# DOD INFoS ɛC
# Education, Training, Awareness & Products (ETA&P)

Joan M. Pohly, DISA/IPMO, (703) 681-1346, pohlyj@ncr.disa.mil

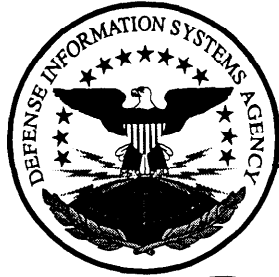April 1998

# Form SF298 Citation Data

| Report Date<br>*("DD MON YYYY")*<br>00041998 | Report Type<br>N/A | Dates Covered (from... to)<br>*("DD MON YYYY")* |
|---|---|---|

| Title and Subtitle<br>DOD INFOSEC Education, Training, Awareness & Products (ETA&P) | Contract or Grant Number |
|---|---|
| | Program Element Number |
| Authors | Project Number |
| | Task Number |
| | Work Unit Number |
| Performing Organization Name(s) and Address(es)<br>DISA | Performing Organization Number(s) |
| Sponsoring/Monitoring Agency Name(s) and Address(es) | Monitoring Agency Acronym |
| | Monitoring Agency Report Number(s) |

| Distribution/Availability Statement<br>Approved for public release, distribution unlimited |
|---|
| Supplementary Notes |
| Abstract |
| Subject Terms |

| Document Classification<br>unclassified | Classification of SF298<br>unclassified |
|---|---|
| Classification of Abstract<br>unclassified | Limitation of Abstract<br>unlimited |
| Number of Pages<br>56 | |

| REPORT DOCUMENTATION PAGE | Form Approved OMB No. 074-0188 |
|---|---|

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

| 1. AGENCY USE ONLY (Leave blank) | 2. REPORT DATE 4/21/98 | 3. REPORT TYPE AND DATES COVERED Briefing |
|---|---|---|

| 4. TITLE AND SUBTITLE DoD INFOSEC Education, Training, Awareness & Products (ETA&P) | 5. FUNDING NUMBERS |
|---|---|
| 6. AUTHOR(S) Joan M. Pohyl, | |

| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) IATAC Information Assurance Technology Analysis Center 3190 Fairview Park Drive Falls Church VA 22042 | 8. PERFORMING ORGANIZATION REPORT NUMBER |
|---|---|

| 9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Technical Information Center DTIC-IA 8725 John J. Kingman Rd, Suite 944 Ft. Belvoir, VA 22060 | 10. SPONSORING / MONITORING AGENCY REPORT NUMBER |
|---|---|

**11. SUPPLEMENTARY NOTES**

| 12a. DISTRIBUTION / AVAILABILITY STATEMENT | 12b. DISTRIBUTION CODE A |
|---|---|

**13. ABSTRACT (Maximum 200 Words)**

This DISA briefing outlines the full set of DoD INFOSEC education, training, awareness and products available to the field. It documents DISA location in the information infrastructure, the DoD missions and functions, the customers, approach, and key working groups and forums. It also identifies the training facility, and the course that are offered by area and by job function. It also describes the current training products and other educational opportunities and schools.

| 14. SUBJECT TERMS INFOSEC training | | | 15. NUMBER OF PAGES |
|---|---|---|---|
| | | | 16. PRICE CODE |

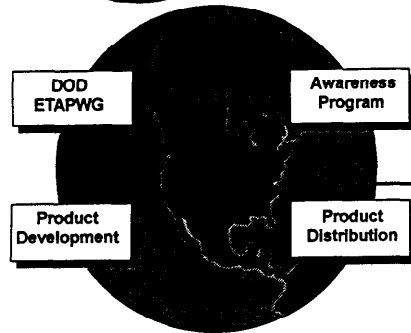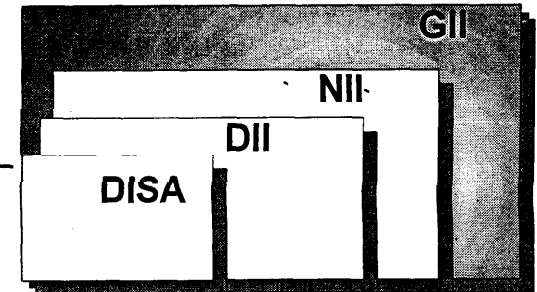| 17. SECURITY CLASSIFICATION OF REPORT Unclassified | 18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED | 19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED | 20. LIMITATION OF ABSTRACT None |
|---|---|---|---|

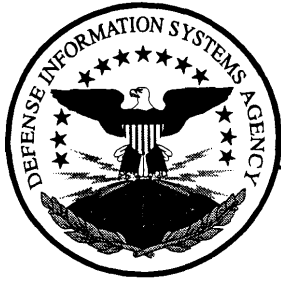# Operations

# Training & Awareness Mission

## DOD Mission & Functions

Vital link in securing the
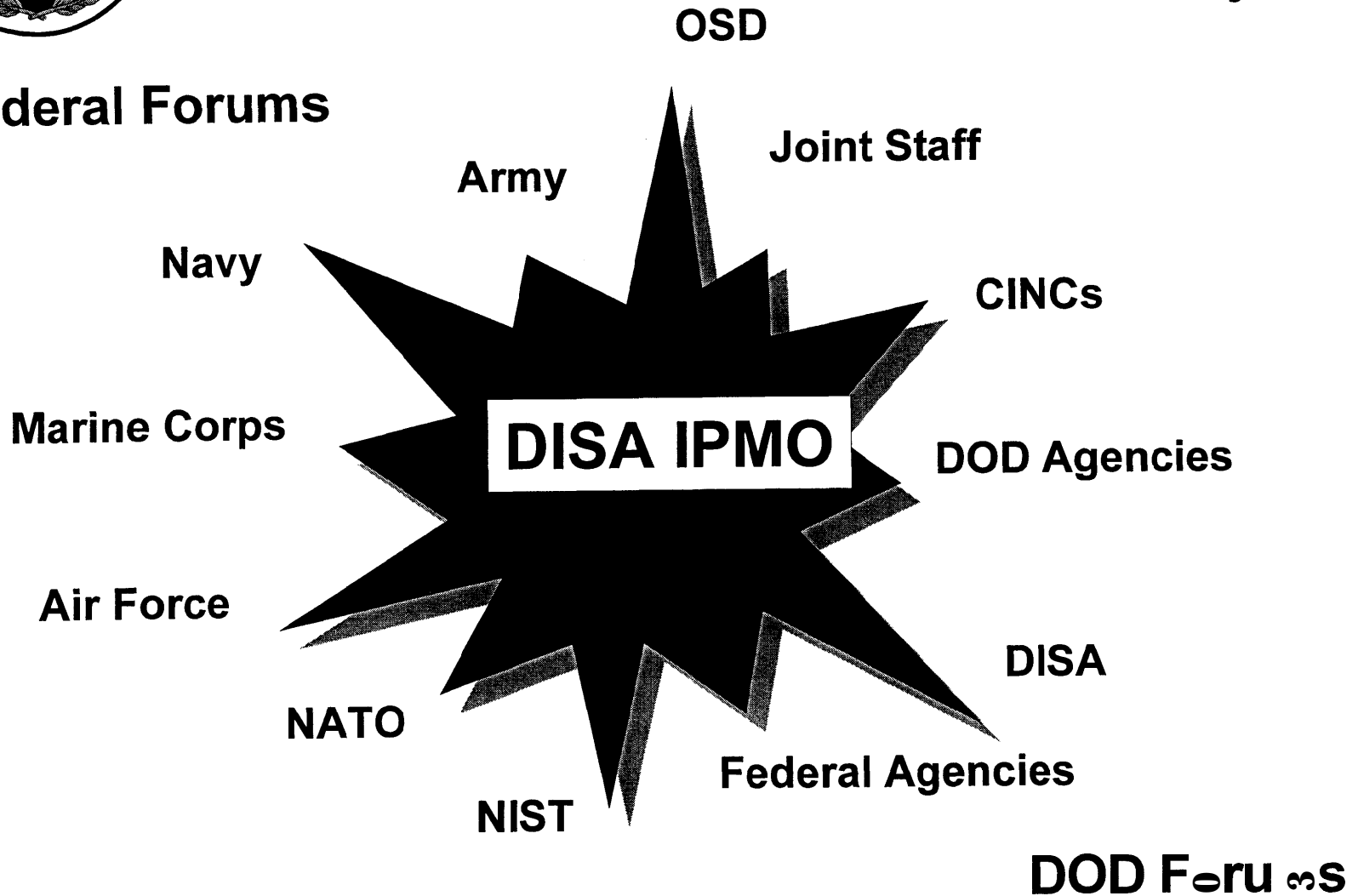information infrastructure

. **Support ASD/C3I**

- **Facilitate development of standardized DOD-wide INFOSEC training**

- **Develop products for use in a comprehensive DOD INFOSEC awareness program**

- **Promote training & awareness products for use DOD-wide**

- **Promote development of curriculum to support an INFOSEC career field/professional program**

- **Influence national-level INFOSEC education, training and awareness**

DOD
ETAPWG

Awareness
Program

Product
Development

Product
Distribution

GII

NII

DII

DISA

C4IFTW

Command
and
Control

Transmission

Messaging

Combat
Support

GCCS   DISN   DMS   GCSS

Technical Architecture Framework for Information Management

Partnerships

Modeling and Simulation

INFOSEC

Building Codes and Permits

Software Tools

Mainline Commercial Products

Engineering

Standard Architecture

Data Elements

Leading Edge Services

OSD

**Federal Forums**

Joint Staff

Army

Navy

CINCs

Marine Corps

**DISA IPMO**

DOD Agencies

Air Force

DISA

NATO

Federal Agencies

NIST

DOD Forums

# Approach

Champion products →
- Resource
- Promote
- Produce

Leverage INFOSEC ETAP forums →
- DOD (DII)
- Federal/National (NII)
- International (GII)

Rely on existing ETAP infrastructure →
- CINCs
- Services
- Agencies
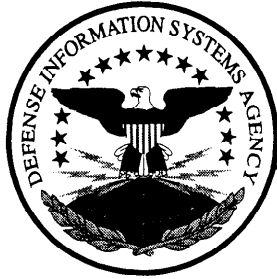
# Key Working Groups & Forums

## Classified Community

- **Security Policy Forum**
    - **Training and Professional Development Committee (TPDC)**
    - **INFOSEC Working Group (ISSWG)** (IPMO chairs)
- **NSTISSC**
    - **INFOSEC Education, Training and Awareness Issue Group**
- **MISSI Life Cycle Logistics Working Group**

## Unclassified Community

- **NIST Computer Security Program Managers Forum**
    - **Federal Information Systems Security Educators Association (FISSEA)**
- **Association of Computing Machinery (ACM)(via NPS)**
- **National Colloquium for INFOSEC Education**
- **Army C2 Protect Training Working Group**

# DOD IA ETAPWG: Overview

## Education, Training, Awareness and Professionalization Working Group

- ETAPWG Charter under ASD/C3I Information Assurance Group (IAG)

- Address IA/INFOSEC ETA issues on behalf of ASD/C3I

- CINC, Service and Agency membership
  - ETA providers
  - ETA program managers
- Purpose is to:
  - Identify gaps in instruction
  - Recommend/develop solutions
  - Determine champions for initiatives
  - Eliminate duplication of effort
  - Standardize what is being taught

| CINCs/JS | Services | Agencies |
|---|---|---|
| USACOM | USA | DeCA |
| PACOM | DISC4 | DFAS |
| DISA PAC | TRADOC | DISA |
| CENTCOM | USN | DIA |
| EUCOM | CNO/N6 | DSS |
| SOUTHCOM | CNET | DLA |
| SOCOM | USAF | NDU |
| SPACECOM | AFCA | NRO |
| STRATCOM | AETC | NSA |
| TRANSCOM | AIA | NCS |
| Joint Staff | AU/Cadre | ISSO |
| J6 | USMC | |
| J7 | C4I | |
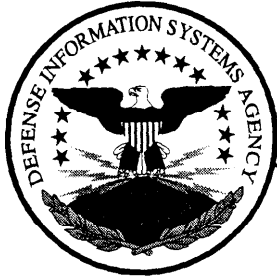
# INFOSEC Training Facility (ITF)

## *DODIAETA@ncr.disa.mil*

- **Provides capability for delivering INFOSEC courseware in NCR**
    - **2 computer classrooms (1 PC; 1PC & UNIX)**

- **Validate content and pilot/evaluate courseware**

- **Supports non-IPMO developed courses**
    - **Operational Computer Security (ND225)(NSA)**
    - **INFOSEC Basics (ISSB)(formerly DODSI)**
    - **DII COE (DISA)**
    - **ARMS (DISA)**

*Skyline (Sky 4)*
*Falls Church VA*

- **Available to DOD and others**
    - **User provides instructor; ITF provides support @ no cost**
    - **Army requesting use as 2nd site for System Admin training**
    - **Navy using for training in NCR**

- **INFOSEC training to DISA/GOSC reservists on weekends**

# ETA Products:
## Current
## and
## On the Horizon

# INFOSEC Post Graduate Education

- Joint IPMO/Navy/Navy Postgraduate School (NPS) initiative

- Goal: Infuse INFOSEC into appropriate curriculums at DOD degree granting institution

- NPS is joint institution: CINCs, Services, Agencies

- NPS lead development w/IPMO
    - Introduction to Computer Security (completed)
    - Management of Security in Information Systems (current)
    - Secure Systems (planned)
    - Network Security (planned)

- NPS taking lead to transfer course materials to DOD and private sector academic institutions
    - ACM (Association for Computing Machinery)
    - Other academic forums
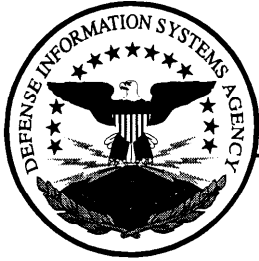
# INFOSEC Courseware

## IPMO sponsored: no cost/low cost

*Computer Based Training (Unclassified, DOS based 286)*

- **DOD CS 100: Introduction to Computer Systems Security**
  - Targets unclassified environment (DOD version of NSA IN-170)
  - 8 hours

*Platform Instruction (ITF or MTT)*

- **INFOSEC 101: INFOSEC for End Users** (1 day)
- **INFOSEC 300: INFOSEC for ISSMs & ISSOs (5** days)
- **INFOSEC 315: DITSCAP (2** days)
- **INFOSEC 310 Windows NT Security for SAs (5** days)

*Training Materials (PowerPoint)*

- **INFOSEC 201: INFOSEC for Managers** (web only)
- **INFOSEC 205: Malicious Logic** (web only)

*Available at no cost via WWW or from DISA/IPMO upon request*

# DOD Information Technology Security Certification & Accreditation Process

*DITSCAP*

- IPMO role
  - Develop DOD level modules; validate DOD-wide
  - Front end for Service/Agency detailed training
- Awareness/literacy level
  - Overview of DITSCAP (.25 day)
    - initial Effort Required
    - Long Term Benefits
  - DITSCAP Task & Step Review (1.75 day)
    - Review DITSCAP process by phase
    - DITSCAP templates & "boilerplate"
    - Identify places to go for additional assistance
- Audience
  - Primary : ISSO, Mid-Management
  - Secondary:
    - Sr Management
    - @Personnel w/ C&A as part of their job
- Delivery
  - Platform (available @ ITF)
  - Train-the-Trainer  (w/Services/agencies)
  - Convert to interactive multimedia CBT (3 QTR FY98)
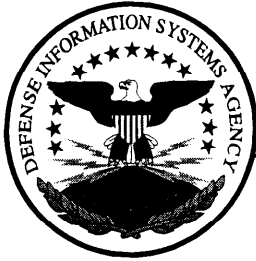
# INFOSEC Courseware

## On the Horizon

- **IPMO: Designated Approving Authority (DAA)**
  - Based on GSA and DODSI materials
  - Updating course; adding practical exercise
  - Prepare classroom course (3rd QTR FY98)
  - Convert to CBT (4th QTR FY98)
- **IPMO: Information Assurance for Auditors and Evaluators (w/ DODIG)**
  - DODIG lead for military IGs
  - DODIG leading coordination to transition to Federal-wide IG audience
  - Pilot held 3-4 March 98 @ ITF
  - .ConverttoCBT(3rdQTRFY98)
- **Defense Acquisition University (DAU):Information Resource Management (IRM) 101**
  - INFOSEC inputs provided to DAU for web based course
  - POC: Norline Depeiza (depeizn@acq.osd.mil)
  - Web site: http://192.239.92.37/IRM101_project_web/welcome.html

# Public Key Infrastructure

- **IPMO role**
  - Develop DOD level modules; validate DOD-wide
  - Front end for Service/Agency detailed training

- **Audience**
  - Users
  - Local Registration Authorities (LRAs)
  - Registration Authorities

- **Initially in conjunction with Defense Travel Service (DTS)**
  - Piggy-back on DTS training strategy

- **Delivery medium**
  - Awareness Video: June 98
  - Platform course: July 98 (pilot)
  - Train the trainer program
  - Convert to interactive multimedia CBT (4 QTR FY98)

| |
|---|
| Refresher/ Reinforcement (On-line Updates) |
| Education (Concepts) |
| *Training* (Doing) |
| *Literacy* (Understanding) |
| *Awareness* (Recognition) |

# Windows NT Security for System Administrators (INFOSEC 310)

- Drawn from Army and Navy Systems Administrator courses
  - Army, 5th SIG CMD: 5 days
  - Navy, CNET, Corry Station: 8 weeks (Multi-platform)

- DISA/IPMO course: Windows NT, 5 days
  - Roles & responsibilities, policies & procedures (.5 days)
  - Operating system security overview (4.5 days)
    - Threats and vulnerabilities
    - Countermeasures
    - Tools/firewall lab planned for future (FY99)

- Schedule: l-2 classes/month for remainder of FY98
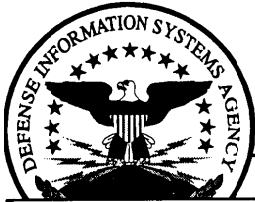
| Function / Courses | Sys Admin | Network Security | ISSO ISSM | TASO | IRM | End User | Mid-Mgr | Sr Mgr | Certifier |
|---|---|---|---|---|---|---|---|---|---|
| Operational Computer Security (ND225)(NSA) | X | X | X | X | X | | X | | X |
| INFOSEC Basics* (ISSB)(DODSI)(IPMO) | X | X | X | X | X | X | X | | X |
| INFOSEC for ISSOs & ISSMs (IPMO)* | X | X | X | | | | | | X |
| INFOSEC for ISSOs (Army) | X | X | X | | | | | | X |
| Fortezza Installer (Army) | X | X (Installer) | | | | | | | |
| INFOSEC Mgmt (AMC 305)(Army) | X | X | X | | | | X | | X |
| ISA (CNET)** | X | X | | | | | | | |
| NS&VT (CNET)** | X | X | | | | | | | |
| DITSCAP (DISA) | X | X | X | | | | X | X | X |
| INFOSEC for End Users (IPMO)* | | | | | | X | X | | |

\* For ITF courses, go to : http://www.disa.mil/ciss/cissitf

\*\* For info on source ratings & prerequisites go to: http:/www.cnet.navy.mil/netpdtc/cantrac/cantrac.htm
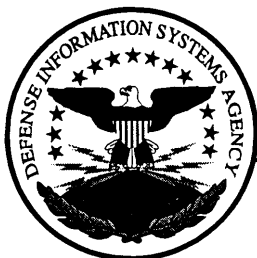
# INFOSEC Courses on the Horizon

| Function / Courses | Sys Admin | Network Security | ISSO ISSM | TASO | IRM | End User | Mid-Mgr | Sr Mgr | Certifier |
|---|---|---|---|---|---|---|---|---|---|
| Sys Admin & Network Security (Army)(2QTR FY98) | X | X | X | | | | | | |
| DAA (GSA/DODSI) (Navy)(IPMO)(4 QTR FY98) | | | X | | X | | X | | X |
| Windows NT Security for Sys Admin (INFOSEC 310) (IPMO) (2 QTR FY98) | X | X | X | | | | | | |
| Advanced Network Analyst (CNET) (4thQtr FY98) | | X | X | | | | | | |
| ISSM (CNET) (Pilot, 2 QTR FY98) | X | X | | | | | | | |
| DITSCAP (DOD) (IPMO)(2 QTR FY98) | X | X | X | | | | x | x | X |
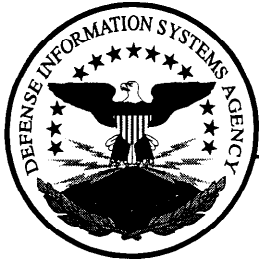
# INFOSEC CBTs & Videos

## IPMO championed/community validated

- **Computer Based Training** *(Unclassified; DOS-based 286)*

  - **ND-170: Introduction to Computer System Security** (NSA)
    - Targets Classified environment (basis for DOD CS-100)
  - **ND-150: Introduction to Information Systems Security** (NSA)
  - **OP-301: OPSEC Fundamentals for Managers and Supervisors** (NSA)

- **Videos** *(VHS, Unclassified)*

  - **Networks at Risk** (NCS) (10 min)
  - **Protect Your AIS** (USGov) (6 vignettes)
  - **The Information Front Line** (IC) (10 min)
  - **Bringing Down the House** (IC) (11 min)
  - **Exploring MISSI** (IPMO w/NSA)( 10 min)
  - **Computer Security 101** (DOJ) (~10 min)
  - **Computer Security: The Executive Role** (DOJ)(~10 min)
  - **Protect Your AIS** (FAA Version)(48 min)
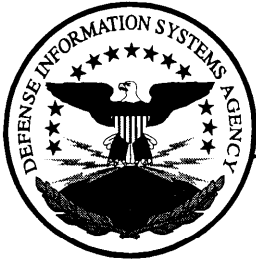
# INFOSEC Multimedia Products

## CD-ROM Format

### Current

- **INFOSEC Awareness** (Unclassified, Windows, 486)
    - **DISA specific/DOD useable**
    - **Fulfills Public Law 100-235 requirements**
- **IW Basics**
- **DOD INFOSEC Awareness**

### On the Horizon

- **Federal INFOSEC Awareness (w/TPDC, NSTISSC ETA Issue Group)**
- **Operational Information Systems Security (OISS)(2 vol)(WC)**

*WC - web connected

# INFOSEC CBTs & Videos
## Current

| CBTs & Videos / Functions | Sys Admin | Network Security | ISSO ISSM | CERT | TASO | IRM | End User | Mid Mgmt | Sr Mgmt |
|---|---|---|---|---|---|---|---|---|---|
| ND-150 Intro to Info Sys Security (NSA) | X | X | X | X | X | X | X | X | |
| ND-170 Intro to Comp. Sys Security (Classified Environment)(NSA) | X | X | X | X | X | X | X | | |
| CS-100 Intro to Comp. Sys Security (Unclassified Environment) (IPMO) | X | X | X | X | X | X | X | | |
| OP-301 OPSEC Fundamentals for Mgrs & Supervisors (NSA) | X | X | X | | | | | | |
| INFOSEC Awareness CD-ROM (IPMO) | | | | | X | X | X | X | X |
| IW Basics (IPMO) | X | X | X | | X | X | X | X | X |
| Networks at Risk (NCS)(10 min) | X | X | X | X | X | X | X | X | X |
| Protect Your AIS (IC)(6 vignettes)(10min) | X | X | X | X | X | X | X | X | |
| The Information Front Line (IW)(IC)(10min) | X | X | X | X | X | X | X | X | X |
| Bringing Down the House (IW)(NSA)(11 min) | X | X | X | X | X | X | X | X | X |
| Exploring MISSI (w/NSA) | X | X | X | | X | X | X | X | |
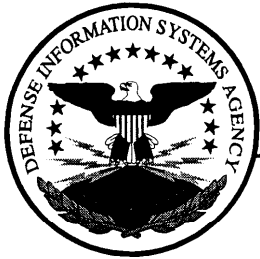
# INFOSEC Awareness Products
## *Training Resources Electronic Catalog (TREC)*

- **Multi-disciplinary: INFOSEC & related disciplines**
  - IW
  - C2W
  - E W
  - PSYSOPS
  - Physical Security
  - Info Assurance
  - Info Protect
  - Info Operations
  - . OPSEC
  - . COMSEC
  - . COMPUSEC
  - . TEMPEST

- **Centralized source of security ETA "products"**
  - Government owned/sponsored
  - Courses, CBTs, Training aids, Posters

- **Shared responsibility:**
  - IPMO manages configuration/dissemination
  - Providers/developers "own" their data; provide updates

- **Cooperative effort w/CINCs/Services/Agencies & Federal Depts & Agencies**
  - Promoted at national level as Federal solution
  - Interim version (Access) available via DISA v web site

- **Transitioning to Web based product ( 2nd QTR FY98)**
  - Search and sort capabilities using browser
  - Hot links to provider web sites for registration
  - Provider update on web

# TREC Homepage

**Results**

N

# INFOSEC Awareness Products

**DISSPatch ◆**
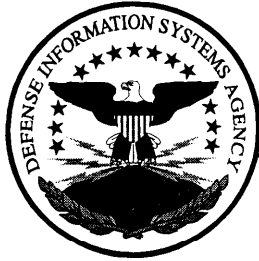
- **DOD's INFOSEC newsletter**
- **Unclassified**
- **Availability**
  - **ASSIST BBS**
  - **Web sites (DISA, NSA/SIPRNET)**
  - **Paper copies (8000+ issues distributed)**
- **DOD & Federal wide**
- **Content**
  - **Focus article**
  - **Resources (products & courses)**
  - **Events (conferences/symposia)**
  - **Where to get more information**
  - **Service /Product POCs**

# Training Delivery
## to the
## Desktop

# Developing Interactive Multimedia Training & Awareness Products

*Systematic approach to efficiently provide high quality ETA products at reasonable cost*

- Apply National Institute for Standards and Technology (NIST) ETA levels
- Map course content; identify applicability to each level
- Build modular; -- "plug & play"
- Focus on delivery to the desktop
  - Computer-based training (CBT)
  - Network-based, Web-updateable (Connected CD-ROM)

- Integrate CBT with classroom instruction; payoff in
  - Reduced time in class, or
  - Additional topics covered/hands on provided, and
  - Post - refresher/reinforcement

- Ensure all courseware is
  - Free of copyright restriction
  - Government owned
  - Available at no cost to DOD

Refresher/
Reinforcement
(On-line Updates)

Education
(Concepts)

Training
(Doing)

----------------

Literacy
(Understanding)

Awareness
(Recognition)
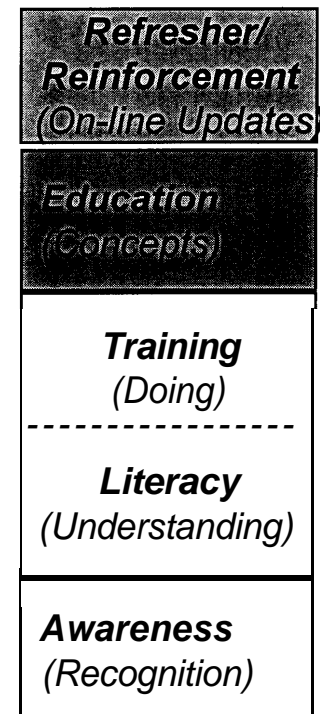
# Training Delivery to the Desktop

## *"Connected" CD-ROM*

- Full interactive, multimedia functionality on CD-ROM

- Run on network (intranet) or individual workstations w/CD-ROM readers

- Linked to web site for updates to training content (text files)

- Numerous features:
  - Metrics collection
  - Testing
  - Book marking
  - "Closed caption"

# Training Delivery to the Desktop

## *Advantages/Disadvantages*

### *Advantages*

- Standard course content and delivery
- Reduce time in classroom OR Reallocate time in classroom to
    - Add new topics
    - Increase hands on portion
- Use web-site to provide updates to training content
- Reduce need to conduct refresher training in classroom setting
- Lower cost

### *Disadvantages*

- No direct, immediate interaction with instructor....but can
    - Reduce need by using prerequisites to bring students to desired level
    - Web based "Ask the Professor"
- Identity of student taking the course...
    - No different than correspondence course
    - Use existing infrastructure
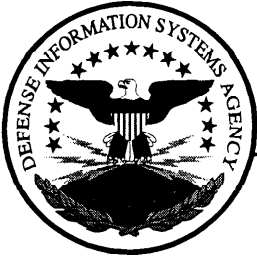
# Developing Interactive Multimedia Training & Awareness Products

## Deliverable to the desktop-- via CD-ROM reader or network... & web updateable

### *Example: INFOSEC Awareness CD-ROM*

| Cost | CD-ROM | Notes |
|------|--------|-------|
| Cost to develop CD-ROM master | $35,000.00 | |
| Number  disseminated | 8647 | Number does not include DISA personnel who have accessed the presentation via the DISANET |
| Cost to produce 8647 CD-ROMs @ $1.85  each | $16,000.00 | Actual cost after the first 3500 is $1.58 each |
| Total cost to develop & produce | $51,000.00 | |
| Cost per student | $5.90 | |

# DOD INFOSEC Awareness

## Course Content Map

INFOSEC Tech Asst.
Your ISSO/ISSM
INFOSEC Training
INFOSEC Awareness
Products

**Main Menu**

Glossary

Where to Find Help

Exit

**Why Information Systems Security**

**External Threat**

**How INFOSEC Evolved**

**Malicious Logic**

**Your Roles and Responsibilities**

Recent News

Definition of INFOSEC

Public Law

Policy

- OMB Circular
- DOD Directive
- ITRM

The Intruder

Intruder Techniques

Intruders Observed

DOD Functions Affected

INFOSEC in INFOWAR

Definition of INFOWAR

Evolution
- 1960
- 1970
- 1980
- Present

Global Connectivity

- Pentagon
- Capitol
- Rome Labs

What is Malicious Logic
- Trojan Horses
- Bombs
- Worms
- Viruses

How does it spread?

Virus Growth

Common Myths

Types of Information
- SABI
- ED1
- EC
- Classified
- Unclassified

Passwords

Encryption
- PKI
- DES

Files Backup & Storage

*When user criteria are finalized a course test will be included.

Enclosure 2

# INFOWAR Basics
## Course Content Map

**Glossary**　　**POCs**　　**Exit**

| Definitions |
| --- |

| Basic Principles |
| --- |

| You Are A Critical Link |
| --- |

| The Information Age |
| --- |

| Electronic Revolution (Technology Explosion, Information Vulnerabilities) |
| --- |

| Global Connectivity |
| --- |

| Revolution in Military Affairs (The Old Situation, The New Situation) |
| --- |

| An Actual Incident (Rome Labs) |
| --- |

| Components of INFOWAR |
| --- |

| The Value of Integration |
| --- |

| Information Superiority |
| --- |

- Deception
- Information Attack
- Psyop
- Destruction (Lethal, Non-Lethal)
- Info Ops
- Electronic Warfare (Jamming)
- Security Measures
  - Computer (Hanover Hacker)
  - Communications
  - Physical
  - Information
  - Emanations
  - Operations (Pizza Storm)

| DOD's Responsibility |
| --- |

| Command Responsibility |
| --- |

| Your Role |
| --- |

27 March 1998

# Federal INFOSEC Awareness

## Course Content Map

**Main Menu**

**Glossary**

**Exit**

**Why Information Systems Security**

**Threat**

**How INFOSEC Evolved**

**Malicious Logic**

**Your Roles and Responsibilitie**
s

**Recent News**

**Definition of INFOSEC**

**Public Law**

**Policy**

OMB Circular
Other Dept/Agency

**The Intruder**

**Intruder Techniques**

**Intruders Observed**

**Information Assurance in INFOSEC**

**Definition of Information Assurance**

**Evolution**
· 1960
· 1970
· 1980
· Present

**Global Connectivity**

· Croatian Students
· Rome Labs
· Whitehouse Messaging

**What is Malicious Logic**
- Trojan Horses
-Bombs
-worms
- Viruses

**How does it spread?**

**Virus Growth**

**Mis-conceptions**

**Types of Information**
- Classified
- Unclassified

**New Dev**
-EC
- SABI

**Passwords**

**Encryption**
- Public Key
- Private Key

**Files Backup & Storage**

*When user criteria are finalized a course test will be included.

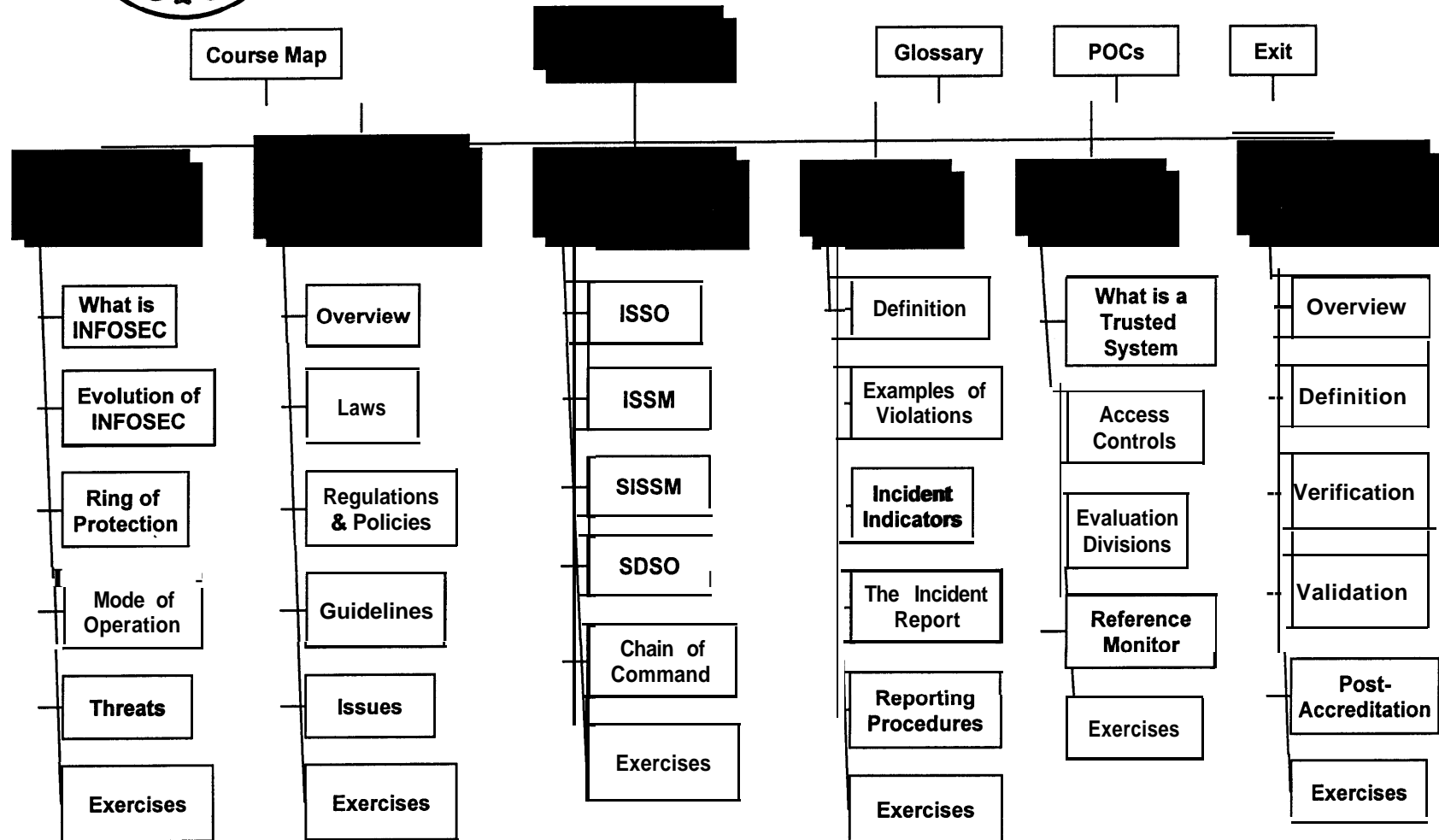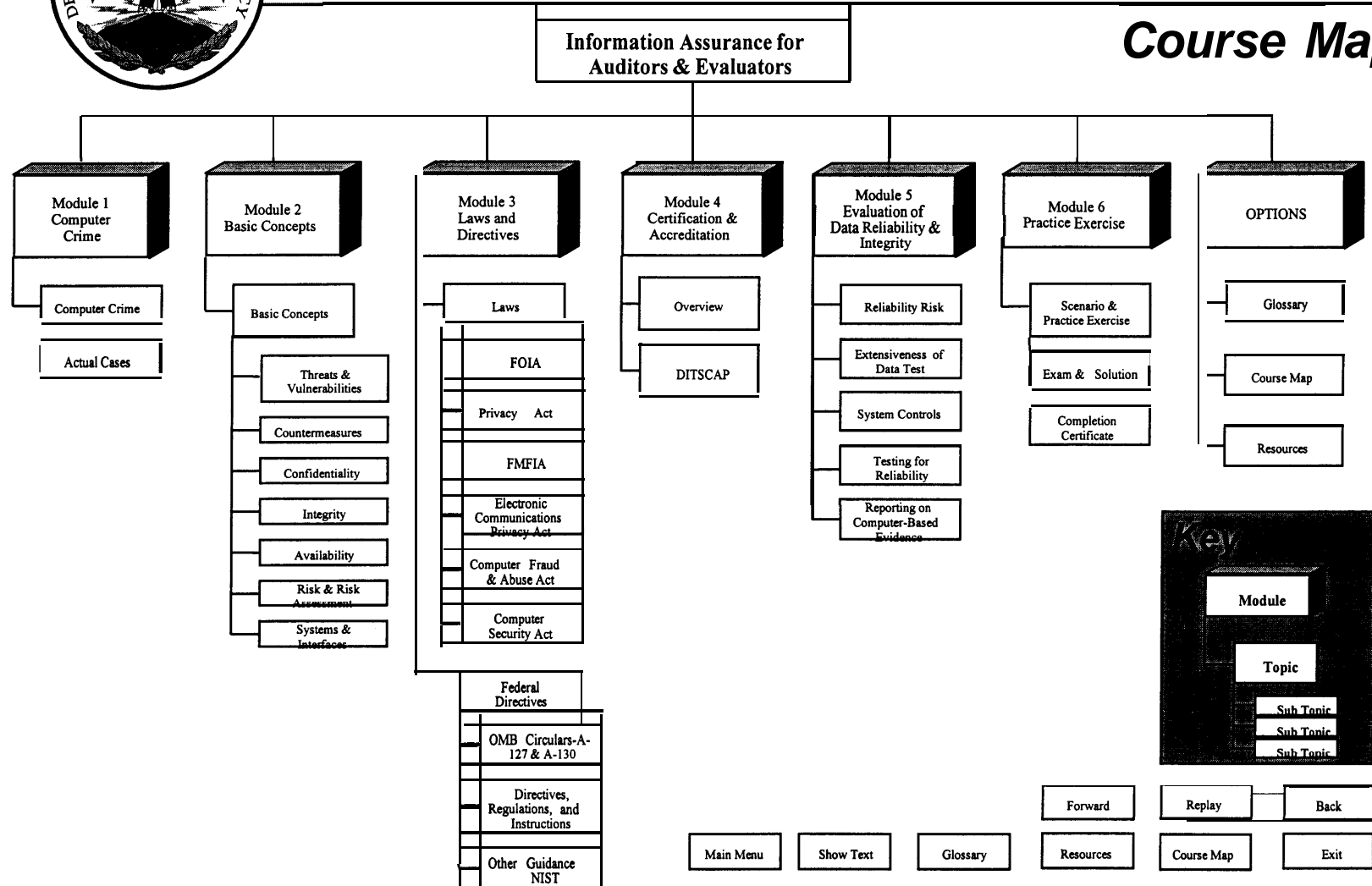# Operational Information Systems Security (OISS), Vol.1
## Course Content Map

**Course Map** | **Glossary** | **POCs** | **Exit**

| | | | | | |
|---|---|---|---|---|---|
| What is INFOSEC | Overview | ISSO | Definition | What is a Trusted System | Overview |
| Evolution of INFOSEC | Laws | ISSM | Examples of Violations | Access Controls | Definition |
| Ring of Protection | Regulations & Policies | SISSM | Incident Indicators | Evaluation Divisions | Verification |
| Mode of Operation | Guidelines | SDSO | The Incident Report | Reference Monitor | Validation |
| Threats | Issues | Chain of Command | Reporting Procedures | Exercises | Post-Accreditation |
| Exercises | Exercises | Exercises | Exercises | | Exercises |

27 March 1998

# Operational Information Systems Security (OISS), Vol.2
## Course Content Map

- Workstation Basics
- General Security
- Windows NT
- UNIX

- Network Basics
- Common Vulnerabilities
- Examples of Violations
- Security Services
- Security Devices

- Types and Handling
- Managing Media

- What is Encryption
- Key-based Systems
- Security Services

- What is Malicious Code
- Spread of Malicious Code
- Viruses
- Detecting and Preventing

- Why Risk Management
- Risk Management Cycle

- Why Audit
- Auditing Goals
- Audit Trail

27 March 1998

# IA for Auditors and Evaluators

## Information Assurance for Auditors & Evaluators

## Course Map

### Module 1 Computer Crime
- Computer Crime
- Actual Cases

### Module 2 Basic Concepts
- Basic Concepts
  - Threats & Vulnerabilities
  - Countermeasures
  - Confidentiality
  - Integrity
  - Availability
  - Risk & Risk Assessment
  - Systems & Interfaces

### Module 3 Laws and Directives
- Laws
  - FOIA
  - Privacy Act
  - FMFIA
  - Electronic Communications Privacy Act
  - Computer Fraud & Abuse Act
  - Computer Security Act
- Federal Directives
  - OMB Circulars-A-127 & A-130
  - Directives, Regulations, and Instructions
  - Other Guidance NIST

### Module 4 Certification & Accreditation
- Overview
- DITSCAP

### Module 5 Evaluation of Data Reliability & Integrity
- Reliability Risk
- Extensiveness of Data Test
- System Controls
- Testing for Reliability
- Reporting on Computer-Based Evidence

### Module 6 Practice Exercise
- Scenario & Practice Exercise
- Exam & Solution
- Completion Certificate

### OPTIONS
- Glossary
- Course Map
- Resources

Key

Module

Topic

Sub Topic
Sub Topic
Sub Topic

| Forward | Replay | Back |

| Main Menu | Show Text | Glossary | Resources | Course Map | Exit |

The first time through Module 5, the Topics are run in sequence as shown.
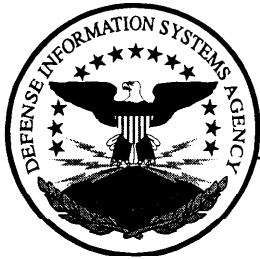Upon completion, the user may access the topics in any order.
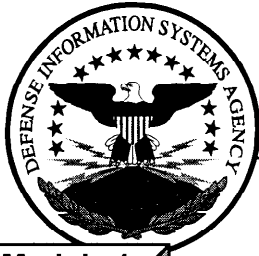
*Windows 3. 1 version*
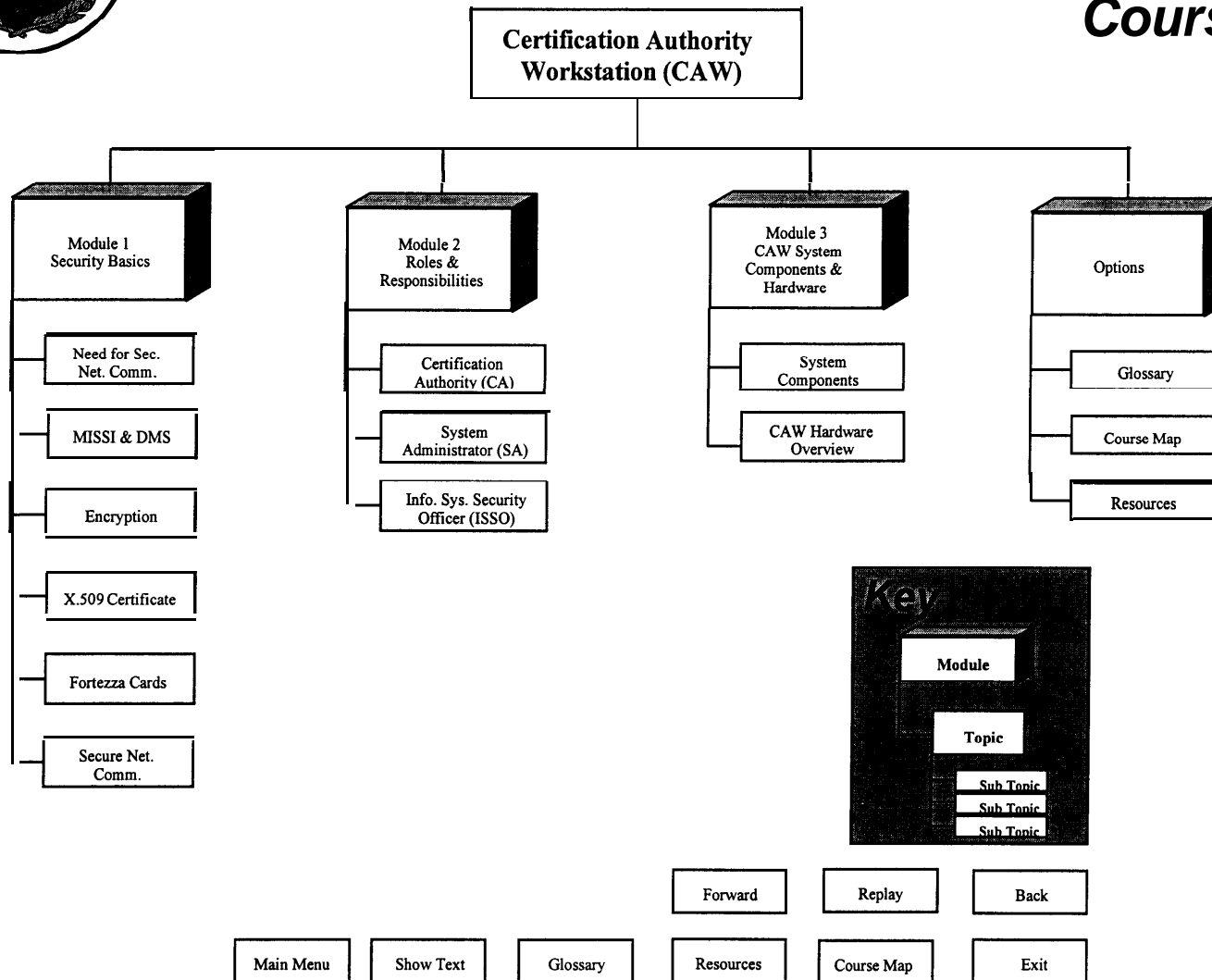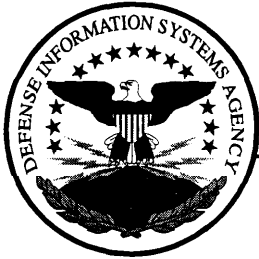
# FORTEZZA Installers Course

*Course Content Map*

**Module 1**

**Introduction**

- **Module Descriptions TLO-1**
  - Introduction
  - PC Card Technology
  - Core Concepts and Applications
  - Diagnostics and Troubleshooting
  - Help
- **MISSI Concepts TLO-2**

**Module 2**

**PC Card Technology**

- **Concepts of PC Card Technology TLO-3**
  - PC Cards, Sockets, & Hosts
  - Mech/Elec Aspects & Software
  - PC Card Use & Compatibility
- **Installation of PC Card Readers and Drivers TLO-4**
  - Greystone
  - Curtis Cardshark
  - Phoenix (Carry PCD-VA-220)
  - External Laptop

**Module 3**

**Core Concepts & Applications**

- **FORTEZZA Basic Concepts TLO-5**
  - Security Algorithms
  - Security Services
  - Certificates
  - Encryption
- **Installation of FORTEZZA Applications TLO-6**
  - PC MAXI Mail
  - MS Armor Mail
  - AT&T Secret Agent

**Module 4**

**Diagnostics & Troubleshooting**

- **Problem Resolution TLO-7**
  - PE 1
  - PE 2
  - PE 3
  - PE 4
  - PE 5
  - PE 6
  - PE 7
  - PE 8
  - PE 9

**Options**

- Glossary
- Acronyms
- References
- Course Map
- Navigation
- Internet Links
- Note Pad

**Key**

Module

Lesson *

Topic **

Topic

Topic

Topic

[ * ] These lessons are to be taken sequentially

[ ** ] These topics are to be taken sequentially

# Certificate Authority Workstation (CAW)

## Course Map

**Certification Authority Workstation (CAW)**

**Module 1**
Security Basics

- Need for Sec. Net. Comm.
- MISSI & DMS
- Encryption
- X.509 Certificate
- Fortezza Cards
- Secure Net. Comm.

**Module 2**
Roles & Responsibilities

- Certification Authority (CA)
- System Administrator (SA)
- Info. Sys. Security Officer (ISSO)

**Module 3**
CAW System Components & Hardware

- System Components
- CAW Hardware Overview

**Options**

- Glossary
- Course Map
- Resources

**Key**

Module

Topic

Sub Topic
Sub Topic
Sub Topic

| Forward | Replay | Back |

| Main Menu | Show Text | Glossary | Resources | Course Map | Exit |

# Information Assurance Support Environment (IASE)

# Information Assurance Support Environment (IASE)

## ASD/C3I directed; for use DOD-wide

- **Web-based DOD Help Environment for INFOSEC/ Information Assurance professionals**

- **Functional Areas**
  - **ETA**
  - **SABI/MLS**
  - **DITSCAP**
  - **Policy**
  - **C&A/ST&E**
  - **ITSC Contract**
  - **Tools**

ASSIST    Tools

Education, Training, & Awareness

SABI    MLS

DITSCAP

CAP

# IASE Features

- **Person to receive request/provide information requested**
- **Request for Information Ticket System**
- **Frequently Asked Questions (FAQ)**
- **Solutions Database**
- **Chat/Discussion Rooms**
- **Whiteboard**
- **Mail List**
  - **Subscriptions**
  - **By Topic**
- **Bulletin Board System**
- **"Search our Site"**

ASSIST   Tools

Education, Training, & Awareness

SABI   MLS

DITSCAP

CAP
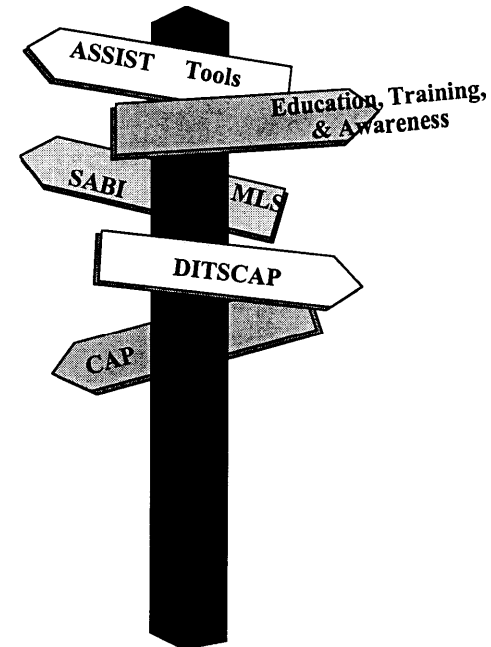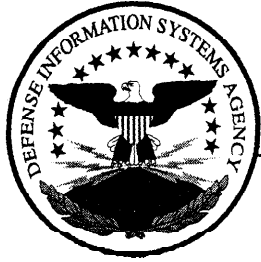
- **Unclassified Site:**
  - **NIPRNet: .mil and .gov accounts required**
  - URL: *http://mattche.iiie.disa.mil/*
  - **Information Desk Unclassified E-Mail:** *IASE@ncr.disa.mil*
  - **IP Address:** *199.208.247.11*
- **Classified Site:**
  - **SIPRNet accounts required**
  - U RL: *http://cassie.iiie.disa.smil.mil*
  - **Information Desk Classified (SIPRNet) E-Mail:** *iase@iiie.disa.smil.mil*
- **Hours of Operation:**
  - **Information Desk: M-F, 8-5**
  - **IASE Web Site: 24 x 7**
- **Telephone: 703-681-IASE**

# SA & User Licensing
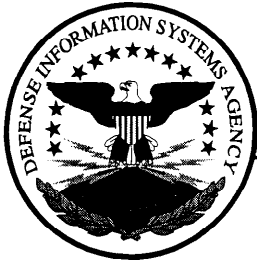
- ◆ **Series of high-level reports and assessments highlighting need for "professionalization" of military, civilian and contractor personnel performing systems administration functions**
    - ◆ **DSB Report, Nov 96, Finding #10**
    - ◆ **GAO Report, May 96**

- ● **Recent events demonstrate need for skilled system administrators to maintain configurations**
    - ◆ **Eligible Receiver '97**

- ◆ **Requirement for DOD SA Licensing Program briefed to MCEB Sep 97**
    - ◆ **SIPRNet SA licensing to be completed NLT Jan 99**

- **Information Systems Security Officers/ Information System Security Managers**
- **Network Managers**
- **Certifiers**
- **Incident Response Teams**
- **Data Base Administrators**
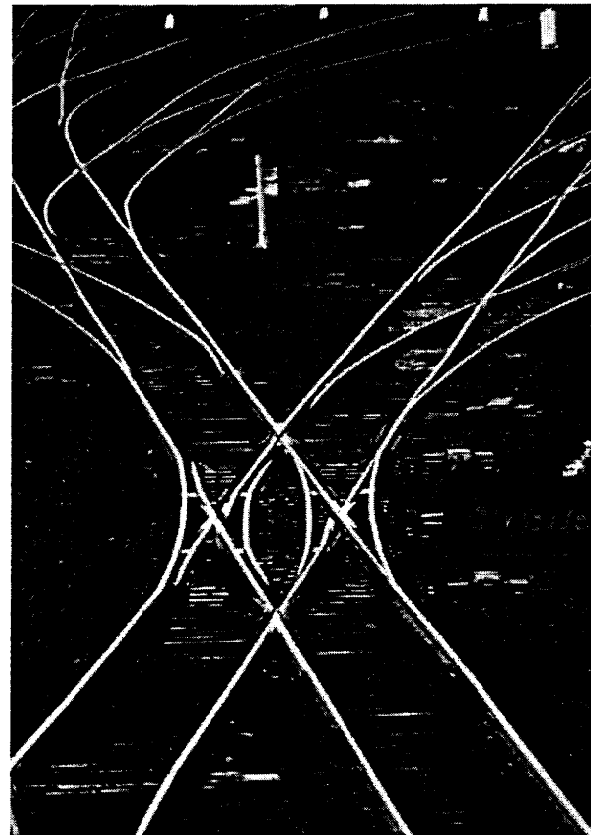
- **Action Officers**
- **Crisis Managers**
- **Data Automation Authorities**

"Other System Professionals"

"Other Users"

4

# DOD Notional Sys Admin Criteria (Government System-OSD)

**Sustainment**

## Operating System

Microsoft Windows NT certificate
20 working days
$6,000

**Sustainment**

## Security Features

INFOSEC for System Administrators (Windows NT)
10 working days
TDY costs

## Environment

OSD System Operations (OJT)(local implementation)
10 working days
Time vs $
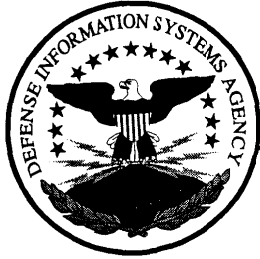
**Sustainment**

## Operating System

UNIX System Administrator
15 working days
$3,800

**Sustainment**

## Security Features

INFOSEC for System
Administrators (UNIX)
10 working days
TDY costs

## Environment

GCCS System Operations
(OJT)(local implementation)
10 working days
Time vs $
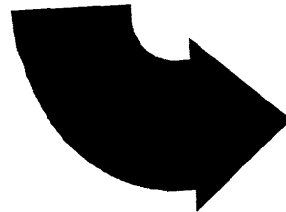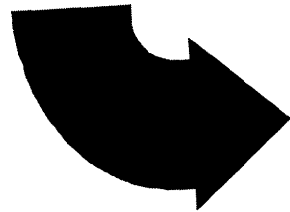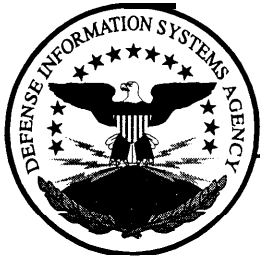
# System Administrator Licensing
## DISA Approach

**Level 3** • Level 2 licensing, AND
- Knowledge of multiple OS
- 5+ years experience

**Level 2** • Level 1 licensing, **AND**
- INFOSEC 310 ( Windows NT Security for System Administrators), **OR** Equivalent (for specific operating system)
- 3+ years experience

*Level 3*

*Level 2*

*Level 1*

**Level 1** • OS knowledge (commercial)
- 0-3 year experience
  **And ONE of the following**
- INFOSEC Basics (CBT) and OISS (Operational Information System Security) (Vol 1&2) (CBT), OR one of the following classroom courses
- INFOSEC 300 (INFOSEC for ISSOs/ISSMs) (Classroom) OR
- ND-225 (Operational Computer Security) (Classroom) OR
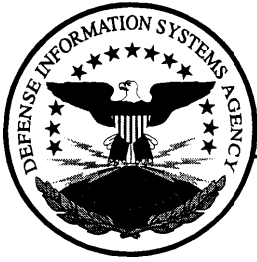- ISSB (Information System Security Basics) (Classroom), OR
- Equivalent course
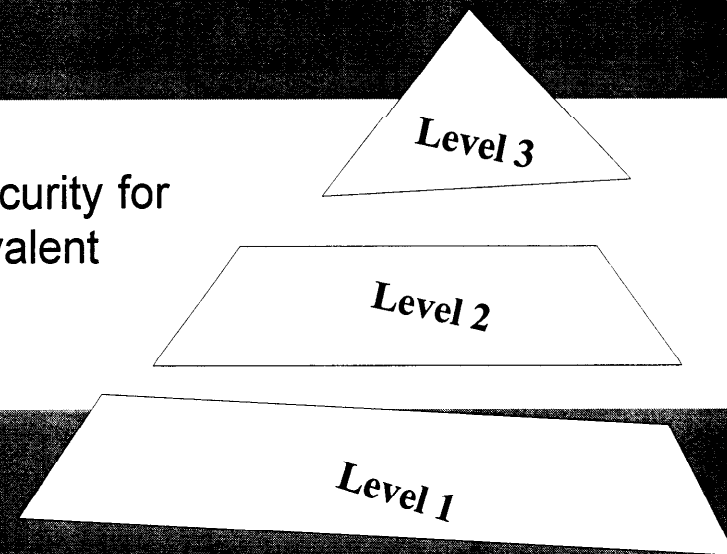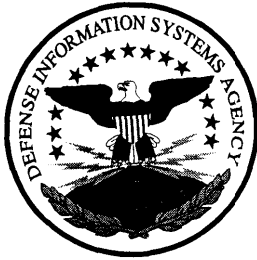
- Issue password AFTER successful completion of initial awareness indoctrination

- Vehicles for user licensing
  - DISA INFOSEC Awareness CBT
  - DOD INFOSEC Awareness CBT
  - Equivalent

# MISSI

# IPMO MISSI ETA Strategy

## FORTEZZA & CAW

- **Apply general strategy**
  - Champion products
  - Leverage existing forums
  - Rely on existing infrastructure

- **Leverage *MISSI Life Cycle Support Working Group***

- **Transition to Government "owned" courses w/delivery by existing training infrastructure**

- **Develop CBT products to minimize time in classroom**

- **Service/Agency**
  - Deliver training via existing infrastructure
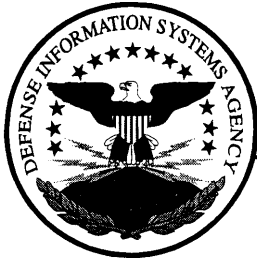
# FORTEZZA Installers Course
## *FORTEZZA for Win 3.1*

- **Platform (3 days): Focus on applications & trouble shooting**

- **Computer-based Training (CBT) (9 hours)**
    - **Covers entire course**
    - **Documentation**
    - **Practical Exercises**
    - **Web-sites for more information**

- **MISSI Familiarization Video *(Exploring MISSI)*(10min)**
    - **Standalone**
    - **Insert in all System Admin training courses**

- **Tobyhanna Army Depot: DOD Trainer for FORTEZZA Installers Course**
    - **DISA provided exportable package; NSA provided equipment**
    - **NSA to ensure "hot line" for training technical assistance (I-800-GO MISSI)**
    - **Cost per course @ Tobyhanna (up to 15 students): ~$4,500**
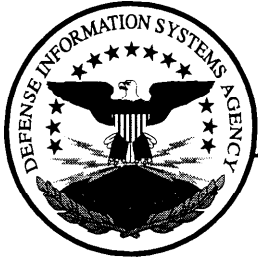
# Approach to CAW Training

- Start with NSA developed course materials
    - CAW 4.2; platform course
    - Identify portions suitable for transitioning to CBT/video

- Develop associated "connected" CBT
    - Full interactive/multimedia functionality on CD-ROM
    - Run on network or individual workstations with CD-ROM readers
    - Linked to web site for training updates

- Use
    - Reduce time in classroom
    - Reference
    - Refresher

# Summary

# On the Horizon

## Completed/nearing completion

| Products | 1QTR FY98 | 2QTR FY98 | 3QTR FY98 | 4QTR FY98 |
|---|---|---|---|---|
| Fortezza Installer for Windows 3.1 | △ ▲ | | | |
| Exploring MISSI (video) | △ ▲ | | | |
| DOD INFOSEC (CD-ROM) | △ △ ▲ | | | |
| Federal INFOSEC (CD-ROM) | | △ ▲ | | |
| DITSCAP (Platform) | △ ▲ | | | |
| DITSCAP (CD-ROM) | △ ▲ | | | |
| IW Glossary (Web-based) | △ ▲ | | | |
| CBT Style Guide (Web-based) | △ ▲ | | | |
| TREC (Web-based) | △ ▲ | | | |
| Sys Admin: Security Basics for Windows | △ ▲ | | | |
| Sys Admin: Operational Information Systems Security (CD-ROM) | ▲ ▲ (Vol1 Vol2) | | | |

## Underway

- FORTEZZA Installer for Windows NT
- CAW (4.2)
- SABI Awareness
- Information Operations Awareness
- IW Attack-Defend Desktop Exercise
- Web Site Security
- Designated Approving Authority (DAA)
- INFOSEC Basics
- Certification/Licensing Review Course
- Incident Handling Procedures
- Certifier Course
- PKI
- INFOSEC for System Administrators
- Secure Systems (NPS)
- Network Security (NPS)
- ETA Requirements Database
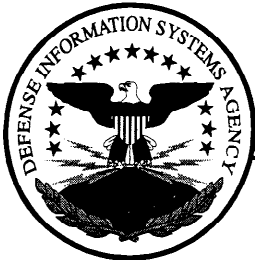
# DOD INFOSEC ETA&P POCs

- **Marjorie York**
  - **703-681-I 323**
  - **yorkm@ncr.disa.mil**

- **George Bieber**
  - **703-681-I 324**
  - **bieberg@ncr.disa.mil**

- **Joan Pohly**
  - 703-681-I 346
  - pohlyj@ncr.disa.mil

- **For Products**
  - 703-681-7944/1344
  - Fax: 703-681-I 386
  - DSN: 761-xxxx
  - cissa@ncr.disa.mil

| DOD ETAPWG | Awareness Program |
| Product Development | Product Distribution |