Content
(a) National policy and guidance
AIS security
Communications security
Employee accountability for agency information
Protection of information

(b) Threats to and vulnerabilities of systems
Definition of terms (e.g., threats, vulnerabilities, risk)
Major categories of threats (e.g., fraud, Hostile Intelligence Service (HOIS), malicious logic, hackers, environmental and technological hazards, disgruntled employees, careless employees, HUMINT, and monitoring)
Threat impact areas

(c) Legal elements
Criminal prosecution
Evidence collection and preservation
Fraud, waste and abuse
Investigative authorities

(d) Countermeasures
Assessments (e.g., surveys, inspections)
Cover and deception
Education, training, and awareness
HUMINT
Monitoring (e.g., data, line)
Technical surveillance countermeasures

(e) Concepts of risk management
Consequences (e.g. corrective action, risk assessment)
Cost/benefit analysis of controls
Implementation of cost-effective controls

(f) Concepts of system life Cycle Management
Demonstration and validation (testing)
Development
Implementation
Operations and maintenance (e.g., configuration management)
Requirements definition (e.g. architecture)
Security (e.g., certification and accreditation)

(g) Concepts of trust
Assurance
Mechanism
Policy

(h) Modes of operation
Compartmented/partitioned
Dedicated
Multilevel
System-high

(i) Roles of various organizational personnel
Audit office
<table>
<thead>
<tr>
<th>Facets of NSTISS</th>
<th>IX.a</th>
<th>VII</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application of cryptographic systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup of data and files</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protection against malicious logic</td>
<td>II.c</td>
<td>X, XI, XIII</td>
</tr>
<tr>
<td>Protection of areas</td>
<td>IX</td>
<td>X, XI, XIII</td>
</tr>
<tr>
<td>Protection of data communications</td>
<td>IX</td>
<td>X, XI, XIII</td>
</tr>
<tr>
<td>Protection of equipment</td>
<td>IX</td>
<td>X, XI, XIII</td>
</tr>
<tr>
<td>Protection of files and data</td>
<td>IX</td>
<td>X, XI, XIII</td>
</tr>
<tr>
<td>Protection of keying material</td>
<td>IX</td>
<td>X, XI, XIII</td>
</tr>
<tr>
<td>Protection of magnetic storage media</td>
<td>IX</td>
<td>X, XI, XIII</td>
</tr>
<tr>
<td>Protection of passwords</td>
<td>IX</td>
<td>X, XI, XIII</td>
</tr>
<tr>
<td>Protection of voice communications</td>
<td>IX</td>
<td>X, XI, XIII</td>
</tr>
<tr>
<td>Reporting security violations</td>
<td>V</td>
<td>X, XI, XIII</td>
</tr>
<tr>
<td>Transmission security countermeasures (e.g., callsigns, frequency, and pattern</td>
<td></td>
<td></td>
</tr>
<tr>
<td>forewarning protection</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

E. SYSTEM OPERATING ENVIRONMENT (Awareness Level)

**Instructional Content**

Describe agency "control points" for purchase and maintenance of Agency AIS and telecommunications systems

Outline Agency specific AIS and telecommunications systems

Review agency AIS and telecommunications security policies

(1) Topical Content

(a) AIS

Firmware | I.a
Hardware | I.a
Software | I.b

(b) Telecommunications systems

Hardware | I.e
Software | I.e

(c) Agency specific security policies

Guidance | IV, X, XI
Points of contact | IV, X, XI
Roles and responsibilities | IV, X, XI

(d) Agency specific AIS and telecommunications policies

Points of contact | IV, X, XI
References | IV, X, XI

F. NSTISS PLANNING AND MANAGEMENT (Performance Level)

**Instructional Content**

Discuss practical performance measures employed in designing security measures and programs

Introduce generic security planning guidelines/documents

(1) Topical Content

(a) Security planning

Directives and procedures for NSTISS policy | II
NSTISS program budget | II
NSTISS program evaluation | II
NSTISS training (content and audience definition) | II

(b) Risk management

Acceptance of risk (accreditation) | VII, VIII
Corrective actions | VII, VIII
Information identification | VII, VIII
Risk analysis and/or vulnerability assessment components | VII, VIII
Risk analysis results evaluation | VII, VIII
Roles and responsibilities of all the players in the risk analysis process | VII, VIII

(c) Systems lifecycle management

Acquisition | II.c
Design review and systems test performance (ensure required safeguards are
operational adequacy)

Determination of security specifications
Evaluation of sensitivity of the application based upon risk analysis
Management control process (ensure that appropriate administrative, physical, and technical safeguards are incorporated into all new applications and into existing applications)
Systems certification and accreditation process

(d) Contingency planning/disaster recovery
Agency response procedures and continuity of operations
Contingency plan components
Determination of backup requirements
Development of plans for recovery actions after a disruptive event
Development of procedures for offsite processing
Emergency destruction procedures
Guidelines for determining critical and essential workload
Team member responsibilities in responding to an emergency situation

G. NSTISS POLICIES AND PROCEDURES (Performance Level)

Instructional Content
List and describe: elements of vulnerability and threat that exist an AIS/telecommunications system with corresponding protection measures
List and describe: specific technological, policy, and educational solutions for NSTISS

(1) Topical Content
(a) 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
Standalone systems and peripherals
Storage area controls

(b) Personal security practices and procedures
Access authorization/verification (need to know)
Contractors
Employee clearances
Position sensitivity
Security training and awareness (initial and refresher)
Systems maintenance personnel

(c) Software security
Assurance
Configuration management (change controls)
Configuration management (documentation)
Configuration management (programming standards and controls)
Software security mechanisms to protect information (access privileges)
Software security mechanisms to protect information (application security features)
Software security mechanisms to protect information (audit trails and logging)
Software security mechanisms to protect information (concept of least privilege)
Software security mechanisms to protect information (identification and authentication)
Software security mechanisms to protect information (internal labeling)
Software security mechanisms to protect information (malicious logic protection)
Software security mechanisms to protect information (need to know controls)
Software security mechanisms to protect information (operating systems security features)
Software security mechanisms to protect information (segregation of duties)

(d) Network security
Dial up versus dedicated
End-to-end access control
Privileges (class, nodes)
Public versus private
Traffic analysis

(e) Administrative security procedural controls
Attribution
Construction, changing, issuing and deleting
Copyright protection and licensing
Destruction of media
Documentation, logs and journals
Emergency destruction
External marking of media
<table>
<thead>
<tr>
<th>Media downgraded and declassification</th>
<th>IV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preparation of security plans</td>
<td>IV</td>
</tr>
<tr>
<td>Reporting of computer misuse or abuse</td>
<td>IV</td>
</tr>
<tr>
<td>Repudiation</td>
<td>IV</td>
</tr>
<tr>
<td>Sanitization of media</td>
<td>IV</td>
</tr>
<tr>
<td>Transportation of media</td>
<td>IV</td>
</tr>
</tbody>
</table>

(f) Auditing and monitoring
- Conducting security reviews: VI, XII
- Effectiveness of security programs: VIII, XII
- Investigation of security breaches: VIII, XII
- Monitoring systems for accuracy and abnormalities: VIII, XII
- Privacy: VIII, XII
- Review of accountability controls: VIII, XII
- Review of audit trails and logs: VIII, XII
- Review of software design standards: IL.c, XVI
- Verification, validation, testing, and evaluation processes: IL.c, XVI

(g) Cryptosecurity
- Cryptovariable or key: VII
- Electronic key management system: VIII
- Encryption/decryption method, procedure, algorithm: VII

(h) Key Management
- Access, control and storage of COMSEC material: VIII
- Destruction procedures for COMSEC material: VIII
- Identify and inventory COMSEC material: VIII
- Key management protocols (bundling, electronic key, over-the-air rekeying): VIII
- Report COMSEC incidents: VIII

(i) Transmission Security
- Burst transmission: III.h, XIV
- Convert channel control (cross talk): III.h, XIV
- Dial back: III.h
- Directional signals: III.h
- Frequency hopping: III.h, XIV
- Jamming: III.h, XIV
- Line of sight: III.h
- Line authentication: III.h
- Low power: III.h
- Masking: III.h
- Optical systems: III.h
- Protected wireline: III.h
- Screening: III.h
- Spread spectrum transmission: III.h, XIV

(j) TEMPEST Security
- Attenuation: III.h
- Banding: III.h
- Cabling: III.h
- Filtered power: III.h
- Grounding: III.h
- Shielding: III.h
- TEMPEST separation: III.h
- Zone of control/zoning: III.h, XV.g