Center for Development of Security Excellence

CDSE

Learn. Perform. Protect.

Security Education and Training Requirements

1

Information Security Webinar

CDSE

Security Education Requirements

Host: Lisa Rainey, SAPPC

Information Security Curriculum Manager, DSS - CDSE

- Distinguished career-security professional
- Security Asset Protection Professional Certification (SAPPC)
- Retired US Army
- Security Manager/Antiterrorism Officer
- Physical Security Program management
- Personnel Security Program management
- Mobilization/Readiness management
- OPSEC Officer
- Contracting Officers Representative

Administrative Announcements

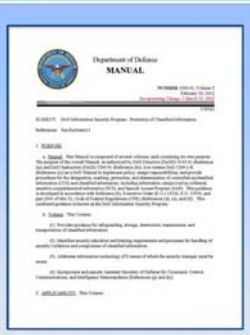
CDSE

- **Use the Q & A box to ask questions.**
- **These slides can be downloaded. Select the file in the File Share box below.**
- **Enclosure 5 of Volume 3 DoD Manual 5200.01 is also provided in the File Share box.**
- **This webinar will present poll questions.**

3

Poll 1

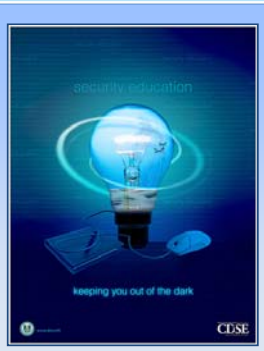
DoDM 5200.01, Vol. 3, Encl. 5


Department of Defense
MANUAL

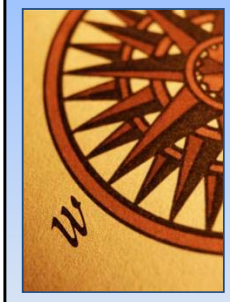
Personnel receive security education and training that:

- Provides necessary knowledge and information
- Promotes understanding, awareness, and motivation

Security Education and Training Resources



Initial Orientation



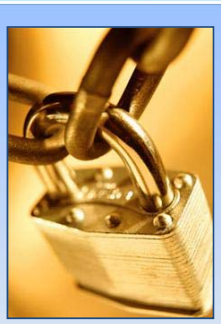
Intended to:

- Define classified information and CUI
- Understand policies and principles
- Know your responsibilities and sanctions
- Provide proper protection
- Review of *all* unclassified information before release

Initial Orientation

Include:

- Names of senior agency official and activity security management personnel
- Their responsibilities
- If involved in protecting classified or CUI



8

Initial Access Training

- Policies and principles
- Derivative classification practices, to include:
  - Classification levels
  - Damage criteria
  - Conditions and restrictions
  - Proper response when questioned about open sources

Poll 2

Initial Access: Safeguarding Training

- Methods and procedures for using, storing, reproducing, transmitting, disseminating, and destroying classified information
- Protection if emergency evacuation
- Procedures for improperly protected information

11

Poll 3

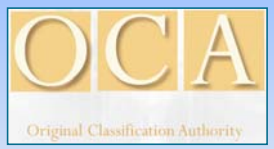
Initial Access: Security Classification Guides

- Guidance for program, system, operation or weapon system elements
- Classification levels, reasons, duration of classification
- Other special guidance

13

Initial Access: Security Classification Guides

- Must be approved and signed by an OCA
- Used as the authoritative source for derivative classification
- Ensures classification consistency for same types of information



14

Obtaining Classification Guidance

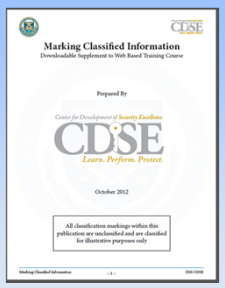
1. Security manager and/or program or project office
2. Defense Technical Information Center at www.dtic.mil
3. Higher headquarters office

15

Initial Access: Marking

- Applying authorized markings
- Levels, duration, and sources of classification
- Observing and respecting OCA decisions
- Maintaining lists of sources

DOD Manual 5200.01, Vol. 2



16

Initial Access: Marking

- Control markings
- Challenging classification decisions
- Downgrading or declassifying
- Marking and sharing "working papers"

17

Initial Access: Security Incident Training

- Security incidents, violations, and compromises
- Disseminating classified information

18

Poll 4

Initial Access: Information Assurance Training

- Use of information systems
- Procedures for marking, handling, storage, transportation, and destruction
- Using removable storage
- Unauthorized disclosure

20

Chat Question

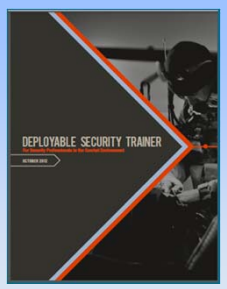
Can you identify some situations that may require special training requirements?

Enter your responses in the chat box.

21

Special Training Requirements

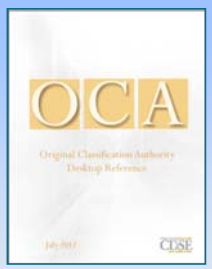
1. Foreign travel or association
2. Escort, hand-carry, or courier
3. Special control or safeguarding
4. International or acquisition programs
5. FGI, coalition or bilateral environments



OCA Training

- OCA Training documented
- Training required for personnel preparing recommendations
- Training must address
  - Responsibilities
  - Classification principles
  - Safeguarding
  - Criminal, civil, and administrative sanctions

DOD Manual 5200.01, Vol. 3, Encl. 5, Sec. 5



23

Declassification Authority Training

- Declassifying information
- Declassification guides
- Component declassification plan
- Declassification database
- Referral process

DoD Manual 5200.01, Vol. 3, Encl. 5, Sec. 6

24

Annual Refresher Training

- Reinforces the 3 "p's"
- Foreign Intel threats & techniques
- Espionage/Unauthorized disclosure
- Changes in security policy
- Self-inspection concern

25

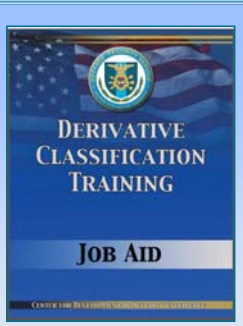
Annual Refresher Training

OCAs:
- Training required annually

Derivative Classifiers:
- Training every two years

Declassification Authorities:
- Training every two years

Be sure to track training you've conducted!



26

Continuing Security Education and Training

READ & INITIAL

- I have read and understand the material presented to me in this briefing. I will abide by the DoD Security Policy and the NISPOM as applicable. I understand that if I commit a Security violation, I will be held responsible and subject to sanctions.

- Print name:____John Dough_____
- Signature:_____*John Dough*_____
- Date:_____Today_____

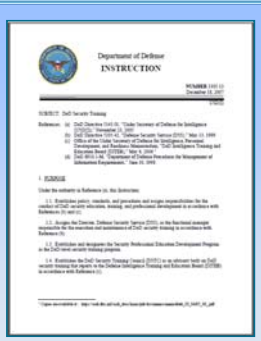
27

Termination Briefings

- Emphasizes continued responsibility
- Reporting instructions
- Retention of classified/CUI
- Public release review
- Reinforces civil and criminal penalties

28

Management and Oversight Training


Department of Defense
INSTRUCTION

- Original and derivative classification
- Classification/Control markings
- Downgrading and declassifying
- Safeguarding
- SCG's and declassification guides
- Access Control
- Incident Reporting
- Requirements for creating, maintaining, and terminating SAPs

DoD Manual 5200.01, Vol. 3, Encl. 5, Sec. 10

29

Management and Oversight Training

- Certification & Accreditation of Secure Networks
- Declassification reviews
- Program Oversight & Self-inspections

30

Program Oversight

Remember:

- Training must be evaluated
- Training records maintained
- Assess quality and effectiveness

31

Contacts and Resources

- Access CDSE Job Aids OCA Desktop Reference, Marking Classified Information, and Deployable Security Trainer at http://www.cdse.edu/resources/supplemental-job-aids.html
- A handout and frequently asked questions from this webinar will be posted at http://www.cdse.edu/catalog/webinars/security-education.html
- Email information security training related questions to DSS at informationsecurity.training@dss.mil

32