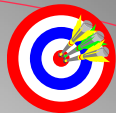





INFORMATION SYSTEM SECURITY

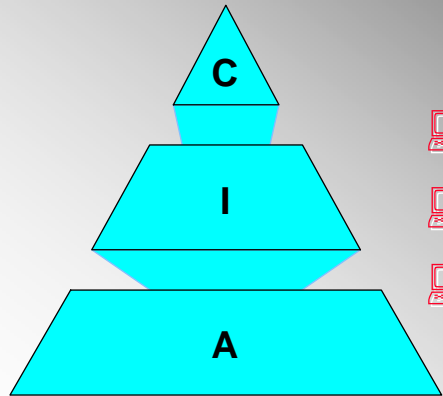
For
System Administrators



Objectives

-  Discuss the principles of Computer Security
-  Identify required IS security documentation
-  Identify the purpose of a System Security Plan (SSP)

Foundations of Computer Security



 **Confidentiality**

 **Integrity**

 **Availability**

CONFIDENTIALITY



**PROTECTION OF
DATA IN OR
PROCESSED BY
THE COMPUTER
SYSTEM FROM
DISCLOSURE**



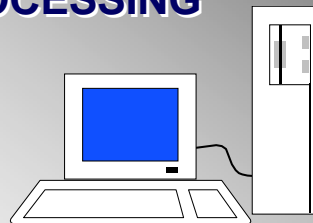
INTEGRITY

**PROTECTION OF ALL
COMPONENTS OF HARDWARE
AND SOFTWARE USED DURING
CLASSIFIED PROCESSING**

FROM:

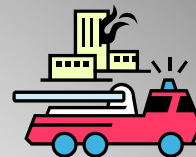
 **MANIPULATION**

 **DELETION**



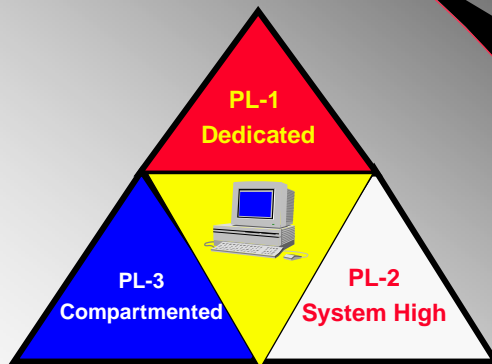
AVAILABILITY

**Protecting the
computer from
malicious logic
or natural
disasters**




Protection Levels

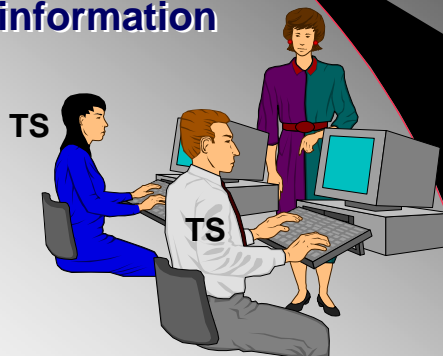
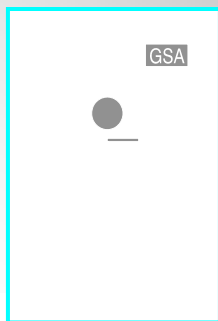
NISPOM 8-402



Protection Level (PL) 1

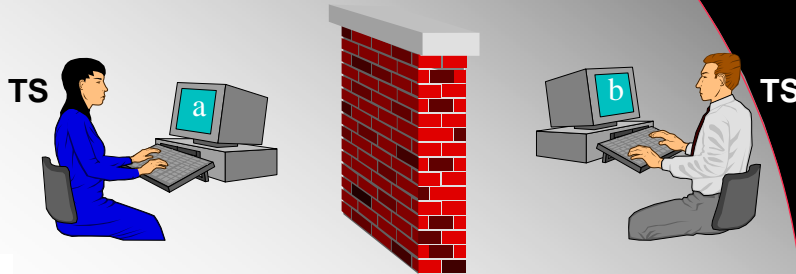
Dedicated Security Mode

 Clearance, N-T-K and, if applicable, all formal access approvals for all information



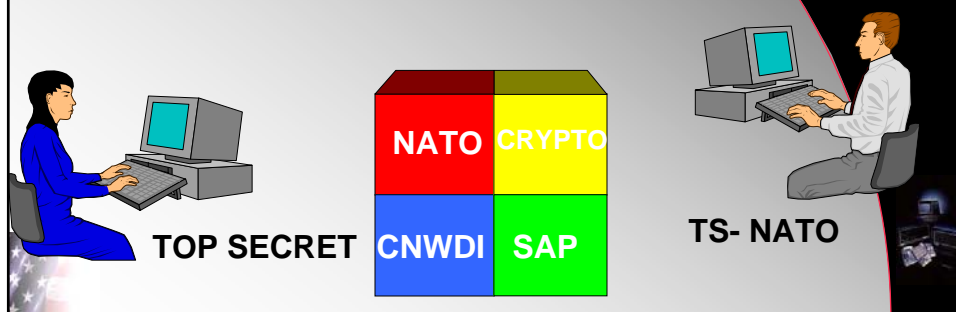
Protection Level (PL) 2 System High Security Mode

 Clearance and access approvals for all information but with different N-T-K



Protection Level (PL) 3 Compartmented Security Mode

 Clearance for most restrictive information, but different formal access approvals



Confidentiality Matrix

TABLE 5 - Protection Profile Table for Confidentiality

Requirements (Paragraph)	PL 1	PL 2	PL 3
Audit Capability (8-602)	Audit 1,	Audit 2,	Audit 3 Audit 4
Data Transmission (8-605)	Trans 1, ISL62	Trans 1	Trans 1
Access Controls (8-606)	Access 1,	Access 2	Access 3
Identification & Authentication (8-607)	I&A 1,	I&A 2,3,4	I&A2,4,5
Resource Control (8-608)		ResrcCtrl 1,	ResrcCtrl 1
Session Controls (8-609)	SessCtrl 1,	SessCtrl 2	SessCtrl 2
Security Documentation (8-610)	Doc 1,	Doc 1	Doc 1
Separation of Functions (8-611)			Separation
System Recovery (8-612)	SR 1	SR 1	SR 1
System Assurance (8-613)	SysAssur 1,	SysAssur 1	SysAssur 2
Security Testing (8-614)	Test 1,	Test 2	Test 3

Levels of Concern 8-403 Confidentiality

Level of Concern	Qualifiers
High	TOP SECRET and SECRET Restricted Data (SIGMA 1,2,14,15)
Medium	SECRET SECRET Restricted Data
Basic	CONFIDENTIAL



Security Documentation

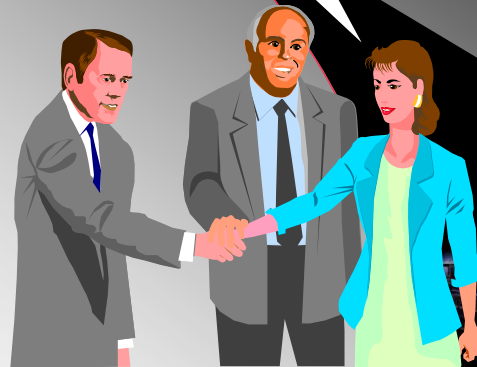
NISPOM 8-610



CSA (DoD) Role*

- Perform oversight, program review, training, and certification and accreditation of ISSs used by its contractors 8-202

We're your CSA Reps here to help you!



8-101a

Contractor Role*

- ❏ Publish and promulgate an IS Security Policy 8-101
- ❏ Appoint and train an Information Systems Security Manager (ISSM)



8-101b

IS Security Manager (ISSM)*

- ❏ Not necessarily the Facility Security Officer (FSO)
- ❏ Designated by Management
- ❏ The CSA's point of contact for IS security





IS Security Officer (ISSO)*

- ❑ Appointed by ISSM in facilities with multiple accredited IS
- ❑ Assists in day-to-day IS security operations
- ❑ Has PCL, NTK, and formal access approvals for all information processed on accredited IS



17

Basis for Accreditation

- ❑ Documentation (SSP)
- ❑ Analysis and evaluation of security risks
- ❑ Safeguards associated with operation of the AIS



Required Security Documentation

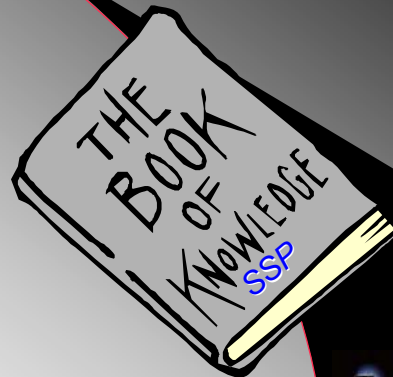
- Information System Security Policy
- Configuration Management Plan
- System Security Plan (SSP)
- Certification and Accreditation Documentation

8-610

19

What is the purpose of an SSP?









- Implements security policy
- User's *How-To* guide
- "Inspection" guide



8-610a(1)

SSP INCLUDES

System Identification

-  Master
-  Profile
-  Security personnel
-  System description
 -  Mission or purpose
 -  System architecture
 -  block diagram
 -  security support structure








8-610a.(1)(a)

21

SSP Includes, cont

System Requirements

-  Classification Level (C-S-TS)
-  Personnel Clearance Level of Users
-  Need to Know of Users
-  Formal Access Approvals involved
-  Protection Level (PL1, 2, or 3)

22

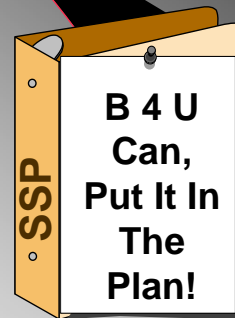
SSP-Protection Measures

- 📄 Audit Capabilities
- 📄 Access Controls
- 📄 Resource Controls
- 📄 System Recovery
- 📄 Security Testing
- 📄 Data Transmission
- 📄 I & A
- 📄 Session Controls
- 📄 System Assurance
- 📄 Physical Security

23

SSP-Protection Measures

- 📄 Trusted Downloading
- 📄 Software controls
- 📄 Media controls
- 📄 Maintenance
- 📄 Clearing and sanitization
- 📄 Self Inspections



24

SSP-Variations and Vulnerabilities

- 📄 Description of approved variations from protection measures

 - 📄 Attach documentation

- 📄 Documentation of any unique threat or vulnerabilities to system

 - 📄 Document if none exists

25

SSP-Might Also Include

- 📄 MOU for connections to separately accredited networks & systems

- 📄 Special purpose type systems
 - 📄 embedded systems

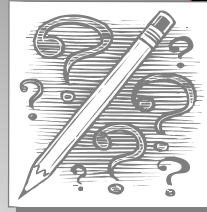
- 📄 Other contractual issues



26

Audit Records

- 📁 Who fills out what?
 - 📁 ISSOs & Users
- 📁 What logs are required? - Manual
 - 📁 Maintenance
 - 📁 Hardware & Software
 - 📁 Upgrade/Downgrade
 - 📁 Sanitization
 - 📁 Weekly Audit Log
 - 📁 Custodian
 - 📁 Seal Log (If Applicable)
 - 📁 Receipt/Dispatch (If Applicable)



27

Audit Records - cont'd

- 📁 What logs are required - Automated
 - 📁 if technically capable
- 📁 Successful and unsuccessful logons and logoffs
- 📁 Unsuccessful accesses to security-relevant objects and directories, including:
 - 📁 creation
 - 📁 open
 - 📁 modification and deletion
- 📁 Changes in user authenticators, i.e., passwords
- 📁 Denial of system access resulting from an excessive number of unsuccessful logon attempts.
- 📁 If not technically capable, the Authorized Users list will be retained as an audit record

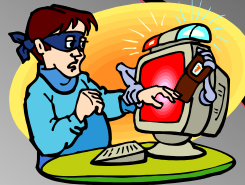


28

Re-Accreditation & Protection Measures

Re-Accreditation

-  Every Three Years
-  Major Changes

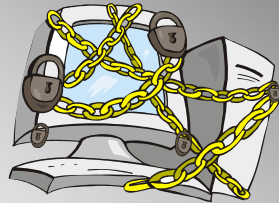


Protection Measures






-  unique Identifier
-  individual User Ids and Authentication
 -  passwords



29



Passwords

-  Minimum 8 Characters
-  Classified to the highest level of the system
-  Changed at least every 365 days
-  Changed when compromised
-  Automated generation when possible



30

DoD Warning Banner

-  **Required**
-  **Positive User Action**
-  **Prominently displayed**

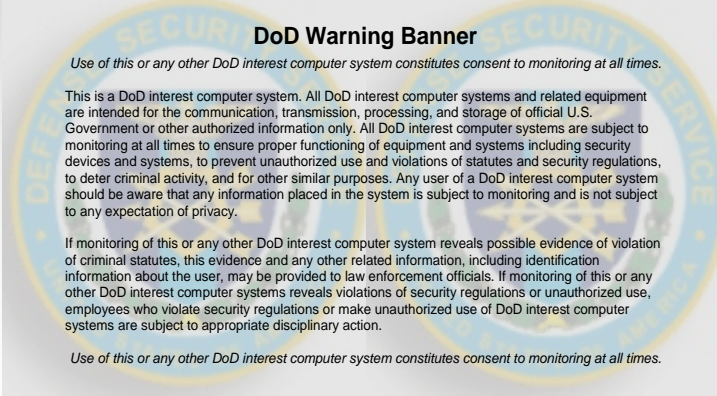
DoD Warning Banner

Use of this or any other DoD interest computer system constitutes consent to monitoring at all times.






This is a DoD interest computer system. All DoD interest computer systems and related equipment are intended for the communication, transmission, processing, and storage of official U.S. Government or other authorized information only. All DoD interest computer systems are subject to monitoring at all times to ensure proper functioning of equipment and systems including security devices and systems, to prevent unauthorized use and violations of statutes and security regulations, to deter criminal activity, and for other similar purposes. Any user of a DoD interest computer system should be aware that any information placed in the system is subject to monitoring and is not subject to any expectation of privacy.

If monitoring of this or any other DoD interest computer system reveals possible evidence of violation of criminal statutes, this evidence and any other related information, including identification information about the user, may be provided to law enforcement officials. If monitoring of this or any other DoD interest computer systems reveals violations of security regulations or unauthorized use, employees who violate security regulations or make unauthorized use of DoD interest computer systems are subject to appropriate disciplinary action.

Use of this or any other DoD interest computer system constitutes consent to monitoring at all times.



Login Attempts

-  **Maximum of 5 attempts**
-  **Lockout after X minutes**
 -  **SSP specific - DSS recommends 30 minutes**
-  **System Administrator resets account or account disabled for X minutes**
 -  **SSP specific - DSS recommends 30 minutes**

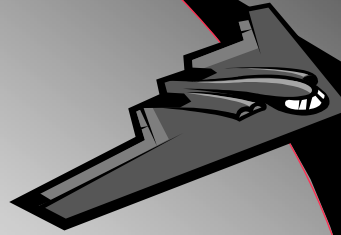


Special Categories

Section 5, Chapter 8

May not meet all NISPOM Requirements

- ☐ **Single-users Stand-alones**
 - ☐ Only one users accesses system
- ☐ **Pure Servers**
 - ☐ No user code on system
- ☐ **Tactical, Embedded Special-Purpose Systems**
 - ☐ Configured as directed by customer



33

Clearing and Sanitization



34

Clearing

Removal of data from an IS, its storage devices and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using normal system capabilities (i.e., keyboard strokes).

DCID 6/3

Sanitization

The process of removing information from media or equipment such that data recovery using any known technique or analysis is prevented, as well as the removal of all classified labels and markings.

DCID 6/3

Clearing and Sanitization Matrix

www.dss.mil

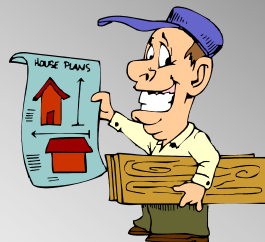
- 🖥️ **Hard drives**
 - 🗑️ May be degaussed or destroyed
- 🖥️ **CPUs**
 - 🗑️ Remove power for one minute
- 🖥️ **Printers**
 - 🗑️ Print one page (font test) then power down



37




Configuration Management Plan

- 🖥️ **Formal change control procedures for security-relevant hardware and software**
- 🖥️ **Management of all documentation**
- 🖥️ **Implement, test and verify CM plan**



38





CM Plan Documents:

-  Procedures to identify and document type, model and brand of IS hardware
-  Procedures to identify and document product names and version or release numbers and location of security relevant software
-  System connectivity

8-311
ISL Q-45

39

Periods Processing

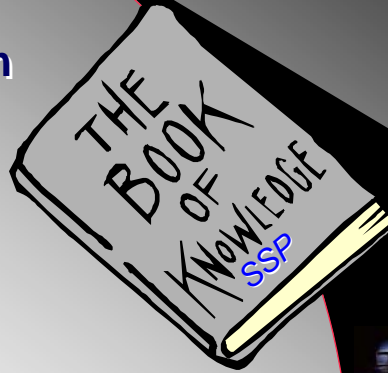
-  Separate Sessions
-  Different Classification Levels
-  Different Need-To-Know
-  Removable Media for each processing session



40

Summary

- 📖 Principals of Computing Security
- 📖 System Security Plan
 - 📖 Purpose
 - 📖 Contents
- 📖 NISPOM = What
- 📖 SSP = How



The End