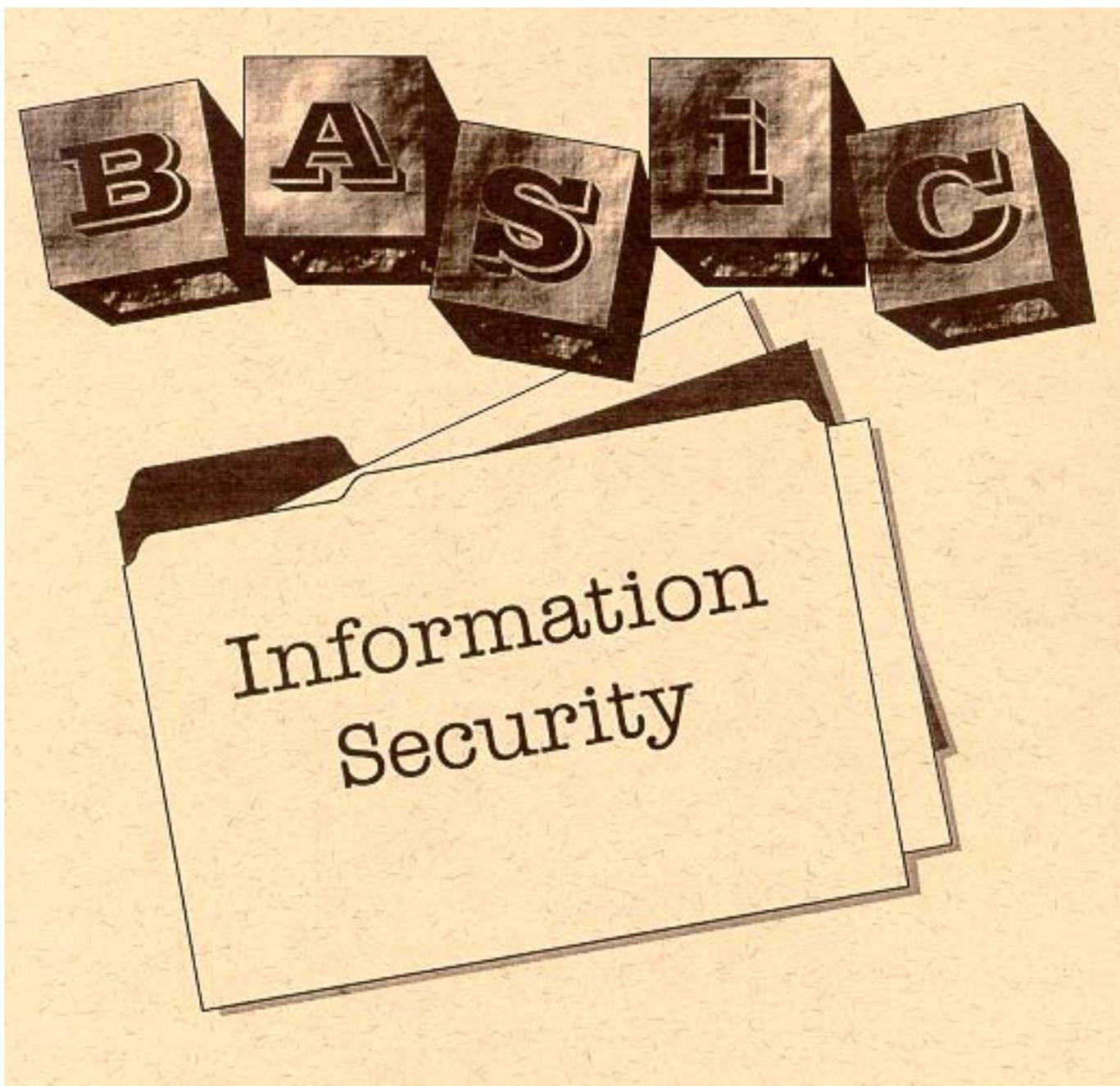


COURSE
IF 001.08

EDITION
A



Defense Security Service
Academy

The Instructors at the Defense Security Service Academy (DSSA) are interested in providing timely responses to inquiries.

Use the following At-A-Glance lists to identify your inquiry type. Once you have done this, follow the directions below and email or phone.

ADMINISTRATIVE INQUIRY:

REQUESTS FOR --

- Disenrollment
- Course Reissue
- Enrollment Extension

CHANGE IN --

- Address
- Unit
- Rank or Grade

PROBLEMS WITH --

- Enrollment
- Incorrect SSN
- Incorrect RYE Date

COURSE CONTENT INQUIRY:

LESSON OR EXAM IN ERROR WITH --

- Field Manual Procedure
- Doctrine
- Technical Manual Procedure
- Equipment Specification -

INCORRECT REFERENCE OR EXTRACT

- Regulation
- Pamphlet
- Field Manual
- Policy

CONFUSING INFORMATION

- Example
- Organization
- Wording
- Situation
- Illustration
- Chart
- Figure
- Table

DIFFICULTY LEVEL

* Too High * Too Low

NOTICE

We have made every effort to ensure that the content of this Course accords with all applicable policies in effect at the time it was printed. However such policies may change in the interval between printings and the technical accuracy of a given edition of the Course cannot be guaranteed in all particulars. Questions regarding technical accuracy should be directed to the DSSA Information Security Team (see General information: Content Assistance). However you should base your responses to the questions in the Course examination solely on the information provided in the Course and not on any other source.

**This course contains no classified information.
All security markings used in this Course are for
illustration and training purposes only.**

August 1997

*DEFENSE SECURITY SERVICE ACADEMY
DEFENSE SECURITY SERVICE
Linthicum, MD 21090*



Welcome to *Basic Information Security (BIS)*!

Basic Information Security is intended to give you the baseline requirements for the Information Security Program. It provides an overview of the program and details the requirements and procedures that you will encounter in your dealings with classified materials.

We recognize that the Information Security Program may not be your primary focus. We've designed BIS for those who handle classified materials but do not perform or oversee full-time security duties that involve classified information. We realize that your time is valuable and that tasks associated with classified information have to be done quickly and efficiently. And we also realize that you probably perform these tasks only once in a while. To assist you, we have covered the minimum requirements and have addressed the common situations you are likely to run into when working with classified materials.

Bear in mind that the procedures discussed are the DoD required procedures. Your Component headquarters has likely supplemented these procedures with their own. And even your activity may have added its own security procedures. Be sure to check with your security manager for more information on your specific security program.

We are always in greater danger from those we trust than from those whom we do not, and adherence to sound security practices is the best safeguard not only against others but also against our own frailties. As a possessor of classified information, you are the primary defense against unauthorized disclosure, responsible for guarding a part of our nation's security. Much depends on your success. I hope you will find that *Basic Information Security* prepares you to succeed.

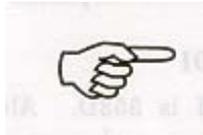
Kevin Jones
Director

Contents

	Page
General Information	i
Course Objectives	vii
Acronyms and Abbreviations	ix
Introduction	ix
1 Introduction to the Information Security Program	1-1
2 Basic Classification Management	2-1
3 Duration of Classification	3-1
4 Marking Classified Information	4-1
5 Derivative Classification Issues	5-1
6 Effective Security Practices	6-1
7 Safekeeping and Storage	7-1
8 Transmission and Transportation	8-1
9 Disposal and Destruction	9-1

General Information

PURPOSE



This Course is designed to help Government personnel - both military and civilian - gain an understanding of the Information Security Program and its basic policies for classifying and declassifying information and apply the requirements and techniques that ensure that classified information is clearly identified and properly protected.

ADMINISTRATION

The DSS Academy(DSSA) administrators the DSSA subcourses.

ENROLLMENT ASSISTANCE

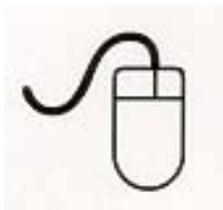


On any matter concerning your enrollment, (a change in your mailing address, nonreceipt of materials, your exam score, etc.) communicate with DSSA, use one of these numbers:

* **Commercial: (410) 865-2295 or 2732.**

* **DSN:283-7295/7732.**

To e-mail :



- Send comment to DSSA.IF@mail.dss.mil

STUDYING THE LESSONS



To get the most out of each lesson we urge you to follow this procedure

Note the lesson objectives and refer to them from time to time as you go through the lesson text Complete the review exercises for the lesson. Refer to the lesson text to check your answers.

CONTENT ASSISTANCE



If you have a question about the content of this Course or if you have a correction or suggestion to make to improve its content, contact the DSSA Information Security Team (INFST). To phone us, use one of these numbers:

- Commercial: (410) 865-2295/2732
- DSN: 283-7295/7732

To e-mail us:

- Send comments to DSS.IF@mail.dss.mil

To write us:

- Send a letter to:

**DSS Academy
ATTN:IF
938 Elkridge Landing Rd.,
Linthicum, MD 21090**



ADDITIONAL DSSA COURSES

For **our catalog**, write to DSSA, ATTN: Registrar. Visit our home page at <http://www.dss.mil/training>

TIME LIMIT



DSSA allows you up to one year to complete this Course. If you are employed by the Defense Security Service and your enrollment in this Course has been directed by a supervisor, then the Course may be completed during duty hours.

COURSE OBJECTIVES

When you have completed this course, you should be able to do the following:



- * Describe the nature and purpose of the Information Security Program
- * Identify the national and Department of Defense organizations that have a policies and procedures of the Information Security Program and describe their functions.
- * Distinguish between "original classification" and "derivative classification."
- * Describe the process that should be followed when an original classification authority is making a decision on whether to classify an item of information.
- * Properly classifies materials using the derivative classification process.
- * Determine the declassification instructions that would be placed on an originally classified document and on a derivative classified document and properly interpret for others the declassification instructions found on documents.
- * Apply the proper classification and associated markings onto an originally classified document and a derivative classified document and interpret for others the various markings found on classified materials.
- * Implement the proper procedures for handling classified materials in your office environment.

EXAMINATION



When you feel confident that you can meet the objectives for the entire Course, do the following:

- Access the ENROL web site:
<https://enrol.dss.mil/enrol/default.asp>
- Go to this course
- And click on the exam URL.

The examination is an open book test; passing score is 76 percent (at least 76 items correct out of 100). If you score less than 76 percent, take the test again.

DSSA CERTIFICATE

When you have successfully completed the exam an online Certificate of Completion will be available for printing.

Acronyms & Abbreviations

APO	Army Post Office
ASD(C31)	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
C	Confidential
CNO	Chief of Naval Operations
CNWDI	Critical Nuclear Weapons Design Information
COMSEC	Communications Security
GSA	Cognizant Security Agency
CSS	Constant Surveillance Service
CTS	Cosmic Top Secret (NATO)
DA	Department of Army
DCI	Director of Central Intelligence
DCS	Defense Courier Service
DID Form 173	(Fictional form)
DID Form 2	Armed Services Identification Card
DID Form 2501	Courier Authorization Card
DECL	Declassify on
DEN	Denmark
DIVA	Defense Interoperability Validation Agency (fictional)
DoD	Department of Defense
DoD 5200.1-1	Index of Security Classification Guides
DoD 5200.1-R	Information Security Program
DOE	Department of Energy
E.O.	Executive Order
FAA	Federal Aviation Agency
FEDEX	Federal Express
FGI	Foreign Government Information
FOIA	Freedom of Information Act
FPO	Fleet Post Office
FIRD	Formerly Restricted Data
FSS	Federal Supply Schedule
GSA	General Services Administration
IDS	Intrusion Detection System
ISCAP	Interagency Security Classification Appeals Panel
ISOO	Information Security Oversight Office
ISP	Information Security Program
MEX	Mexico
MTMC	Military Traffic Management Command

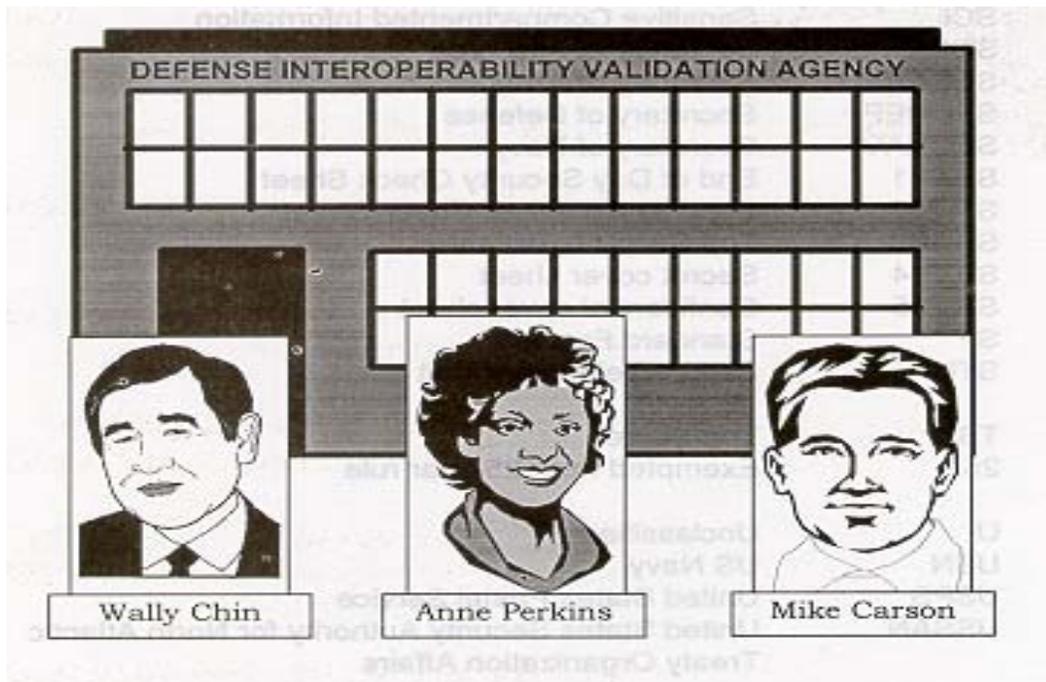
N	Portion marking for Critical Nuclear Weapons Design Information
NACSI	National Communications Security Instruction
NARA	National Archives and Records Administration
NATO	North Atlantic Treaty Organization
NC	NATO Confidential
NISP	National Industrial Security Program
NR	NATO Restricted
NS	NATO Secret
NSA	National Security Agency
NSC	National Security Council
NZ	New Zealand
OADR	Originating Agency's Determination Required
DEI	Dissemination and Extraction of Information
OC	Controlled by Originator
OCA	Original Classification Authority
OMB	Office of Management and Budget
PM	Program Manager
PR	Caution-Proprietary Information Involved
PSS	Protective Security Service
R	Restricted
RD	Restricted Data
S	Secret
SAP	Special Access Program
SCG	Security Classification Guide
SCI	Sensitive Compartmented Information
SECAF	Secretary of Air Force
SECARMY	Secretary of Army
SECDEF	Secretary of Defense
SECNAV	Secretary of Navy
SF 701	End of Day Security Check Sheet
SF 702	Security Container Check Sheet
SF 703	Top Secret cover sheet
SF 704	Secret cover sheet
SIF 705	Confidential cover sheet
SF	Standard Form
STU	Secure Telephone Unit
TS	Top Secret
25X	Exempted from 25-year rule
U	Unclassified
USN	US Navy
USPS	United States Postal Service
USSAN	United States Security Authority for North Atlantic Treaty Organization Affairs
X	Exempted from 10-year rule

Introduction. . .

Welcome to Basic Information Security! This course is designed to provide you basic knowledge and skills concerning the Information Security Program. As you move through the lessons, you'll meet some of the personnel who deal with security issues at the fictitious Defense Interoperability Validation Agency (DIVA).

Three of the people you will meet - Wally Chin, Anne Perkins, and Mike Carson - are from DIVA's Security Office. As they instruct and advise DIVA employees, you will get an overview of the Information Security Program: the organizations that oversee and guide it, how information is classified originally by a few authorities within the Department of Defense and how their decisions are carried forward by the many others in the DoD who derivatively classify the sensitive information they encounter in their work, how classified information is downgraded and declassified, how classified materials are marked and handled in the office, and how they are stored, transmitted, and destroyed.

We hope you'll find that DIVA is not so different from your own organization, and that seeing how the DIVA people cope with their security duties will help you in carrying out your own. Now let's get started!



LESSON 1

INTRODUCTION TO THE INFORMATION SECURITY PROGRAM



One of the U.S. Government's most valuable assets is national security information. It must be protected because in the wrong hands it could be used to damage, even devastate, our national security. To protect it we identify it as sensitive, classify it, and then ensure that only authorized personnel with a need-to-know access it. In this lesson, we'll look at the Information Security Program: at its origins, at Executive Order 12958 that drives it, at the Federal agencies that oversee it, and at how DoD implements it. At the end of this lesson, you will be able to do the following:

- Define "classified information."
- Describe the nature and purpose of the Information Security Program.
- State the basic classification policy of Executive Order 12958.
- Identify types of information that require the application of special rules.
- List the functions of the Information Security Oversight Office and identify the use of Standard Form 311.
- Describe how the Department of Defense implements the information security program.

What is Classified Information?



Wally Chin

The Defense Interoperability Validation Agency (DIVA) requires all new employees to attend a security education class. Let's look in on one.

"First, I'd like to welcome you to DIVA! I'm Wally Chin, a security specialist with the Security Office. I've been with the agency for several years and really enjoy working here!"

"Many of you will be working on projects involving classified information. Today we'll discuss the program that governs classified information. In fact, let's start by figuring out exactly what classified information is. There are three factors to consider. Who can give me one of them?"

"It's information that we don't want our enemies to get hold of," Josh Smith says.

"Right, Josh! But is it just our enemies who shouldn't get hold of it? Nowadays especially, the threat is much broader than that. We want to prevent *any* unauthorized disclosure of the information. So let's expand on Josh's point and say that one aspect of classified information is that it is *information that requires protection from unauthorized disclosure*. All right, that's one factor. Who has another one?"

"It's information that's related to our government. What I mean is that if a company like Lockheed Martin develops information for its own use, not the government's, the information isn't eligible for classification," says Alice Connors.

"That's right, Alice. Lockheed Martin might call that information 'company proprietary,' but they can't classify it. To be eligible for classification, information must be *owned by, produced by, or for,*

or under the control of the U.S. government. It's got to be official government information."



"Wait," says Josh. "What do you mean by 'under the control of the U.S. government. Anytime anyone hands something over to someone else, it's under the 'control' of the receiver. So if Lockheed Martin handed over some of their information to the U.S. government, wouldn't that information be under the 'control' of the U.S. government, and thus eligible for classification?" "With classified information, 'control' is more than just physical possession of it, Josh. 'Control' means *the authority to regulate access to the information.*

"So far we've got two pieces of the puzzle," continues Wally.

"How about the third?"

"Well, I suppose if you're going to classify a piece of information, you've got to let people know that the information is classified," Alice offers.

"Bingo! Once you determine that information should be classified, you've got to *designate* it! Now let's put the three factors together. In general...

Classified information is information that is...

- **Owned by, produced by, or for, or under the control of the U.S. Government**
- **Determined to require protection against unauthorized disclosure, and**
- **So designated.**

"Josh, can you tell us what the three designations for classified information are? "

"Sure. We designate classified information by marking it *Top Secret, Secret, or Confidential.*"

The Need for the Information Security Program

uniform guidance
The ISP

"Correct! This brings up another important point -the need for a uniform program to govern the classification of information. The program must give us a single sheet of music - uniform guidance -to classify information. And not just to classify it. We need uniform guidance to store it, transport it, destroy it, and so forth. And the program must not only *determine* the guidance. It must also *oversee the application* of that guidance. That's just what the information security program is and does. The ISP has been evolving since the 1950s. It's based on a series of presidential executive orders and follow on administrative directives. So now let's turn our attention to the executive order that provides the direction for today's Information Security Program.

Executive Order 12958



"We've always protected certain information in the Government," Wally begins. "We can find examples of Secret documents and non-disclosure agreements as far back as the Constitutional Convention and George Washington's administration. But for years this protection was done rather informally, with various departments and agencies having their own rules - even their own security classifications! Imagine what it would be like if that were the case today, with all the dealings we have with other agencies around here. Talk about confusion!

"World War II focused attention on the problems and dangers that resulted from a lack of standard information security systems in the Government. Then in 1951, President Truman issued Executive



Order 10290. This order established the first, umbrella' program to protect classified information in *all* departments and agencies of the Executive Branch, not just the military departments. So for the first time a standard information security program was applied to all of the executive branch agencies. Note that *an executive order applies only to the Executive Branch*. It does *not* apply to the Legislative and Judicial Branches of our government. These branches establish their own rules for safeguarding classified information.

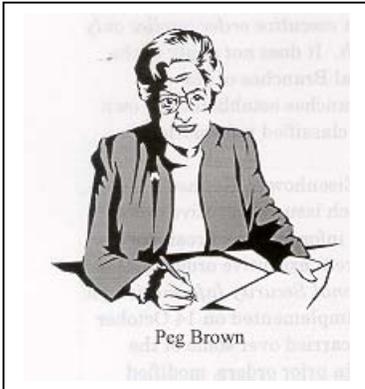
"Presidents Truman, Eisenhower, Kennedy, Nixon, Carter, and Reagan each issued executive orders dealing with classified information. President Clinton issued the current executive order, E.O. 12958, *Classified National Security Information* on 17 April 1995. It was implemented on 14 October 1995. E.O. 12958 has carried over some of the principles established in prior orders, modified others, and established a few new ones.

The basic classification policy of E.O. 12958 is...

- **Information will be classified when necessary to prevent damage to the national security, but only when necessary.**
- **The information will remain classified as long as necessary, but no longer.**

"Now, let's try to apply the basic policy to a situation," Wally says. "You'll learn about original classification and the delegation of original classification authority in the next session. For now, just suppose you're the Director of DIVA and you have been delegated the authority to originally classify information. Someone comes to you with a new piece of information. In accordance with the basic policy, what would you have to ask yourself?"

"I think the key phrases are 'when necessary to prevent damage to the national security' and 'but only when necessary,'" Peg Brown says. "It's not like I can look at the piece of information and just say to myself, 'Hey, this looks important. It should be classified.' I have to ask whether unauthorized disclosure of the information will cause any damage to our national security. Only if it will cause damage is the information eligible to be classified."



"Exactly right, Peg. Now suppose you, as Director of DIVA, determine that the new information should be classified. What does the basic policy mean when it states that 'the information will remain classified as long as necessary, but no longer'?"

"I think it means that the information shouldn't stay classified when disclosing the information no longer puts national security at risk," Peg says.

"Right again, Peg. Over time almost all information loses both value and sensitivity. Why keep information classified when there's no harm caused by its disclosure? This Executive Order *promotes declassification and public access to information as soon as national security considerations permit.*

Information That Requires Special Rules-----

"Some types of classified information do not fall under E.O. 12958. 'Restricted Data' is one of them. It's information related to atomic weapons and nuclear material and falls under the Atomic Energy Act of 1954. The Department of Energy (DOE) is the executive agency for implementing the Atomic Energy Act, so DOE develops the procedures for classifying, declassifying and handling 'Restricted Data.' 'Formerly Restricted Data' has been removed from the 'Restricted Data' category by a joint determination of DOE and DoD. They jointly decide on the declassification of 'Formerly Restricted Data,' while DOE develops the handling procedures.

"Communications Security (COMSEC) information, Sensitive Compartmented Information (SCI), and Special Access Program (SAP) information fall under E. O. 12958, but the procedures for accessing and handling these types of classified information are developed by specified organizations. The National Security Agency (NSA) develops COMSEC procedures; the Director of Central Intelligence (DCI) develops the SCI procedures; and the appropriate program manager develops the Special Access Program procedures.

Information that requires the application of special rules:

- * **Restricted Data - DOE**
- * **Formerly Restricted Data - DOE in conjunction with DoD**
- * **Communications Security (COMSEC) information - NSA**
- * **Sensitive Compartmented Information (SCI) DCI**
- * **Special Access Program (SAP) information SAP PM**

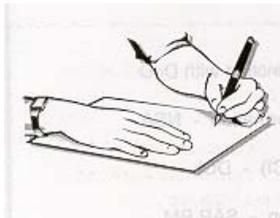
"So if you handle any of these types of information, look up which organization has cognizance over the development of special rules for them, find out what those rules are, and properly apply them.

Executive Branch Oversight

"Let's look now at the two organizations that provide oversight and management for the Information Security Program within the entire Executive Branch.

Executive Branch oversight of the Information Security Program is provided by:

- National Security Council (NSC)
- Information Security Oversight Office (ISOO)



"The *National Security Council* provides overall policy direction for the Information Security Program. As the NSC helps the President develop and issue national security policies, it guides and directs the implementation and application of E.O. 12958. The NSC exercises its guidance primarily through the *Information Security Oversight Office (ISOO)* (pronounced EYE-soo). E.O. 12958 made ISOO responsible for administering and monitoring the Information Security Program for the NSC. So, although it is not a part of the NSC, ISOO functions as its operating arm for information security.

"ISOO issues *OMB Directive No. 1, Classified National Security Information*. It implements the Executive Order and further defines what the Executive Branch agencies must do to comply with the E.O.'s requirements. In carrying out its responsibilities, ISOO performs several functions.

Functions of the ISOO include...

- Taking action on complaints and suggestions concerning the administration of the ISP.
- Maintaining liaison with agency counterparts.
- Conducting on-site inspections and special document reviews to monitor agency compliance with the ISP.
- Compiling and consolidating data from each agency1department within the Executive *Branch into* an
- Annual Report to the President
- Conducting special studies on identified or potential problem areas and developing remedial approaches for program improvement.
- Developing and disseminating security education materials and monitoring agencies' security education and training programs.



"The fourth item on the list is one that you may find yourself contributing to - ISOO's annual report to the President. Each agency and department within the Executive Branch must submit a *Standard Form 311 (SF 311), Agency Information Security Program Data* to ISOO each year. This form requests information such as how many Top Secret documents you have, the amount of Secret and Confidential documents you have, how many original classification decisions were made during the past year, how many derivative classification decisions were made during the past year, and so on. ISOO combines all of the data and sends its annual report to the President.

DoD provides data concerning its classified holdings to the Information Security Oversight Office...

- By requiring DoD Components to complete an SF 311 each fiscal year and sending that form to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence [ASD(C31)] by October 20.
- By having the ASD(C31) consolidate the information received and submitting its own SF 311 to the Information Security Oversight Office by October 31.

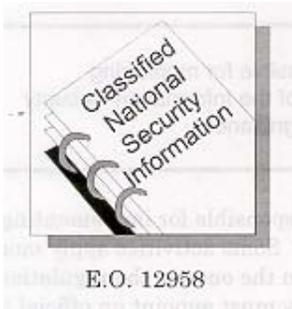
"ISOO's report is significant because it highlights trends and the causes of those trends.

"Here's what the SF 311 looks like.



(IMPORTANT — Read instructions on reverse before completing this form)			INTERAGENCY REPORT CONTROL NUMBER 0230-NAR-AN				
AGENCY SECURITY CLASSIFICATION MANAGEMENT PROGRAM DATA			1. FISCAL YEAR COVERED				
2. DEPARTMENT, INDEPENDENT AGENCY OR ESTABLISHMENT		3. CONTACT FOR ADDITIONAL INFORMATION (Name, office and telephone no.)					
4. SENIOR AGENCY OFFICIAL (Section 5.6, E.O. 12958)							
5. NUMBER OF ORIGINAL CLASSIFICATION AUTHORITIES							
A. TOP SECRET		B. SECRET		C. CONFIDENTIAL			
6. NUMBER OF CLASSIFICATION DECISIONS							
CLASSIFICATION LEVEL		ORIGINAL CLASSIFICATION			DERIVATIVE		
		DECLASSIFY IN 10 YEARS OR LESS (a)		EXEMPT FROM DECLASSIFICATION IN 10 YEARS (b)			
A. TOP SECRET							
B. SECRET							
C. CONFIDENTIAL							
7. MANDATORY REVIEW REQUESTS		CASES CARRIED OVER FROM THE PREVIOUS PERIOD (a)	NEW CASES RECEIVED (b)	CASES CARRIED OVER TO NEXT PERIOD (c)	DECLASSIFICATION DECISIONS (Report in pages)		
					GRANTED IN FULL (d)	GRANTED IN PART (e)	DENIED (f)
A. REQUESTS							
B. APPEALS							
8. PAGES DECLASSIFIED: AUTOMATIC DECLASSIFICATION AND SYSTEMATIC REVIEW FOR DECLASSIFICATION (Sections 3.4 and 3.5 of EO 12958)				9. INTERNAL AGENCY OVERSIGHT Number of Formal Inspections, Surveys, or Program Reviews			
10. EXPLANATORY COMMENTS							
<i>(Use this space to elaborate on any section of this form. If more space is needed, use a blank sheet(s) of paper and attach to form.)</i>							

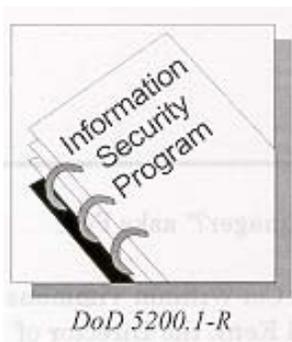
DoD Implementation of E.O. 12958



"Let's take a quick look at how DoD implements E.O. 12958 and then recap our session.

"E.O. 12958 requires that each Executive Branch agency and department involved with classified information must designate a *senior official* who will be responsible for ensuring that the guidance set forth in E.O. 12958 is carried out effectively and uniformly.

The DoD has designated the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence [ASD(C31)] as its senior official for implementing information security policy.



"The Assistant Secretary of Defense for C31 has primary responsibility for providing guidance, oversight, and approval of policy and procedures governing the DoD Information Security Program. The ASD(C31) exercises its oversight through reviewing the SF 31 Is, for example. And the ASD(C31) provides guidance by issuing *Information-R*. This regulation *Security Program, DoD 5200.1* gives the baseline security requirements for all of DoD. DoD 5200.1-R provides guidance and direction on classification management (original classification and derivative classification) and on how to mark, protect, and handle classified materials.

DoD 5200.1-R provides mandatory minimum-security standards for all DoD activities.

"The *Military Departments and DoD Components* add their own requirements to the DoD standards.

They must monitor and oversee the information security program within their respective organizations and designate a *senior agency official* to oversee the program.

Designated senior agency officials are responsible for monitoring and reporting on the status of administration of the Information Security Program at all levels of activity under their cognizance.

"Also, each *activity* is responsible for implementing the 5200.1-R standards. Some activities apply more stringent standards than the ones in the regulation. The head of each activity must appoint an official to serve as its *security manager*.

Security managers are responsible for the administration of an effective Information Security Program within their activity. Emphasis is placed on:

- Security education and training
- Assignment of proper classifications
- Downgrading and declassification
- Safeguarding
- Monitorship



"Do we have a security manager?" asks Peg. "Yes," Wally answers, "Lt Col William Timmons was appointed by General Kent, the Director of DIVA, to be the security manager for DIVA. That's why you'll see his signature on most of the correspondence related to security matters.

Summary



"In this session, you learned that our Information Security Program provides the necessary uniform guidance, oversight, and management for personnel in the Executive Branch who deal with classified information. Josh, Alice and Peg helped us define 'classified information' as official government information that has been determined to require protection against unauthorized disclosure and has been so designated. We said that 'official government information' is information that is owned by, produced by, or for, or under the control of the U.S. Government. Josh pointed out the designations for classified information: Top Secret, Secret, and Confidential. We identified the basic classification policy of E.O. 12958: Classify when necessary, but only when necessary. Classify as long as necessary, but no longer. Special rules apply to Restricted Data, Formerly Restricted Data, COMSEC, SCI, and SAP information. We looked at how the program is managed within the Executive Branch. The National Security Council (NSC) is responsible for policy direction and implementation, while the Information Security Oversight Office (ISOO) shoulders the overall administration and monitoring of the program. We identified the SF 311 as the main way ISOO keeps tabs on the amount of our classified holdings and as a way of monitoring the programs within the agencies. We saw how the DoD implements the program. The Assistant Secretary of Defense for C31 is the senior official with overall responsibility for implementation within DoD. The ASD(C31) issues Information Security Program, DoD 5200.1-R, which gives the baseline security requirements for all of DoD. Designated senior agency officials oversee the ISP for the Military Departments and DoD Components, while each activity's security manager is responsible for its program administration."

REVIEW EXERCISES

1. The definition of "classified information" contains three factors, as follows:
 - a. _____
 - b. _____
 - c. _____ and designated as classified.
2. The Information Security Program as delineated in Executive Order 12958 is necessary for two reasons. The program provides uniform guidance in the classification and handling of the information, and it
 - a. provides guidance for performing personnel security clearances.
 - b. determines who has ownership over the materials.
 - c. oversees the application of the guidance.
 - d. gives us two levels of classification.
3. Executive Order 12958 is significant in that it is the first instance of a uniform Information Security Program being applicable to all Executive Branch agencies.

True. False.
4. The basic classification policy of E.O. 12958 is that information will be classified _____ to prevent damage to the _____ but only _____; and that information will remain classified as _____, but _____.
5. List three types of information that require the application of special rules.
 - a.
 - b.
 - c.

6. Match the organizational entity with its function(s) in implementing and overseeing the Information Security Program.

Function		Organization	
___	a. Collect and consolidate information and send annual report to President	(1)	NSC
___	b. Senior official for security policy in DoD	(2)	ISOO
___	c. Provide overall policy direction for the Executive Branch's Information Security Program	(3)	ASD(C31)
___	d. Develop and disseminate security education materials for Executive Branch agencies	(4)	Activity security manager
___	e. Take action on complaints concerning administration of the Information Security Program within the Executive Branch		
___	f. Administer activity unique Information Security program		

7. DoD _____ is the regulation that mandates the minimum security standards within the Department of Defense.

8. Each agency and department within the Executive Branch submits a report to ISOO that includes data concerning their classified holdings on

- a. a weekly basis.
- b. a monthly basis.
- c. a semi-yearly basis.
- d. a yearly basis.

SOLUTIONS AND REFERENCES

1. a. Owned by, produced by, or for, or under the control of the US Government.
b. Determined to require protection against unauthorized disclosure.
(p. 1-3)
2. c. (p. 1-4)
3. False (pp. 1-4-5)
4. when necessary, national security, when necessary,
long as necessary, no longer (p. 1-5)
5. Any three of the following:

Restricted Data
Formerly Restricted Data
COMSEC
Scl
SAP (p. 1-7)
6. a. (2)
b. (3)
c. (1)
d. (2)
e. (2)
f. (4) (pp. 1-8-12)
7. 5200.1-R. (pp. 1-11-12)
8. d. (pp. 1-8-9)

LESSON 2

BASIC CLASSIFICATION MANAGEMENT



Original Classification Authorities
OCAs

In Lesson 1, you learned that the Information Security Program provides uniform guidance for the management of classified information. In this lesson, we'll identify the basis for the three levels of classification and define them. We'll discuss original classification authority - where it comes from and how personnel in the Executive Branch become original classification authorities (OCAs). We'll cover training for OCAs and limitations on some OCAs' authority. We'll look one by one at the determinations that an OCA must make before originally classifying information. We'll wind up by looking briefly at derivative classification and at the responsibilities of - and procedures for - those who implement the OCAs' decisions. At the end of this lesson, you will be able to do the following:

- Define the terms "Top Secret," "Secret," and "Confidential" as they apply to information.
- Distinguish between original and derivative classification.
- Describe original classification authority.
- Identify the steps in the original classification process
- Identify the responsibilities of original classifiers and derivative classifiers.
- Explain tentative classification and how to challenge a classification.

Classification Designation



Rudy Tucker

"In our last session," Wally begins, "we defined classified information. We said that classified information is official government information that has been determined to require protection against unauthorized disclosure and that has been so designated. We noted that the three designations for classified information are 'Top Secret,' 'Secret,' and 'Confidential.' Can anyone tell me what determines whether information is designated 'Top Secret,' 'Secret,' or 'Confidential'?" "If unauthorized disclosure causes a lot of damage, the information is designated 'Top Secret.' If only minor damage will occur, the information is classified 'Confidential.' 'Secret' falls somewhere in between," offers Rudy Tucker. "Right, Rudy. The difference between the designations is the *extent of the damage that unauthorized disclosure would likely cause.*

Designation	Unauthorized disclosure of this information could reasonably be expected to cause
Top Secret	exceptionally grave damage to our national security that the Original Classification Authority is able to identify or describe.
Secret	serious damage to our national security that the Original Classification Authority is able to identify or describe.
Confidential	damage to our national security that the Original Classification Authority is able to identify or describe.

"Be aware that *all* classified information can cause damage to the national security if disclosed without authorization. Don't fall into the trap of thinking of Confidential information as 'only Confidential.' And if you hear of anyone doing so, you may want to take them aside and give them a bit of one-on-one security education. Remember, *all three types of classified information must be protected.*

The Two Types of Classification

"We've defined classified information. We've discussed the levels of security classification. Now it's time we talked about how information becomes classified," Wally says.

Information becomes classified by either
Original classification
Derivative classification

Original Classification Authority



"Let's look first at original classification. Original classification is an *initial determination that information needs to be protected,*" Wally says. "This determination can be made only by a designated *Original Classification Authority (OCA.)* There are about 5,380 OCAs in the Executive Branch and about 1,400 in the DoD.

Original Classification Authority
(OCA.)

What positions in the DoD carry original classification authority? Any ideas?"



"I'll bet the Secretary of Defense is an OCA," Alice says.

"And how about the Secretaries of the Military Departments?" Peg suggests.

"This is too easy! Yes, the President has delegated original classification authority to the people in these positions. And since they are all very busy, they delegate original classification authority to other officials who need it. For example, at DIVA we have one OCA - General Kent."

"What happens when he's away from DIVA and original classification decisions need to be made?" Rudy asks.

"Good question! People who hold positions move on to other positions, and, as Rudy points out, they're sometimes away on business or vacation. That's why ...



Original classification authority is delegated to the occupant of a position not a person by name.

"That way, whoever is occupying the position, has the authority that goes with it. For instance, in General Kent's absence, DIVA's Deputy Director, Captain Douglas, assumes the position of Director. Since it's the position that has the authority, while Captain Douglas serves as Acting Director, she can exercise original classification authority.

"Note carefully," Wally continues, "That not all OCAs are delegated Top Secret original classification authority. Some OCAs are delegated Secret authority, while others are delegated Confidential authority. *The delegation of the authority will specify the highest level at which the*



OCA's in training

OCA can classify a piece of information. They can classify at that level and below. So OCA's with Confidential original classification authority can't assign the designations Secret or Top Secret to information. And OCA's with Secret original classification authority can't assign the designation Top Secret."

"It seems to me," Rudy says, "that being an OCA is a big responsibility. How do these folks learn what they're supposed to do?"

"All OCA's are required to go through training. This training covers the fundamentals of security classification, limitations on an OCA's authority to classify information, and an OCA's responsibilities. This training is a prerequisite to the exercise of original classification authority."

"Whose job is it to train the OCA's?" Rudy asks.

"The security manager at the OCA's organization," Wally replies.

"But, Wally, those people at high level positions, such as General Kent, are really busy. How are you going to make sure they get the proper training?"



orientation package

"E.O. 12958 stresses that OCA's must be aware of their responsibilities. After all, they're accountable for their classification decisions! To ensure accountability, the E.O. makes the management of classified information a critical element of their performance evaluations. Our security manager tapped me to give the training to General Kent. I used the OCA orientation package developed by the DoD Security Institute. It's a notebook with a five minute orientation videotape called 'The Thinker' that gives an overview of the E.O. There's also a copy of the E.O. and two job aids - 'Desktop Reference Guide' and '13 Steps to Quality

Classification Decisions.' We viewed the videotape and then went over the information in the notebook.

The Original Classification Process



"Now let's look at how an OCA determines whether or not to classify information. Before an OCA can make a classification determination, each item that may require protection needs to be identified. This is called *identification of specific information*. Then the original classification process can begin. Although the process of original classification can be complex and difficult, it consists basically of the following steps.

Original Classification Process

1. Determine current classification status
2. Determine if official government information
3. Determine if in an authorized category
4. Determine if prohibited intent or type
5. Determine likelihood of damage to national security and be able to identify or describe the damage
6. Weigh advantages and disadvantages
7. Assign a level of classification
8. Make a decision about the duration of classification
9. Communicate the decision

Step 1. Determine Current Classification Status _____

"In this step, the OCA must answer the question 'Is the piece of information *already classified*. If the answer is 'yes,' the OCA stops. There's no need to

classify the information a second time! If the answer is 'no,' the OCA proceeds to the next step.

Step 2. Determine If Official Government Information-----



"Next, to be eligible for classification, information must be *official government information*. Last time we said that official government information is owned by, produced by, or for, or under the control of the U.S. Government. Now that you know the long version, we can simply say that the U.S. *Government must own, have a proprietary interest in, or control the information.*

Step 3. Determine If In An Authorized Category-----

Classification Categories in Section 1.5 of E. O. 12958 (para 2-301, DoD 5200.1-R)

a. Military plans, weapons, or operations

b. Foreign government information

c. Intelligence activities (including special activities), intelligence sources or methods, or cryptology

d. Foreign relations or foreign activities of the United States, including confidential sources

e. Scientific, technologic, or economic matters relating to the national security

f. U.S. Government programs for safeguarding nuclear materials or facilities, or

g. Vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security

Step 4. Determine If Prohibited Intent or Type-----

"The OCA must rule out that classification is being considered for some reason other than to protect the national security. In other words, classification

must never be used as a smoke screen to cover up or promote wrongdoing.

E.O. 12958 Prohibitions

You cannot classify information to...

- Conceal violations of law, inefficiency, or administrative error.
- Prevent embarrassment to a person, organization, or agency.
- Restrain competition.
- Prevent or delay the release of information that does not require protection in the interest of national security.

You cannot classify...

- Basic scientific research information unless it clearly relates to national security.

Step 5. Determine Likelihood Of Damage

This step and the next one are particularly difficult. The OCA's good judgment is essential.

"The OCA must now determine that *the unauthorized disclosure of the information could reasonably be expected to cause damage to the national security.*



"And this determination can't be just a vague notion or a hunch. E.O. 12958 requires that the damage *can be identified or described.* "

I Does the OCA have to give a written description of the damage each time a decision is made to classify information?" Josh asks.

"No, it's not necessary for the OCA to produce a written description of the damage at the time of classification. But the OCA must be prepared to do so if the information becomes the subject of a

classification challenge - a request for mandatory review for declassification, or a request for release under the Freedom of Information Act (FOIA)."

"As you can see, there are no easy answers, pat solutions, or handy formulas for the OCA's decisions."

Step 6. Weigh Advantages and Disadvantages-----



Josh says, "It must cost a lot of money to keep information protected - buying the safes to store it and clearing the people to have access to it."

"You bet it does! In fact, the next step is to determine the *advantages and disadvantages of classification*. Here is where the OCA, who is used to making management decisions on a daily basis, must consider the benefits and drawbacks of the classification. If the OCA has a significant doubt about classification during this step, the information should not be classified.

Step 7. Assign the Level Of Classification-----



"Once the determination to classify is made," Wally continues, "the OCA must assign a level of classification. Remember, the levels of classification are based upon the *degree of damage unauthorized disclosure would likely cause*. Unfortunately, there are no handy formulas to determine degrees of damage. Here again it's a judgment call. If there's a significant doubt about the appropriate level of classification, the information must be classified *at the lower level*."

Step 8. Set the Duration-----

"At the same time an OCA decides that information should be classified, he or she must make a decision about *how long the classification should last*," Wally

says. "The OCA has several options available. We'll look at them in a future session.

Step 9. Communicate the Decision-----

"Finally, the OCA must *communicate the decision*. An OCA can communicate a classification decision in two main ways.

Two ways to communicate an original classification decision are...

- Issuing classification guidance.
- Ensuring that the information is properly marked in a document.



a new project

Let's say you're working on a new project. The project involves the creation of a new military aircraft - the TK47 Bomber. Since it's a new project and a new aircraft, the related information is also new. First, General Kent will identify any information that may require protection. He then determines which of that information needs to be classified and assigns a level of classification to each element of information. Perhaps he decides that certain information related to the design of the aircraft will be classified Secret. Other information related to the aircraft's capabilities will be classified Confidential.

"How does General Kent communicate his classification decisions concerning the TK471 Bomber project to the rest of us? He issues *classification guidance*. Classification guidance can take many forms - security classification guides, project directives, memoranda, and plans. In this case, General Kent will issue a Security Classification Guide for the TK47 Bomber. The Executive Order encourages each OCA to issue a security classification guide for each classified system, program, plan, and project. These guides contain

instructions on the classification of project information, including the level of classification. We now cross the border from original classification to ...

Derivative Classification



derivative classification

"As a member of the project team, you are responsible for applying General Kent's classification decisions to project information. Suppose you're developing a report about the project. The first sentence you write is about the aircraft's design. You need to find out if the information is classified, and, if so, at what level. You look in the TK47 Bomber Security Classification Guide. The guide indicates that the aircraft design is classified Secret. Since you include information in your sentence about the design of the TK47 Bomber, you classify your sentence Secret. Then you continue developing the rest of your report in a similar manner. What you're doing is called *derivative classification*."

"So you're saying that only OCAs can perform original classification, but people like us can *derivative classification* perform derivative classification," Josh says."

Derivative classification is the responsibility of..

- All who apply markings in accordance with classification guidance and
- All who incorporate, paraphrase, restate, or generate in new form, information that is already classified.



"Wally, you gave an example of someone applying markings in accordance with classification guidance from an OCA. Could you give an example of the other way to perform derivative classification?" Peg asks.

"Sure, Peg. Let's say you're tasked with writing an information paper about the Russian military. You discover that there is no Security Classification Guide available on the subject. However, you use several classified documents to develop your report. You have to classify your document in accordance with instructions provided by those documents. In this case, *the documents' markings are your instructions*.

"Let me give you a simple situation. Suppose document 1 contains a one sentence paragraph that says 'Russian soldiers receive 80 hours of language training every year.' The paragraph is marked (S), which indicates Secret. In your report you write 'Russian soldiers are provided 80 hours of language training annually.' The words are a bit different, but the information in your sentence is the same as the information in the sentence from document 1. Since the document 1 sentence is marked (S), you should *carry forward the classification* and mark your sentence (S).



derivative classification

"This is a simple example. Believe me, derivative classification is *not* usually an easy process. It takes time and effort and a lot of thought. We're not going to go very deep into derivative classification now. I'm saving that."

Requesting an Original Classification Decision-----

Peg says what if I come up with information I think should be protected. It's never been classified, but I don't have the original classification authority to classify it. What do I do?"

"Good question, Peg! Let's say you think the information should be classified Secret because you think it would cause serious damage to national security if unauthorized disclosure should occur. All you do is mark the information 'TENTATIVE SECRET' and *send it to an OCA with jurisdiction over the information for a classification determination*. The OCA will make a decision and notify you. You mark your document accordingly.

Derivative Classifier's Responsibility



"When OCAs classify information, they are responsible for the classifications they assign. Now, if you develop a derivative document and classify it, who do you suppose is responsible for the assigned classifications?"

"My boss?" Rudy says with an innocent look.

"That's partially true, Rudy. If your boss reviews the document and signs off on it, he or she becomes *jointly responsible* for the assigned classifications. *But you are also responsible for the classification decisions. You are the accountable classifier.*

Approver's Responsibility



"All right, we've established that if your boss reviews your derivatively classified document and signs off on it, he or she becomes jointly responsible for the assigned classifications. Suppose your boss reviews the document you derivatively classified and doesn't agree with some of the markings you've assigned. Your boss feels that the classification guidance doesn't support the markings you've assigned. What do you suppose happens?"

"I suppose my boss would tell me what markings she disagrees with and why," Josh says. "She'd have me review the guidance and re-evaluate my

decision. I'd change or remove markings to reflect the actual classification level of the information following the classification guidance for that information."

Challenges to Classification

"Right! Here's another situation. Suppose you're reading a document that someone else has classified, and you find yourself disagreeing with some of the classification markings assigned to the information. Is there anything you can do?"

"Yes, I read that E.O. 12958 encourages challenges. I could get in touch with the person who classified the document and challenge the classification," Alice says.

"Right, Alice. You could contact the classifier and give the reasons why you think that the classification should be different. Or you could talk to your security manager about it. Most of the time the situation can be handled informally. But if there's a real disagreement, every DoD Component has procedures set up for you to challenge a classification you believe to be improper. If you run into a situation of this sort, come see us in the Security Office. We'll be glad to give you a hand.

Summary

"In this session you learned that classified information is designated by the extent of the damage to national security that unauthorized disclosure would likely cause and that the Original Classification Authority (OCA) is able to identify or describe: Top Secret - exceptionally grave damage, Secret - serious damage, and Confidential - damage.

"Information becomes classified by either original or derivative classification. Original classification authority is delegated to the occupant of a position, not to a person by name. The President delegates this authority to key positions. Whoever occupies those positions may delegate authority for original classification to subordinates requiring it, and so on.



Derivative classifiers
applying markings

"OCAs are delegated authority at the highest level they may assign: Top Secret, Secret, or Confidential. OCAs must receive training before exercising their classification authority. Having identified specific kinds of information that may require protection, if the OCA 1) determines that certain information is not already classified and 2) is official government information that 3) falls within a category authorized by E.O. 12958 but that 4) is not prohibited for classification under E.O. 12958, the OCA then 5) determines the likelihood of damage to national security that can be identified or described and 6) weighs the advantages and disadvantages of classification. The OCA then 7) assigns the level of classification, 8) determines the duration of classification, and 9) communicates the decision to others by issuing classification guidance or by ensuring that information is properly marked in a document.

"Derivative classifiers apply markings following the guidance or carry forward document markings. They may challenge existing classification decisions, and if they originate information that warrants classification, they may request that an OCA review the information and make a decision regarding classification. They are responsible for the classifications they assign, and their supervisors are jointly responsible for the classifications they approve.

REVIEW EXERCISES

1. The level of classification is based on the amount of-
 - a. money that would need to be expended to mitigate the damage caused by an unauthorized disclosure.
 - b. damage that an unauthorized disclosure would cause.
 - c. foreign resources expended to compromise the information.
 - d. security resources expended to protect the information.
2. Top Secret information is information the unauthorized disclosure of which could reasonably be expected to cause _____
_____ to our national security which an OCA is able to identify or describe.
3. Original classification is:
 - a. delegated to a position, not an individual by name.
 - b. applied every time a classified document is written.
 - c. determining whether information has already been classified, at what level, and for how long
 - d. delegated to an individual by name
4. Anyone who occupies a position with original classification authority can classify information at all three levels. True. False.
5. The first step in the original classification process is to determine the current classification status of the information.

True. False.

6. The fifth step in the original classification process is to:
- determine if the information is official government information.
 - determine if the information is in an authorized category.
 - determine if the information has a prohibited intent.
 - determine the likelihood of damage to the national security and be able to identify or describe the damage.
7. In order to be eligible for classification, the information must fall within one of the seven categories listed in E. O. 12958.

True. False.

8. You are the Project Manager for the TX-22 aircraft and have been delegated original classification authority. You decide to classify the TX-22's maximum speed at the Secret level. What is the next step in your classification decision process?

- determine the amount of damage that would be caused by an unauthorized disclosure.
 - determine how long the classification should be applied.
 - determine how to communicate your decision.
 - weigh the advantages and disadvantages of classifying the information.
9. Derivative classification is:
- delegated to a position, not an individual by name.
 - applied every time a classified document is written
 - determining whether information has already been classified and at what level and for how long.
 - delegated to an individual by name.

10. Tentative classification is:

- a. classifying information that reveals an intelligence source.
- b. classifying two items because they are sensitive when related.
- c. classifying two or more pieces of information because when combined they reveal a more sensitive level of information.
- d. classifying information temporarily without having original classification authority.

11. The author of a derivatively classified document is not responsible for the classifications assigned in it if his/her supervisor signs it.

True. False.

12. If you disagree with the classification of an item, your options include:

- a. contacting the classifier and giving the reasons why you think the classification should be different.
- b. contacting your security manager about it.
- c. following the procedures that your Component has set up.
- d. a and b only.
- e. all of the above.

SOLUTIONS AND REFERENCES

1. b. (p. 2-2)
2. exceptionally grave damage (p. 2-2)
3. a. (p. 2-4)
4. False. (pp. 2-4-5)
5. True. (p. 2-6)
6. d. (p. 2-6)
7. True. (p. 2-7)
8. b. (pp. 2-9-10)
9. c. (pp. 2-11-12)
10. d. (pp. 2-12-13)
11. False. (p. 2-13)
12. e. (p. 2-14)

LESSON 3

DURATION OF CLASSIFICATION



Now that you have learned how information becomes classified, we can turn to how long it stays classified - the duration of classification. When classified information loses sensitivity over time, the restrictions on access to it - and the costs of protecting it - may be reduced or eliminated. We'll go over the factors that determine when and how information is reduced to a lower classification (downgrading) or ceases to be classified at all (declassification). At the end of this lesson, you will be able to do the following:

- State the basic policy of E.O. 12958 concerning duration of classification.
- Identify downgrading and declassification authorities.
- Distinguish downgrading from declassification.
- Describe the two types of downgrading.
- List an OCA's declassification options.
- Distinguish the declassification methods.
- Interpret downgrading and declassification instructions.
- Describe how information classified prior to E.O. 12958 is declassified.
- Describe how changes to duration are handled.
- Identify how the transfer of information affects its declassification.

Duration Policy of E.O. 12958

"Hello! Welcome to the afternoon session of our one day class. For those of you I haven't met, I'm Mike Carson with the DIVA Security Office.

"I hope you remember from this morning that one of the last things an OCA does in the original classification process is to make a decision about the *duration* of the classification. In this session we'll take a closer look at duration.

"I hope you also remember the basic classification policy of E.O. 12958 because half of it has a direct impact on duration. Who remembers the policy?" Mike Carson "Well," responds Alice Connors, "I believe ...

The basic classification policy of E.O. 12958 is...

- **Information will be classified when necessary to prevent damage to the national security, but only when necessary.**
- **information will remain classified as long as necessary, but no longer.**

"That's right, Alice. The second statement gives us the duration guidance. Once disclosure of the information no longer puts our national security at risk, the information shouldn't remain classified. I'm sure you remember that E.O. *12958 promotes declassification and public access to information as soon as national security considerations permit.*"

"Let's first identify the people in the DoD who have *declassification and downgrading authority*. They are...

Declassification and Downgrading Authorities in DoD

- * The Secretary of Defense
- * The Secretaries of the Military Departments
- * The original OCA or that OCA's successor
- * Other designated officials who can exercise declassification and downgrading authority over classified information in their functional areas of interest

Downgrading vs. Declassification -----

"All right, now let's see how an assigned classification may be ended. There are two ways: through *downgrading* and *declassification*. Does anyone know what downgrading is?"

Sparky Chang spoke up. "I think that ...

Downgrading is lowering the classification from one level to another.

TOP SECRET information may become SECRET or CONFIDENTIAL. SECRET information may become CONFIDENTIAL.



Sparky Chan

"That's right, Sparky. Notice that Sparky used the word 'lowering.' That's a key word. With downgrading the level of classification is lowered, not eliminated. When information is downgraded, it *remains classified*,

"Now let's define declassification. Sparky, you did such a good job defining downgrading, how about trying this one?"

"Sure, I'll take a stab at it.

Declassification is a determination that classified information no longer requires protection in the interest of national security.

"Two for two! When information no longer requires protection in the interest of national security, it no longer needs to be classified. Classification is *eliminated*."



Rudy Tucker

"So what you're saying," Rudy Tucker says, "is that when information is declassified, it's no longer identified as 'Top Secret,' 'Secret,' or Confidential.' But if information is downgraded, it still carries a classification designation."

"That's right, Rudy. And that's a good way to summarize the difference between the two terms.

Downgrading

"We said that downgrading means lowering the classification from one level to another. How does an OCA *communicate downgrading instructions* to holders of classified information? Well, on classified documents or materials...



Josh Smith

Downgrading instructions usually appear as:

"Downgrade to (level) on (date or event)"

"Note that an OCA can specify a *date* or *event* for downgrading in the process of original classification. Now, using this format, can anyone give us sample downgrading instructions?"

Josh Smith says, "Sure. Let's say it's December 1, 1998. An OCA classifies some information Secret. At the same time, the OCA determines that the information can be downgraded to Confidential in two years. So the downgrading instructions are 'Downgrade to Confidential on December 1, 2000.'"

Automatic Downgrading-----

"Josh says that an OCA determined that some information should be downgraded to Confidential on December 1, 2000. Come December 1, 2000, the information is downgraded. This is called *automatic downgrading*. When information is downgraded in accordance with originally determined downgrading instructions, the OCA *does not have to notify holders of the information*. The markings themselves take care of that."

Downgrading Upon Reconsideration-----

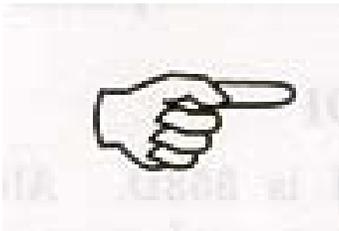
"Suppose an OCA classifies some information as Secret and *doesn't assign any downgrading instructions* to it," Josh says. "Then, *at a later date*, the OCA reviews the information and figures that it can be downgraded to Confidential. What happens?"

"Good question, Josh. We call the situation you described *downgrading upon reconsideration*. The OCA can issue the downgrading instructions but *must notify all known holders of the information.*"

AUTOMATIC DOWNGRADING vs. DOWNGRADING UPON RECONSIDERATION		
TYPE	EXPLANATION	NOTIFICATION REQUIRED?
Automatic	OCA issues downgrading instructions at the time information is originally classified. These original instructions are carried out.	No
Upon Reconsideration	OCA does not issue downgrading instructions at the time information is originally classified. Downgrading instructions are issued at a later time.	Yes

Declassification

"Wally told you that when information is originally classified, an OCA must determine when that information will be declassified," Mike says. "Well, there are exceptions to that rule. For instance,



Declassification instructions are not applied to Restricted Data and *Formerly Restricted Data*. The Department of *Energy* determines when Restricted Data will be declassified. Declassification of *Formerly Restricted Data* takes a joint determination by *DOE and DoD*.

"So if I pick up a document that contains Restricted Data, I won't see any declassification instructions on the front of the document?" asks Peg Brown.

"That's right, Peg. And while we're on the subject, let me show you how declassification instructions appear on the front of a document."



Peg Brown

Declassification instructions usually appear as:

"Declassify on: (option)."

"What do you mean by 'option'?" Peg asks.

"When OCAs determine declassification instructions, they base their decisions on predictions about loss of *the information's sensitivity*.

An OCA's declassification options are:

- * **A specific date within 10 years**
- * **A specific event likely to occur within 10 years**
- * **10 years from the date of classification**
- * **Exempt from the 10-year rule.**

"This means that declassification instructions on a document that was created on 12 June 1997 could appear as:

- Declassify on: April 12, 1998 (specific date)
- Declassify on: Completion of operational testing (event)

- Declassify on: June 12, 2007 (10 years from the date of classification)
- Declassify on: X - (where the blank is filled in with a number from Section 1.6d of the Executive Order - one of the exemption categories)

"Mike, I understand about determining a date or event for declassification. But could you explain a bit more about this 'exempt' stuff " Pegs asks.



"Sure, Peg. We hope that much of the time OCAs will be able to set specific dates or events for declassification. But we know that there will be a lot of cases where they just can't predict the future well enough to do that. And there will be a good bit of information that will still be sensitive even after ten years have passed. That's why the Executive Order has a provision for OCAs to *exempt* information they classify from the 10-year limitation. *Only certain categories of information can be exempted. They're listed in Section 1 6 of the Executive Order and also in paragraph 4-202b of DoD 5200. I-R.*

"So that's what the X's mean. *They show that information has been exempted from the 10-year limitation, and the number shows the category of exemption that applies. OKT'*

Josh pipes up. "Yeah, but doesn't that mean the information will stay classified *forever?* I mean, it won't have a declassification date on it, right?"

"Right, Josh. No date. And if following the markings on the front of the document were the *only* way information ever got declassified, the exempted information would just stay classified forever. But it's far from being the only way, Josh.

Methods of Declassification

"There are five ways that information ends up being declassified," Mike says.

Methods of Declassification

- * **Scheduled**
- * **Automatic**
- * **Re-evaluation**
- * **Systematic Review**
- * **Mandatory Review**

Scheduled



"Scheduled declassification occurs if, at the time the information is originally classified, the OCA is able to set a date or event for declassification. The information is then scheduled to be declassified on that date or when the event occurs. How about an "Sure," says Sparky. "On January 15, 1997, an OCA determines that information is to be declassified on January 15, 2001. Four years pass and on January 15, 2001, the information is declassified. Simple."

Automatic

"Right. Now the second way the information is declassified is something brand new in this new Executive Order: *automatic declassification*. The Order sets up a system to declassify information in *permanently valuable records* when the records become *25 years old*."

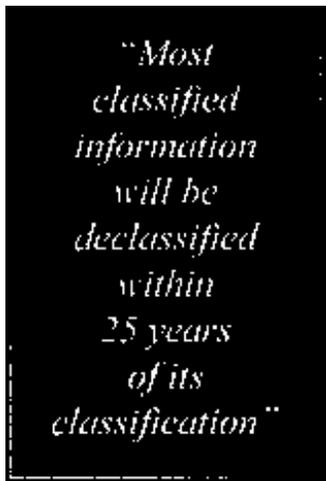
"Permanently valuable records are defined by law -*the Federal Records Management Act*. Our records management folks are responsible for identifying those records here at DIVA.

"The important thing about this '25-year rule' is that it is *automatic*. Permanently valuable records are automatically declassified when they become 25 years old, *unless* an *agency head* designates them to be kept classified more than 25 years. In the whole Department of Defense, there are *only four agency heads*: the Secretary of Defense and the Secretaries of the Army, Navy, and Air Force. Four people! So you can see that the intent of this new Executive Order is that *most classified information will be declassified within 25 years of its classification*."

"Wait a minute!" Eddie Cramer breaks in. "Isn't there a danger that we'll declassify something 25 years old that should still *stay classified*? Couldn't something slip through the cracks of this exempting business?"

"There is that possibility, Eddie. In fact, it's bound to happen sooner or later. But the decision to set up the 25 year rule was based on an idea called *risk management*. The President's decision, as implemented in the Executive Order, was that the risk of something slipping through the cracks at 25 years was an acceptable one, when balanced against the benefits of getting those masses of old information declassified. And 25 years is a long time. Heck, Eddie, some of the people in this room weren't even born 25 years ago!

"While we're on the subject of this 25-year, automatic declassification, let me tell how an exemption would look on the 'Declassify on' line of a document. *Documents exempted by an agency head*



"Most classified information will be declassified within 25 years of its classification"

'25-year rule'

from the 25-year rule will be marked, '25X,' along with a number."



"Kinda like the Xs and the 10-year stuff." Peg remarks.

"Exactly, Peg. And the numbers after the 25X's show the same thing - the *category of exemption* the information falls in. Yes, there's a list of categories eligible for exemption from the 25-year rule, too!

But let's not worry about the 10-year and 25-year exemption categories now. They're in the regulation if you need to look them up.

"The other thing you'll see on material marked with a '25X' is a *declassification date*. When an agency lead exempts records from the 25-year rule, he or she has to set a declassification date for the records.

There's one exception: information about *human intelligence sources* or *confidential human sources* doesn't have to have the date assigned. So you'll see some '25X' material without a declassification date. It will be marked '25XV' "All right, review time! So far, we've looked at

Scheduled declassification:

The original classifier sets a date or event within 10 years for declassification, or designates the information as being exempt from the 10-year limitation. If a date or event is set, the information is declassified at that time.

Automatic declassification:

Information in permanently valuable records which is still classified after 25 years is automatically declassified on the 25th anniversary of its classification unless an agency head exempts it from the 25-year rule.

Re-evaluation



Original Classification Authority

"It's possible that changes in circumstances may remove the need for a piece of information to be classified. Suppose classified information is *compromised*. An OCA, or the OCA's successor, is responsible for re-evaluating the information to see if it should be declassified.

"Perhaps the classified information becomes *obsolete*. For example, suppose an OCA determined that the fact Weapon ABC doesn't work well in the rain should be classified Secret. Since the OCA could not determine a date or event for the declassification of this information, it was designated as exempt from the 10-year rule. As the system evolves, changes are made and it works just fine in the rain. Upon re-evaluation, the OCA should declassify the piece of information.

Systematic Review



'systematic review for declassification.'

"Information generated within DoD and declared permanently valuable is provided to the *National Archives and Records Administration (NARA)*. Some permanently valuable information is classified. So we have a program called '*systematic review for declassification*.' Under this program classified, permanently valuable records are reviewed for declassification after they reach a specific age.

"DoD Components have systematic review programs too. Sometimes, these are focused on specific types of information - like records from the Gulf War."

"I've got a question," Josh says. "If the DoD provides information to the NARA, shouldn't the DoD be involved in its declassification?"

"The DoD is involved, Josh. Information provided by DoD will be reviewed *according to guidelines provided by DoD*. If declassification is questionable, the DoD Component that has classification jurisdiction over the information is asked to make a decision about declassifying."

Mandatory Review-----



request for mandatory review
for declassification

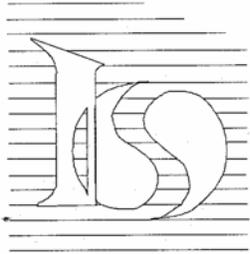
"The fifth method of declassification is *mandatory review*. Let's suppose we're all working on a classified project. We'll call it 'Project Wingo.' Project Wingo concerns the computer system of the future. While it's no secret that Project Wingo exists, no one really knows much about it since most of the information is classified.

"So we're all working on the project. Then one day, we get a letter from Mr. John Q. Public of Ames, Iowa. Mr. Public wants some information concerning Project Wingo. He knows that the information in a specific document he wants is classified. But he wants DIVA to review the information to see if it can be declassified and made available to the public.

"Mr. Public has made a *request for mandatory review for declassification*. When such a request is made the originating agency *must* respond to it in a timely manner."

Request for Mandatory Declassification Review

- *Anyone **can** request an originating agency to review specific information for declassification.*
- *The originating agency must respond to the request **within 60 calendar days (45 working days) and, if the response does not state that the information will be declassified, the agency can take no more than an additional 120 calendar days to provide the requester a final determination.***



Information Security
Oversight Office



"How often does the DoD grant a request for declassification made under mandatory review?" asks Alice.

"Well, according to the Information Security Oversight Office's 1995 *Annual Report to the President*, in Fiscal Year 1995, the DoD acted upon 2,005 cases processed under mandatory review requests. 54% of the cases resulted in full disclosure of the information, 34% were granted in part, and 12% were denied in full."

"What happens if a request for information is only partially granted or denied in full?" Josh asks.

"The originating agency must provide a *brief exploitation to the requester* of why the information cannot be granted in full or at all. The requester *can appeal* the decision to the Interagency Security Classification Appeals Panel (ISCAP)."

"Is all classified information eligible for mandatory declassification review?" Josh asks.

"No, Josh. Certain high-level information is exempt from it."

Information Exempt from Mandatory Declassification Review
Information originated by a President; the White House staff; committees commissions or boards appointed by the President; or others specifically providing advice and counsel to a President or acting on behalf of a President is *exempt* from mandatory review for declassification.

Foreign Government Information

"Now that we've looked at the five methods of declassification, let's turn to the declassification of *foreign government information*. Some of you may be involved in working with classified documents that contain classified foreign government information.

DoD documents that contain classified foreign government information are *not* assigned a date or event for declassification unless specified by or agreed to by the foreign government.

"Any request to declassify foreign government information is referred to the foreign government for determination.

Information Classified Prior to E.O. 12958



"So far we've talked about information classified under E.O. 12958. It became effective on October 14, 1995. What about information that was classified *before October 14, 1995*? How is it declassified? It's pretty simple. If there's a *date* or *event*, go by that. If there's no date or event, the 'Declassify on' line on these documents usually reads 'Source marked OADR' or 'Declassify on: OADR ' ' If not, *consider it marked OADR*. You don't have to actually mark it OADR. '*OADR*' is a marking authorized under the previous Executive Order and means, '*Originating Agency's Determination Required 'to declassify.*'"

Information Classified Prior to October 14, 1995

- * If the information bears a date or event for declassification, declassify the information on the date specified or *when the* event happens.
- * If the information does not have a date or event for declassification, treat the information as *if it were marked OADR*.

Note the following:

- * A "Review On" date is not a declassification date. Information covered by a "Review On" marking must be treated as *OADR*.
 - There is no requirement to remark old documents as OADR. Just treat them as *if they were marked OADR*.

Changes to Duration

"When we talked about methods of declassification, we saw that through re-evaluation and systematic and mandatory reviews, classified information may become declassified earlier than originally anticipated. Let's discuss what happens when the duration of classification changes."

Notification of Changes

The rule when there is a change in the original duration instructions is as follows:

If duration instructions change in any way all known holders of the information must be *notified*.

Regrading Classified Information-----



"Suppose," Mike begins, "it is 14 April 1999 and you are working with a Secret document. You are notified that the document is to be *downgraded to Confidential* on 20 May 1999. What should you do?"

"On 20 May 1999 I'd *cross out the current classification markings and write in the new ones*," says Rudy.

"That's right. And if you were notified instead that the document was to be *upgraded to TOP SECRET* on 20 May 1999, you'd cross out the markings and write in the new ones on that date. In either case, there are a few other things you need to do. You've got to indicate what gives you the *authority* to change the classification, the *date* of the action, and your *name*. This whole process is called *regrading*."

To regrade a document, you should mark it conspicuously to show..

- **All applicable changes**
- **The authority for the action**
- **The date of the action**
- **The identity of the person taking the action**

Extending Downgrading and Declassification Instructions-----

"I understand what happens when instructions are changed so that information is downgraded or declassified *earlier* than originally anticipated," Rudy says. "But suppose an OCA determines that a particular piece of information should be declassified on 1 June 1998. As 1 June 1998 approaches, it appears that the information should not be declassified on that date, but *later on*. What happens?"

"Good question, Rudy.

Extension of downgrading or declassification instructions can take place only if all known holders of the information can be notified of the extension before the originally set date or event.

Transferred Documents or Materials



"Information originally classified by one Federal department or agency, or DoD Component often ends up in the hands of another department, agency, or DoD Component. Sometimes the information is transferred for *official reasons*. Other times, the information is transferred for *storage purposes*. And sometimes, a department, agency, or DoD Component *ceases to exist*. The originally classified information these operations generated has to end up somewhere. Let's see how each of these situations impacts declassification."

Officially Transferred

"For information that is *officially transferred by directive, statute, or executive order...*

The receiving department agency or DoD activity becomes the original classifying authority over such material for purposes of downgrading and declassification.

"Can someone give me an example?"

"I'll try," says Peg. "How about if the folks at Andrews Air Force Base are working on a classified

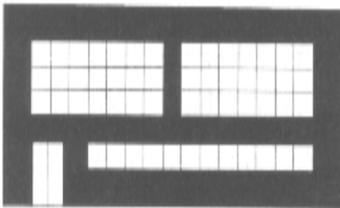
project. Some people here at DIVA are involved. Someone decides that DIVA should take over the project, so all documents and materials are transferred here. DIVA is then responsible for ensuring that the classified information is downgraded or declassified."

Not Officially Transferred

"Great example, Peg! Of course not all information is transferred for official reasons. Sometimes a DoD Component comes into possession of classified information for 'unofficial' reasons. In such cases

The *DoD* activity becomes the *originating agency* for the purpose of declassifying or downgrading such information or material if.

- The information is not officially transferred to another department or agency.
- It is impossible to identify the originating agency.



DIVA
Defense Interoperability
Validation Agency

"I've got a question, Mike," says Rudy. "Suppose some of this unofficially transferred information finds its way into DIVA. But DIVA figures that another department, agency, or DoD Component may be interested in the information. What should DIVA do?"

"If DIVA feels that another department, agency, or DoD Component may be interested in the information, DIVA must get in touch with the organization. DIVA must tell them the *nature of the information* and its *intention to downgrade or declassify the information*. **DIVA will not** declassify or downgrade the information *for a period of time, usually 60 days after notification*. During this period, the other department, agency, or DoD

Component may express objections to the downgrading or declassification,"

Transfer for Storage or Retirement



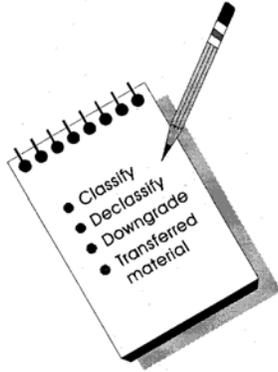
"One final word regarding transferring information. If your component is transferring classified documents or materials to a *Records Center* for storage or to the *NARA* for permanent preservation, *review* the material for downgrading or declassification *before transferring*."

"Before we wrap up, I'd like to thank each of you for attending. And best of luck at DIVA. If you need help on any security matters, please call me."

Summary



"In this session, we covered the duration of classification. We noted that most information should be classified no longer than 10 years and that it may be downgraded or declassified at any time by the OCA. Only certain DoD officials have declassification and downgrading authority. We defined downgrading as lowering the classification from one level to another. Automatic downgrading is lowering the classification level as the OCA instructed at the time of original classification. The OCA may instead downgrade upon reconsideration and issue instructions to all known holders. Declassification is a determination that classified information no longer requires protection in the interest of national security. Based on projected loss of sensitivity, the OCA may decide that the information will be declassified on a date or event within 10 years, 10 years from the date of classification, or that it is exempt from the 10-year rule. The Department of Energy determines when



Restricted Data and Formerly Restricted Data can be declassified since that information is covered under the Atomic Energy Act. We noted five methods of declassification. Scheduled declassification occurs upon the date or event the OCA specified at the time of classification. Permanently valuable records are automatically declassified after 25 years unless exempted by an agency head. Compromised, obsolete, or other information that may have lost its sensitivity may be declassified upon re-evaluation. Permanently valuable DoD classified information is systematically reviewed for declassification. Anyone may request a mandatory review for declassification by the originating agency. Requests to declassify a foreign government's information are referred to that government. U.S. information classified before E.O. 12958 took effect and without a specified date or event for declassification was considered marked OADR under President Reagan's E. O. 12356. You learned that if duration instructions change in any way all known holders must be notified. Documents to be downgraded or upgraded earlier than scheduled must be regraded. Downgrading and declassification instructions may be extended only if all known holders can be notified before the date or event originally set. For officially transferred material, the receiving element becomes the original classifying authority for the purpose of downgrading or declassifying. For unofficially transferred material, the DoD Component becomes the originating agency for duration decisions if it cannot identify the originating agency or if it does not officially transfer the information to another agency. Records to be transferred for storage or preservation are first reviewed for downgrading or declassification."

REVIEW EXERCISES

1. What is E.O. 12958's basic policy concerning the duration of classification?

2. General Davis was the Director of DIVA prior to General Kent. Who has downgrading and declassification authority over the information General Davis originally classified?

3. What's the difference between downgrading and declassification?

4. a. An OCA classifies some information Top Secret but does not assign any downgrading instructions to the information. A year later, the OCA reviews the information and determines that it can be downgraded to Secret. This is called: _____

- b. _____ is when classified information is downgraded in accordance with its original instructions.

5. What are an original classifier's four options for declassification?
 - a. _____
 - b. _____
 - c. _____
 - d. _____

6. Match the methods of declassification with the descriptions.

	Methods		Descriptions
a.	Mandatory	__1.	Declassification instructions say that information should be declassified on 1 Jun 98.
b.	Re-evaluation		The information is declassified on 1 Jun 98.
c.	Scheduled		
d.	Systematic	__2.	Information is compromised and it's determined that the information should be declassified.
e.	Automatic		
		__3.	A program primarily administered by NARA.
		__4.	Information is declassified as a result of an inquiry from an individual.
		__5.	Review of information shows it should be declassified because it's obsolete.
		__6.	A 25-year old permanently valuable record becomes declassified.

7. A classified document contains Restricted Data. What impact does this have on declassification?

8. Interpret the following declassification instructions:

- a. Declassify on: X3
- b. Declassify on: 1 August 1998
- c. Declassify on: deployment of Company A to Saudi Arabia

9. A U.S. classified document contains classified information from the Government of France. The Government of France should be consulted before declassifying its classified information.
- True False
10. You are working with a classified document. It is dated July 9, 1978. It does not have any declassification instructions. As far as declassification is concerned, how should you treat the information in the document?
11. It's October 2, 1997. You're working with a Secret document that is to be downgraded to Confidential on September 30, 1999. You receive notice that the downgrading instructions have changed. The new downgrading instructions say "Downgrade to Confidential on September 30, 1998." What do you do?
12. Fort Carson receives a presidential directive to transfer some classified information to DIVA. Once the information is transferred, DIVA becomes its downgrading and declassification authority.
- True False
13. DIVA inherits information originally classified by an agency that no longer exists. DIVA feels Fort Belvoir might be interested in the information. Most of the information is due to be declassified within 2 months. What should DIVA do?

SOLUTIONS AND REFERENCES

1. E.O. 12958's basic policy concerning duration is that information should remain classified as long as necessary, but no longer. (p. 3-2)
2. Since General Kent is General Davis' successor, General Kent is the declassification and downgrading authority. Remember, authority is delegated to a position, not a person. (p. 3-3)
3. In downgrading, the classification is lowered; in declassification, classification is eliminated. (pp. 3-3-4)
4.
 - a. Downgrading upon reconsideration
 - b. Automatic downgrading (pp. 3-5-6)
5.
 - a. A specific date within 10 years
 - b. A specific event within 10 years
 - c. 10 years from the date of classification
 - d. Exempt from the "10-year rule" (p. 3-7)
6.
 1. c
 2. b
 3. d
 4. a
 5. b
 6. e (pp. 3-9-14)
7. If a document contains Restricted Data, declassification instructions will not be placed on the document. (pp. 3-6-7)
8.
 - a. The information is exempt from the "10-year rule."
 - b. Declassify the information on August 1, 1998.
 - c. Declassify the information when Company A is deployed to Saudi Arabia. (pp. 3-7-8)
9. True. (p. 3-15)
10. For information classified prior to October 14, 1995 - the date on which E.O. 12958 was implemented - and without declassification instructions, you should treat the information as though it were marked OADR. (p. 3-15)

11. You remark it. You replace the old downgrading date with "30 Sep 98." On the front of the document you put your name as the person who made the change, the date you made the change, and a notation stating the authority that authorized the change. (p. 3-17)
12. True. (p. 3-18)
13. DIVA must tell Fort Belvoir about the information. DIVA must also tell Fort Belvoir that the information is to be declassified within 2 months. DIVA will not take any action regarding downgrading or declassification for 60 days after it notified Fort Belvoir. (p. 3-19)

LESSON 4

MARKING CLASSIFIED INFORMATION



How do we let people know that they are working with classified information? We mark it, of course. But, as you probably know, marking is not as simple as stamping Top Secret, Secret, or Confidential on a document. In this lesson, we'll go over the basics of marking documents and other materials that contain our country's classified information. We'll also discuss how we deal with classified information received from foreign governments and international organizations such as NATO. At the end of this lesson, you will be able to do the following:

- * Explain why classified information is marked.
- * Apply required markings to classified documents.
- * Apply required markings to NATO and foreign government information.
- * Apply required markings to classified materials other than documents.

This lesson contains no classified information. All sample documents contain hypothetical information only. All security markings are for illustration and training purposes only.

Why is Classified Information Marked?

Anne Perkins, Deputy Chief of the Security Branch at the Defense Interoperability Validation Agency (DIVA), drops by Hawk Pearson's office to see if he needs a ride home. They carpool to work, but this morning Hawk came in early to finish a report.



"Hi, Hawk. How's the report coming along?"

"Just four pages to go. Marking is really tedious! I know that it's important to alert users that they are working with classified information, Anne. A document with, say, 'TOP SECRET' stamped on it tells me I have to protect it. It's the other things that don't seem worth all the bother."

"Well, Hawk, consider the value of portion markings. Without the portion markings in that document you're working from, you wouldn't know which parts are classified and which aren't, let alone their levels of classification! "And the markings on a document's face can tell you a lot besides its overall classification. You'll find out if there are any special controls, such as reproduction or dissemination limitations. You'll learn if there are any special safeguarding requirements. If it's an originally classified document, you can learn who the OCA was by looking at the 'Classified by' line. If it's a derivatively classified document, you can find out from the 'Derived from' line what classified

document, security classification guide or other classification guidance provided the classification information. And you can see when protection requirements change from the downgrading and declassification instructions. The next time you're feeling worn out by marking, refer to this chart. It can't take the drudgery out of marking, but it will remind you of the importance of what you're doing!"

Markings serve to ...

- Alert the user that something is classified.
- Tell the user the degree of protection required.
- Specify what portions of a document contain or reveal classified information.
- Identify who classified the information or what source the author used to get classification guidance.
- Show the reason for the classification of the information.
- Provide instructions on how long the information is classified.
- Give notice of special controls and safeguarding requirements.

"I guess markings do serve many important purposes, Anne. Well, I'd better get this document done by 4:30 or instead of riding with you I'll be walking home!"

Let's leave Anne and Hawk to their transportation arrangements and review how information becomes classified. It's important to know this because it impacts certain marking requirements.

Original and Derivative Classification

You should recall from Lesson 2 that

- Is the *initial determination* **that a piece of information needs to be classified.**
- **Can be performed only by a designated Original Classification Authority (OCA).**



General Kent

Do you also recall that General Kent, DIVA's Director, is the OCA for all information originally classified at DIVA? And that in his absence, Captain Douglas, DIVA's Deputy Director, is designated original classification authority? And that other DIVA employees derivatively classify information? In fact, within the Department of Defense derivative classification is done much more often than original classification.

Derivative classification is performed when a person...

- **Pulls information out of classified documents and materials -reports, information papers, maps, photographs, etc. - and creates a different classified document.**
- **Classifies information in accordance with guidance provided by an OCA and so marks the document or whatever is being created.**

We'll have much more to say about derivative classification in the next lesson.

Basic Security Markings



Mike Carson

We'll look first at the markings that are needed for any classified document. Let's listen in as Mike Carson, a security specialist with DIVA, explains the basics of marking a classified document to Doris Duncan of DIVA's Weapons Systems Division.

"Mike, thanks in advance for your help. I finally finished putting together that document we spoke about. Now I need your help with marking it."

"I'm glad you called, Doris. So many people plunge head first into the marking process without knowing anything about it. Improperly marking a Mike Carson document can cause all sorts of problems. We'll start with the basics and move on from there. And speaking of the basics, let me give you this." Mike pulls a piece of paper from a folder he's carrying.

CLASSIFICATION MARKINGS	
Unabbreviated marking	Symbol
TOP SECRET	(TS)
SECRET	(S)
CONFIDENTIAL	(C)
UNCLASSIFIED	(U)

What Must Be Marked?

"Before we begin marking your document, though, let's look at what parts of your document require markings.

The following parts of a document must be marked...

- * Portions**
- * Interior pages**
- * First page**
- * Title page (if it exists)**
- * Front and back covers (if they exist)**

Marking a Classified Document

"I'm ready, Mike. My document has two pages and a cover. Since the cover's on top let's start there."

"Sorry, Doris. I know the cover *seems* like a logical place to begin. But we can't completely mark the cover until we've marked the rest of the document! So we're going to mark the document *from the inside out*. We'll mark the document's *portions* first, then

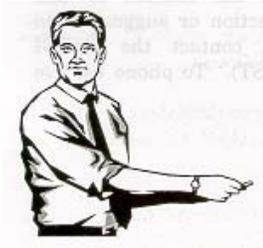
its *interior pages*, then its *first page*, and then, finally, its *cover*."

"I don't get it, but I'm ready when you are."

Marking the Portions-----

"All right, the first parts of any classified document that must be marked are the *portions*."

"Sounds like a recipe," Doris says. "What's a 'portion'?"



Portions are small segments of information. They include:

- * **Paragraphs**
- * **Subparagraphs**
- * **Illustrative material (charts, graphs, photos, etc.)**
- * **Captions of illustrative materials**
- * **Headers of major sections**
- * **Title and subject line of document**

"Got it. I've got lots of portions in my document."

"You've probably picked up some ideas concerning portion marking by working with other classified documents," Mike says. "But here's something that spells out a lot of the requirements in a handy format." Mike hands Doris the table shown on the next page.

PORTION MARKING REQUIREMENTS
DoD 5200.1-R

PORTION	MARKING	PLACEMENT	ADDITIONAL INFORMATION
Paragraph	Symbol	Between the paragraph number (or letter) and the paragraph or immediately to the left of the paragraph	Mark each paragraph in a classified document.
Subparagraph	Symbol	Between the subparagraph number (or letter) and the subparagraph or immediately to the left of the subparagraph	You are not required to portion mark subparagraphs if they are of the same classification level as the paragraph that leads into them. Subparagraphs should always be marked when there is a need to eliminate doubt about their classification.
Illustrative Material	Unabbreviated	Within or next to illustrative material	Mark each illustration in a classified document,
Captions	Symbol	Between the caption number (or letter) and the caption or immediately to the left of the caption	Captions are marked based on the content of the caption (not the content of the illustrative material).
Header	Symbol	Immediately to the left	Normally, a portion mark is not required for a header unless it contains or reveals classified information. However, when one or more headers in a document requires marking, all headers should be marked.
Title of document or subject line	Symbol	Immediately to the right	Always mark a classified document's title and/or subject line.

"Keep in mind that the chart contains the minimum markings required by *DoD 5200. 1-R, Information Security Program*. DIVA uses only these markings, but other DoD components have additional requirements. O.K. Now we need the classification of the information in each portion."

"I've already done that! Last week, you suggested..."

When creating a derivatively classified document you should keep track of the appropriate classifications as you develop it.

"Good! Many people put their documents together, then have to go back through their source documents to determine the classification level of the information in each portion. They double their work! Let's look at your classification levels."



- The subject is Unclassified.
- The first header is Confidential.
- Paragraph 1 is Unclassified.
- Subparagraph La. is Confidential.
- Subparagraph Lb. is Unclassified.
- Figure 1 is Confidential.
- Figure 1's caption is Unclassified.
- The second header is Unclassified.
- Paragraph 2 is Confidential.
- Subparagraphs 2.a. and 2.b. are Confidential.
- The third header is Unclassified.
- Paragraph 3 is Confidential.
- Subparagraphs 3.a. and 3.b. are Secret.

"Looks good, Doris. Now use the table to mark the portions of your document."

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

LASER WIDGET FIELD TEST (U)

13 January 1997

DEFENSE INTEROPERABILITY VALIDATION AGENCY
4719 DORCHESTER STREET
SPRINGFIELD, VIRGINIA 22150

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

13 January 1997

SUBJECT: Laser Widget Field Tests (U)

(C) THRUST CONVERGENCE DEMONSTRATION

1. (U) Field test conducted on November 25, 1995 at Site B confirm thrust convergence of laser widget propulsion system.
 - a. (C) Thrusts were achieved by employing multiple widgets in the octagonal design configuration (Mode C).
 - b. (U) Figure 1 indicates thrust exerted at varying angles on incidence.

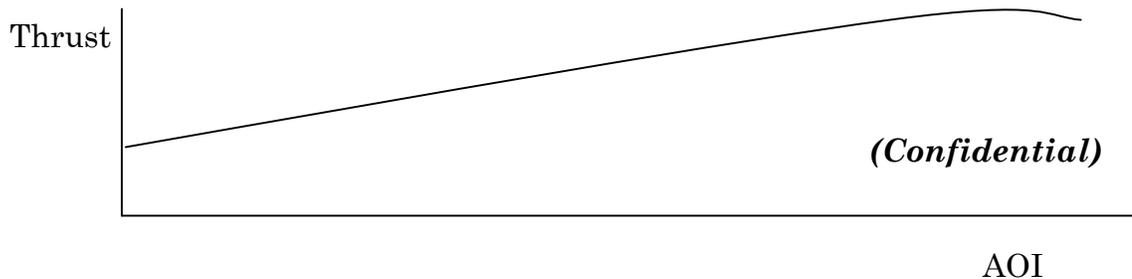


Figure 1. (U) Static Range Data

CALIBRATION RECOMMENDATION

2. (C) Recommend that system be calibrated for countermeasure as follows:
 - a. (C) Electro-optical susceptibility was noted at 43° to 67° angle of incidence
 - b. (C) Directed energy susceptibility was noted at 23° to 36° angle of incidence.

SUBJECT: Laser Widget Field Tests **(U)**

(U) THRUST OFFSET

3. **(C)** Field test conducted on December 2, 1995 at Site confirm thrust offset of 35 modulated tones.

- a. **(S)** offsets were delineated by the design configuration of Nodal G.
- b. **(S)** The offsets will vary according to the angles.



"Perfect! Your markings make clear which portions contain or reveal classified information and their levels of classification. You focus on each portion in itself, not as it relates to associated information. For example, you marked the lead-in portions of paragraphs 1 and 3 according to their information's level of classification, not according to the level of classification of the information contained in the sub-paragraphs. There are two other things you should know about portion markings, Doris...

- If every portion in a document is classified at the same level, you need not mark each portion. Include a statement that alerts a user that all portions are at a particular level.
- Sometimes portions contain information that falls into a special category or is subject to additional controls. If so, the portion marking must show this. For example, a portion containing Secret Restricted Data is marked (*S-RD*).

"Here's another table. It shows the **full warning** notices placed on the face of the document as well as the applicable portion markings.

WARNING NOTICES and CONTROL MARKINGS

OVERALL DOCUMENT MARKING	MARKING
<p style="text-align: center;">RESTRICTED DATA</p> <p>This material contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions.</p>	<p>(Classification-RD) EXAMPLE: (S-RD)</p>
<p style="text-align: center;">FORMERLY RESTRICTED DATA</p> <p>Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination. Section 144.b., Atomic Energy Act, 1954.</p>	<p>(Classification-FIRD) EXAMPLE: (S-FRD)</p>
<p style="text-align: center;">Critical Nuclear Weapons Design Information. DoD Directive 5210.2 applies. (CNWDI)</p>	<p>(Classification-RD)(N) EXAMPLE: (S-RD)(N)</p>
<p style="text-align: center;">DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR</p>	<p>(Classification-OC) EXAMPLE: (S-OC)</p>
<p style="text-align: center;">CAUTION-PROPRIETARY INFORMATION INVOLVED</p>	<p>(Classification-PR) EXAMPLE: (S-PR)</p>

Marking Interior Pages-----

“Now let’s mark the pages, Doris”

For marking purposes, a page...

is *one side of a sheet of paper that contains information*. If a side of paper is *blank*, for purposes of marking, it is *not* considered a page.

“First, we’ll mark all of the *interior pages*. An interior page is *any page other than the first page or the title page* (if you have a title page.)

To mark an interior page...

Conspicuously display at the *top and bottom* of the page the *unabbreviated marking* for the *highest level of classified information on the page*. The marking should stand out and be noticeable.

“Page 2 of your document is your only interior page. How would you mark it?”

“The highest level of classified information on page 2 is Secret, so I’d mark it ‘SECRET’.”

“That’s right. Go ahead and mark the page.”

Doris marks page 2 of her document as shown on the next page.

SECRET

SUBJECT: Laser Widget Field Tests (U)

(U) THRUST OFFSET

3. (C) Field test conducted on December 2, 1995 at Site confirm thrust offset of 35 modulated tones.

- a. (S) Offsets were delineated by the design configuration of Nodal G.
- b. (S) The offsets will vary according to the angles.



SECRET

Overall Classification Markings

"Since you have just the one interior page, we can start to put the *overall document classification markings* on the proper places. The overall document classification is the *highest classification of information contained in the document*.



The highest classification of information in a document must be marked on the

- front cover, if any.
- title page, if any.
- first page.
- outside of the back cover, if any.

Marking the First Page

"Since we're working 'inside-out' with this document, I suppose we go next to the first page."

"Right, Doris. If a document has no front cover, the 'first page' will be the front page. If it has a cover, the 'first page' is the first page you see when you open the cover. The title page and the 'first page' may be the same. *All documents have a 'first page,' but not all documents have a cover or a title page,*"

Doris marks the first page as follows.

SECRET

13 January 1997

SUBJECT: Laser Widget Field Tests (U)

(C) THRUST CONVERGENCE DEMONSTRATION

1. (U) Field test conducted on November 25, 1995 at Site B confirm thrust convergence of laser widget propulsion system.

a. (C) Thrusts were achieved by employing multiple widgets in the octagonal design configuration (Mode C).

b. (U) Figure 1 indicates thrust exerted at varying angles on incidence.

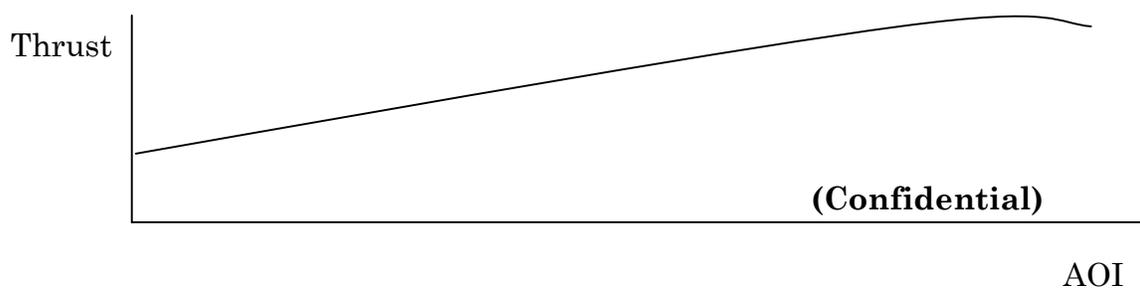


Figure 1. (U) Static Range Data

(U) CALIBRATION RECOMMENDATION

2. (C) Recommend that system be calibrated for countermeasure as follows:

a. (C) Electro-optical susceptibility was noted at 43° to 67° angle of incidence

b. (C) Directed energy susceptibility was noted at 23° to 36° angle of incidence.

SECRET

"Correct again! Even though your first page does not contain any Secret information, you knew that you still must put the marking for *the highest classification of information contained within the entire document on the first page*. We do this so anyone intending to read the document will know as soon as they look at the first page that the document contains Secret information.

Marking Title Pages



"Now, Doris, let's do the cover. But before we do that let me ask you this. If your document had a *title page*, how would you mark it?"

"I would put the *overall document classification marking* on it, regardless of the level of classification of the information actually on the title page itself. That's so the reader would be warned that the document contains that level of classification of information."

"Very good, Doris, now let's mark your cover."

Marking Covers

"Remember, not all documents have covers. Some documents are only one page. Some documents are simply multiple pages stapled together. Since you have chosen to put a cover on your document, Doris, the *overall document classification marking must be placed on the cover*."

Doris marks the cover as follows.

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

SECRET

LASER WIDGET FIELD TEST (U)
13 January 1997

DEFENSE INTEROPERABILITY VALIDATION AGENCY
4719 DORCHESTER STREET
SPRINGFIELD, VIRGINIA 22150

SECRET

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

Associated Markings



"Up to this point, Doris, the markings that you put on your document provide classification information. Now we're going to put markings on your document that give *information other than classification levels*. We call these markings '*associated markings*.' Associated markings go on the face of your document. For marking purposes, we refer to the first thing you see as you look at the front of a document (cover, title page, or first page), as the *face of the document*. As we noted, not all documents have a *cover*, like yours. When you look at some documents, the first thing you see is the *title page*. Or you might see the *first page*. So, although in this case you'll be putting these associated markings on a cover, remember that *associated markings go on the face of the document, whatever that face may be*.

"And remember when we spoke last week about the two classification processes?"

"Original and derivative classification?"

"Right. Well, the associated markings that you put on the face of a document vary according to whether the document is an originally classified one or a derivatively classified one. Let's look at a list of the markings first, then we'll look at how an originally *classified document is marked and then how a derivatively classified one is marked*."



Associated markings that go on the face are:

- "Classified by" line if original classification
- "Classified why" line if original classification
- "Derived from" line if derivative classification
- Downgrading instructions (if applicable)
- The "Declassify on" line
- The agency and office where the document originated and the date
- Additional warning notices

Associated Markings - Original Classification



General Kent

OCA

"I'm going to show you the associated markings that go on the face of an originally classified document. However, be aware that an originally classified document is *rare*. To say that a document is originally classified means that *an OCA has personally made an original classification decision on every classified item in the document*. And you know for yourself that hardly ever happens. I can't remember the last time our OCA, General Kent, sat down and personally classified every piece of information in a document. Most classified documents are classified through the derivative process. We'll look at the associated markings for a derivative document in a minute.

The "Classified By" Line-----

"The '*Classified by*' line indicates *who classified the information* in the document."

"So if I were an OCA and I determined that the information needed to be classified, my name would appear on the 'Classified by' line."

"Right, Doris! That and some other information."

An originally classified document's "Classified by" line contains the *name or personal identifier of the OCA* and the *OCA's position title*. If the agency is not: apparent on the document, the 'Classified by' line must include the agency's name.

"The OCA is accountable for the original classification decision, so the OCA's name or identifier is required in addition to the OCA's title."

The "Classified Why" Line-----



"Executive Order 12958 requires that a reason be given why the information in the document is classified. We call this the '*Classified why*' line. Remember, this is required for an originally classified document, *not* a derivatively classified one. To meet this requirement, the OCA either *writes out the reason* or *cites the classification category* from Section 1.5 of the Executive Order (para 2-301, DoD 5200.1-R)."

Downgrading Instructions-----

"Doris, do you remember what downgrading instructions do?"

"Well, I think so.

Downgrading instructions indicate when classified information requires a lower degree of protection *than is* currently provided. TOP SECRET information may become SECRET or CONFIDENTIAL; SECRET information may become CONFIDENTIAL.

"Right, Doris. Of course, not all documents require downgrading instructions. But if the information in the OCA's document can be downgraded sometime in the future, the OCA puts the instructions on the *face of the document*.

The "Declassify on" Line

"Regardless of whether you have downgrading instructions, you *must* have a 'Declassify on' line.

Declassification is a determination that classified information no longer requires protection. When classified documents or materials are declassified classification designations are removed or canceled.

"I remember that the OCA has four options, Mike.



An OCA's declassification options are:

- A specific date within 10 years
- A specific event likely to occur within 10 years
- 10 years from the date of classification
- Exempt from the 10-year rule

"And I also recall that 'OADR' is no longer an option."

"That's right, Doris. 'OADR' is *not* an option under E.O. 12958. It's prohibited!

Agency and Office of Origin, and Date-----

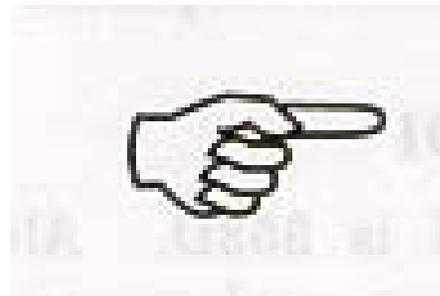
"Other information that must appear on the document are the *agency* and *office* that originated the document and the *date of* the document.

"These items are required administratively anyway, so *if* they appear somewhere other than the face of the document, that's okay. *If* not, then the OCA must include the information.

Additional Warning Notices-----



"*If* the document contains any information that warrants special handling or additional controls, then the OCA must place the appropriate *warning notice* on the face of the document. The notice warns readers that the document contains this type of information. Just refer to the table I gave you for the most common warning notices." Here's what Doris' cover might have looked like if *General Kent had originally classified the document*.



SECRET

LASER WIDGET FIELD TEST (U)

13 January 1997

DEFENSE INTEROPERABILITY VALIDATION AGENCY
4719 DORCHESTER STREET
SPRINGFIELD, VIRGINIA 22150

*Classified by: General John Kent, Director DIVA,
Office of the Director*

Reason: 1.5(a)

Declassify on: 23 August 2004

SECRET

Associated Markings - Derivative Classification

"Now let's talk about the associated markings that go on the face of a *derivatively* classified document. Almost all documents are derivatively classified, including yours, Doris. So these markings are the most common ones. And note that some of them are the same as the associated markings that go on an originally classified document."

The "Derived from" Line-----

"The '*Derived form*' line on a derivatively classified document serves the same function as the 'Classified by' line found on an originally classified one. Basically, it tells the reader *where the classification for the information in the document came from*. The 'Classified by' line on an originally classified document tells you who classified the information. The 'Derived from' line on a derivatively classified document tells you what source or sources provided the classification guidance or instructions for its author.

A derivative document's "Derived from" line contains either...

- The complete identity of a single source (document, Security Classification Guide, or other classification guidance, such as a regulation or directive):
 - (1) Subject of source
 - (2) Agency and office of origin of source
 - (3) Date of source
- or
- The phrase "*Multiple sources*"



Doris says, "I'll bet the 'Derived from' line on my document should say '*Multiple sources.*' I used several classified source documents to develop my document and I referred to them for classification instructions."

"You're right! Whenever you use *more than one source for classification instructions* put 'Multiple sources' on the 'Derived from' line. Of course, if you use *only one source*, write that source on the line. Identify it by its *name, originating agency and office, and date.*

"One other thing ...

If you use more than one source for your classification guidance and you put "Derived from: Multiple sources" on your document you must either list your sources on the face of your *document or maintain a list of your sources with your file copy* so that they will be available if you should need to explain your classifications.

Downgrading Instructions

"And as for an originally classified document, if the information in your document can be downgraded to a *lower classification level in the future*, put those instructions on the *face of your document.*

The "Declassify on" Line

"And as for an originally classified document, regardless of whether you have downgrading instructions, you *must* have a '*Declassify on*' line, unless your document contains '*Restricted Data*' or '*Formerly Restricted Data.*'"

"Where do I get my declassification instructions?"

Using a Single Source Document

"Suppose you use one source document as the basis of your classification instructions. If that's the case, that document's declassification instructions become your document's declassification instructions."

"So if my source document's 'Declassify on' line is:

Declassify on: 2 February 2006

then the 'Declassify on' line on my document is:

Declassify on: 2 February 2006."

"Exactly."

Using Multiple Sources

"Now if you use more than one source and some or all have *different declassification instructions*, then use the most restrictive declassification instruction for your document. The most *restrictive declassification instruction* would be the one that would provide the *longest protective time period*."

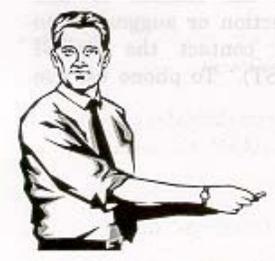
When using multiple sources, place the *most restrictive instruction* on your "Declassify on" line.

"So if I use three source documents that have these declassification instructions:

Declassify on: 25 March 1999 **Declassify on: 31 May 2005**
Declassify on: 15 July 2000

I would put on my document:

Declassify on: 31 May 2005."



"That's correct. The same principle applies if the declassification instructions for the individual information elements in your document vary. Use the *most restrictive declassification instruction* for your document."

"Mike, I don't mean to be a spoil-sport, but what if my source document has '*Declassify on: OADR*' as its declassification instruction. You told me earlier that under E.O. 12958, we can't use it."

"I did. If you use a source whose declassification instruction is 'OADR,' then on your document you write '*Declassify on: Source Marked OADR; Date of source _____*' and you put the *date of the source document* in the blank.



Doris

"Let's take an example. Suppose your source document is dated 23 June 1994. The declassification instructions on it are:

Declassify on: OADR

What declassification instruction would you write on the face of your document?"

"Hmm, I believe my instruction would be:

Declassify on: Source marked OADR; Date of source 23 June 1994."

"You've got it, Doris!"

Now let's make it a little more complex. Remember what I said about using the *most restrictive* declassification instruction. What if you had taken classified information from *three different documents* and used it in your document. All three documents have the declassification instruction

'Declassify on: OADR.' The dates the documents were created are:

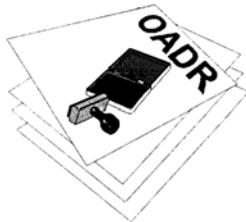
- (1) 15 April 1993
- (2) 5 September 1988
- (3) 25 October 1994

What would your 'Declassify on' line be?"

"Oh, boy! Let me see. I think it should be:

Declassify on: Source marked OADR; Date of source 25 October 1994"

"Go to the head of the class, Doris! Now if your source document was written *before 1982* - *that* is, prior to the time that President Reagan's E.O. 12356 that established OADR took effect - and it has an *indefinite duration* for classification, you treat that document *as if* it had a declassification instruction of 'OADR.' You won't see the phrase 'Declassify on: OADR' on the document, just treat it *as if* it did have it on it.



A source document

Documents and materials classified prior to E.O. 12356 that are not marked for declassification on a specific date or event will be treated *as though they were marked "OADR."*

I

"Now if your source document has one of the E. O. 12958 *indefinite declassification instructions* on it, such as a 10 year exemption marking - for example, X-1 where the blank is filled in with one of the exemption categories from paragraph 1.6(d) of the E.O. - just *carry forward that declassification instruction to your document.*"

"So, Mike, if the source document has:

Declassify on: X3

then I just put that same instruction on the face of my document, right?"



"Right. Now suppose you use two source documents. The dates they were created and their declassification instructions are:

(1) Document date: 12 April 1997

Declassify on: X1

(2) Document date: 22 May 1997

Declassify on: X3

What declassification instruction would you use?"

"That's easy, Mike,

Declassify on: X3

That document was created later so its declassification instruction provides the longer potential time period for classification."

"Correct! Now let's recap what we just went over..."

To determine your declassification instructions:

- If a single E.O. 12958-declassification instruction (date, event, or exemption marking) applies to *all* the classified information in your document, use it.
- If *all* of the information comes from documents marked "OADR, " *put* on your document "Declassify on: Source marked OADR; Date of source _____ placing the *latest date of any of your sources* in the blank.
- If the declassification instructions for the information in your document vary, use the *most restrictive* declassification instruction.

"The order of precedence for declassification instructions is as follows:



Most Restrictive
"25XV;
"X1 "through "X8"
"OADR"
The latest date or event specified for any source
Least Restrictive

Agency and Office of Origin, and Date-----

"Just like an originally classified document, a derivatively classified one must contain the *agency* and *office* that *originated* the document and its *date*.

Additional Warning Notices-----

"And if the derivatively classified document contains any information requiring special handling or additional controls, place the *appropriate warning notice* on the face of the document.

"Okay, Doris, let's finish marking your cover. Where did you get your classified information?"

"I used two source documents:

- (1) a Secret document, 'Laser Widget Tests' written by the DIVA Development Office on 14 March 1994 with declassification instructions of 'OADR.'
- (2) a Secret document, 'Laser Widget Demonstration' by the DIVA Development Office on 29 June 1994 with declassification instruction of 'OADR'."

SECRET

LASER WIDGET FIELD TEST (U)

13 January 1997

DEFENSE INTEROPERABILITY VALIDATION AGENCY
4719 DORCHESTER STREET
SPRINGFIELD, VIRGINIA 22150

Weapons Systems Division

Derived from: Multiple Sources

Declassify on: Source marked OADR;

Date of source: 29 Jun 94

Sources:

- 1. "Laser Widget Tests," DIVA Development Office, dated 14 Mar 94*
- 2. "Laser Widget Demonstration," DIVA Development Office, dated 29 Jun 94*

SECRET

Marking Component Parts

"Just one more item to cover: marking *components*."

A component is a section of a document that is intended to be taken out of the document and used separately.

"Like an appendix or annex?"

"Yes. Suppose your document had an appendix. You would mark it *as if it were a separate document* since someone might pull it out of your document and use it by itself.

Marking a component...

Portion, page, overall, and associated markings are required, however

If an entire component is Unclassified...

* **Mark the top and bottom of the component's face page with "UNCLASSIFIED."**

* **Include a statement like "All portions of this (appendix, annex, etc.) are UNCLASSIFIED."**



"Suppose the overall classification of my appendix is Secret, but the overall classification of my document without the appendix is Confidential. Do I change the document's overall classification to Secret when the appendix is attached?"

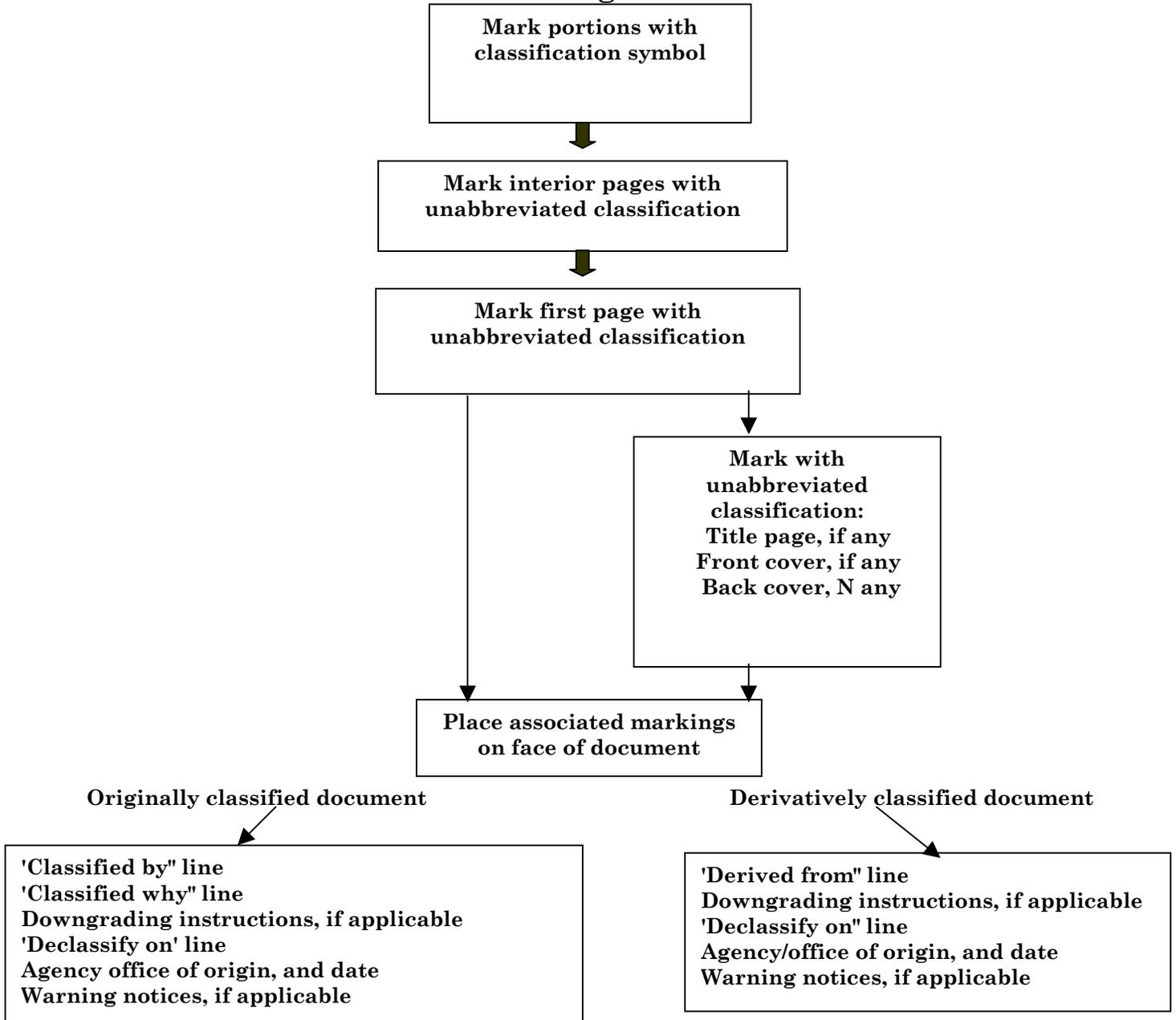
"Yes. However, you need to put an *additional marking* on the *face of your document* to let the user know that *when the appendix is removed, the document is classified Confidential*.

If the component is of a higher classification level than the document it is attached to, add the following marking to the face of the document:

**-UPON REMOVAL OF (TYPE OF COMPONENT)
THIS DOCUMENT BECOMES (CLASSIFICATION LEVEL)."**

"Here's a chart that sums up the marking process."

The Marking Process



REVIEW EXERCISES - Part One

1. List three reasons for marking classified information.
 - a. _____
 - b. _____
 - c. _____

2. Which three parts of every classified document must be marked with the proper classification marking?
 - a. _____
 - b. _____
 - c. _____

3. What three other parts, if contained in a document, must also be marked?
 - a. _____
 - b. _____
 - c. _____

4. The next page shows page 7 (an interior page) of a derivative document. Use the following information to place the proper portion and page markings on it.

The source of classification is a report, "Visual Displays (U)," dated 1 Dec 92., developed by the Human Factors Engineering Office, Fort Belvoir, VA.

From the source document you determine that:

The first paragraph is Unclassified.

The second paragraph is Confidential, declassify on 2 Oct 99.

The first subparagraph is Confidential, declassify on 2 Oct 99.

The second subparagraph is Confidential, declassify on 2 Oct 99.

The third paragraph is Unclassified.

The figure is Secret; its caption is Unclassified.

The fourth paragraph is Confidential, declassify on 12 Jun 2003.

The fifth paragraph is Unclassified.

Three basic types of dynamic quantitative displays were evaluated for use in the STR24 Vehicle.

Based on thorough research, the digital display is recommended for use because:

Digital displays are more accurate than analog displays.

Digital displays record values quicker than analog ones.

The figure below represents the type of display to be incorporated into the STR24 Vehicle.

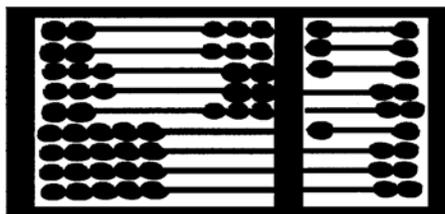


Figure 1. Recommended Display

As the display is developed, care must be taken to ensure that the values displayed in the digital display remain visible long enough to be read.

The digits on the display will appear in green as opposed to red.

5. Use the information below to apply portion, page, and overall markings to this one-page document prepared by DIVA's Weapons Systems Division.

The source of classification is the Security Classification Guide for the AN/ALQ-904 Countermeasures Set (U), issued 7 Oct 91 by the Countermeasures Equipment Project Office, Fort Pell, VA. From the SCG, you determine that:

Paragraph 1 is Confidential, declassify on 2 Nov 99.

Paragraph 2 is Unclassified.

Subparagraph 2a is Unclassified.

Subparagraph 2b is Secret, declassify on 1 Apr 99.

Subparagraph 2c is Secret, declassify on OADR.

Paragraph 3 is Unclassified.

Subparagraph 3a is Confidential, declassify on completion of OT-H.

Subparagraph 3b is Secret, declassify on achievement of IOC.

Subparagraph 3c is Confidential, declassify on achievement of IOC.

DEFENSE INTEROPERABILITY VALIDATION AGENCY
4719 DORCHESTER STREET
SPRINGFIELD, VIRGINIA 22150

INFORMATION PAPER

SUBJECT: AN/ALQ-904 Countermeasures Set

1. Production start for AN/ALQ-904 has been delayed until June 1995 because of serious performance problems discovered during OT-I.
3. Problems encountered include:
 - a. Batteries have a 53% probability of full discharge at 81° F.
 - b. Jamming of ARM terminal homing systems failed 96%.
 - c. Operation at a 73 GHz setting caused unintentional detonation of XM-214 Missile warheads within 300m.
4. Production rescheduling will cause milestone slippage as follows:
 - a. OT-II to Jan 96
 - b. First production delivery to Jun 96.
 - c. IOC to Sep 96.

LTC Fluster / 77765
5 May 92

6. The next page shows the front cover of a report prepared by the Office of the Deputy Assistant Secretary of Defense. Use the information below to mark the front cover.

The subject is Unclassified.

Pages 3 through 25 and pages 28 through 34 contain Confidential information. Page 26 contains Secret information. Page 27 contains Top Secret information.

The sources of classification are:

DA Pamphlet 100-7 (Confidential, declassify on 2 Jun 99)

CNO Letter, 7 Aug 93, subject: Naval Operations in the Pacific (U), (Secret, declassify on OADR)

SCG for the XM29 Missile System (U) (Top Secret, declassify on 15 Jan 99)

Final Report: Southern Pacific Study Group

28 March 1993

Prepared by:
Office of the Deputy Assistant Secretary of Defense
Washington, DC 20305

7. Document A is a Secret letter entitled "Gyro Rate (U)," and was written by the Testing Office of DIVA on 23 January 1990 with declassification instructions of 21 May 1999.

Document B is a Secret letter entitled "Spin Cycle (U)," and was written by the Operations Office of DIVA on 14 September 1992 with a declassification instruction of OADR.

- a. You use Document A in writing a report. Complete the following:

Derived from _____

Declassify on _____

- b. You use both documents for your report. Complete the following:

Derived from _____

Declassify on _____

8. If your "Derived from" line is "Multiple sources," what must appear on your document or be maintained with your file copy?
9. You have extracted Secret information from the following four documents and have put the information into a document that you are writing. What is your "Derived from" line and what is your "Declassify on" line?
- (a) A Secret letter originated by the Operations Office of DIVA, subject: Wainscotting Rate (U), dated 15 February 1996, Declassify on: X4.
- (b) A Secret memo originated by the Testing Office of DIVA, subject: Wainscotting Declination (U), dated 7 September 1996, Declassify on X3.
- (c) A Secret letter originated by the Operations Office of DIVA; subject: Wainscotting Drive (U), dated 9 March 1994; Declassify on: OADR.
- (d) A Secret memo originated by the Testing Office of DIVA, subject: Wainscotting Leftovers (U), dated 23 October 1993, Declassify on: 1 November 2002.

10. Component parts of a document should be marked as if they were completely separate documents.

True. False.

SOLUTIONS AND REFERENCES - Part One

1. Any three of the following:
 - To alert a user that something is classified.
 - To tell the user of the degree of protection required.
 - To specify what portions of a document *contain* or *reveal* classified information.
 - To identify who classified the information or what source the author used to get classification guidance.
 - To show the reason for the classification of the information.
 - To provide instructions on how long the information is classified.
 - To give notice of special controls and safeguarding requirements.
(p. 4-3)

2. The following parts of a classified document must be marked:
 - a. Portions
 - b. Interior pages
 - c. First Page (p. 4-6)

3. The following parts of a classified document must be marked if the document has them:
 - a. Title page
 - b. Front cover
 - c. Back cover (p. 4-6)

4. CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

SECRET

(U) Three basic types of dynamic quantitative displays were evaluated for use in the STR24 Vehicle.

(C) Based on thorough research, the digital display is recommended for use because:

(C) Digital displays are more accurate than analog displays.

(C) Digital displays record values quicker than analog ones.

(U) The figure below represents the type of display to be incorporated into the STR24 Vehicle.

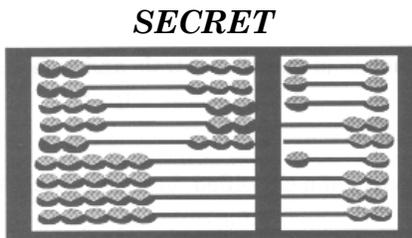


Figure 1. (U) Recommended Display

(C) As the display is developed, care must be taken to ensure that the values displayed in the digital display remain visible long enough to be read.

(U) The digits on the display will appear in green as opposed to red.

SECRET

5. CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

SECRET

DEFENSE INTEROPERABILITY VALIDATION AGENCY
4719 DORCHESTER STREET
SPRINGFIELD, VIRGINIA 22150

INFORMATION PAPER

SUBJECT: AN/ALQ-904 Countermeasures Set (14)

1. (C) Production start for AN/ALQ-904 has been delayed until June 1995 because of serious performance problems discovered during OT-1.
2. (U) Problems encountered include:
 - a. (U) Batteries have a 53% probability of full discharge at 810 F.
 - b. (S) Jamming of ARM terminal homing systems failed 96%.
 - c. (S) Operation at a 73 GHz setting caused unintentional detonation of XM-214 Missile warheads within 300m.
3. (U) Production rescheduling will cause milestone slippage as follows:
 - a. (C) OT-II to Jan 96.
 - b. (S) First production delivery to Jun 96.
 - c. (C) IOC to Sep 96.

*Derived from SCG for ANIALQ-904, Countermeasures
Set (U), Equipment Project Office, Ft Pell, 7 Oct 91*

Declassify on: Source marked OADR, date of source 7 Oct 91 LTC Fluster / 77765 5 May 92

SECRET

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY
(pp. 4-8, 16, 26-32)

6. CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

TOP SECRET

Final Report: Southern Pacific Study Group

28 March 1993

Derived from: Multiple sources

Downgrade to Secret on 1S Jan 99

Declassify on: Source marked OADR, date of source 7 Aug 93

Prepared by:

Office of the Deputy Assistant Secretary of Defense Washington, DC 20305

TOP SECRET

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

(pp. 4-18-19, 26-32)

7. a. Derived from: Letter, subj: Gyro Rate (U), Testing Office, DIVA,
dated 23 Jan 90

Declassify on: 21 May 99
- b. Derived from: Multiple sources

Declassify on: Source marked OADR, date of source 14 Sep 92
(pp. 4-26-32)
8. A list of the sources.

(p. 4-27)
9. Derived from: Multiple sources

Declassify on: X3 (pp. 4-26-32)
10. True.

(p. 4-34)

Marking a Transmittal Letter

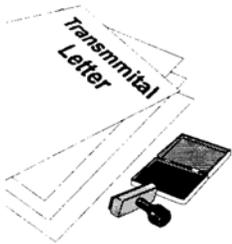
Mike picked up his folder, and got up to leave.

"Any other goodies in that folder, Mike?" Doris asks.

"Well, let me see. Do you think you'll be sending your report to anyone?"

"I'm sure we'll send it to the California field office."

"Then you'll be needing a *transmittal letter*. I can give you a sample - an unclassified transmittal letter attached to a classified document. And the instructions for using an unclassified transmittal letter with a classified document are right there in the text of the letter."



"Mike, this sample letter is great! I see that the only markings required are the *overall classification marking* and the *notice* at the bottom. That makes sense since the transmittal letter itself is Unclassified. There's no reason it would need a 'Classified by' or 'Derived from' line, a 'Declassify on' line, or any downgrading instructions."

"This stuff isn't so hard to figure out after all, is it, Doris?"

SECRET

DEFENSE INTEROPERABILITY VALIDATION AGENCY
4719 DORCHESTER STREET
SPRINGFIELD, VIRGINIA 22150

17 February 1997

MEMORANDUM FOR Transmittal Letter Writers

SUBJECT: Unclassified Transmittal Letters

1. This is a sample of an unclassified transmittal letter that has, as an attachment, another document that is classified SECRET.
2. If the attached document was Unclassified, the transmittal letter would not have markings. Instead, SECRET appears because it is the overall classification of the attached document.
3. Observe the notice at the bottom of this letter. It tells a user that upon removal of the attachment, this letter is unclassified.
4. If any of the attachments contain information that warrants a special notice, the warning notice must appear on the face of the transmittal letter.
5. All markings need appear only on the face of the transmittal letter.

You R. Writer

Attachment

*UPON REMOVAL OF ATTACHMENT
THIS DOCEYMENT BECOMES UNCLASSIPIED*

SECRET

Marking an Electronically Transmitted Message



"Do you ever send messages, Doris?"

"Sure. I sent one the other day."

"Here's a sample message with the requirements written in the text."

"For incoming electronically transmitted messages, the system can apply the top and bottom page markings, but they must stand out from the text."

"Mike, I appreciate the help and the samples. I'll be sure to pass out this stuff to our people who need it."

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

SECRET

SUBJ: DD FORM 173 TEXT (U)

1. (U) The first item of information in the text of a classified electronically transmitted message is its overall classification.
2. (S) Portion marking requirements for messages are the same as for other documents.
3. (S) The "Classified by" line or the "Derived from" line appears at the end, just prior to the downgrading/declassification instructions.
4. (C) Downgrading and declassification instructions appear on the last line of text.

***Derived from: Ltr, HQ AMC, subj. DD Form 173, 14 Mar 89
DECL 24 Aug 98***

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

Marking Working Papers



"While we're at it, let's review another topic we discussed last week - how to mark working papers. Remember we said that in preparing our final versions of classified documents, we often develop preliminary drafts? We refer to them as 'working papers'. We said that working papers are not the final products themselves, but simply something we use to get to the final product.

When marking a working paper...

- * Put the *date it was created* on it.
- * Mark it with the *highest level of classified information* it contains or reveals.
- * Mark it just as you would a *finished document* if:
 - you keep the papers for *more than 180 days* from its date of origin, or
 - you release the paper *outside your activity*.

"Remember that you must *protect* the working paper at the *proper level of classification* and, just as important, *get rid of it* (properly destroy it) *as soon as you finish the final product*."

Some Special Markings

"Remember warning notices? They alert readers that a document contains information requiring *additional handling procedures* or *special controls*. Let's look at those you're likely to run across, Doris.

Restricted Data

“Restricted Data is information related to atomic weapons and nuclear material. It is under the control of the Department of Energy. If Restricted Data is put in a DoD document, the following marking goes on the face of the document:

RESTRICTED DATA
This material contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions.

"And recall that if the document contains Restricted Data, *no "Declassify on" line* should be displayed. *Only the DOE can declassify Restricted Data.* Mark portions containing Restricted Data as follows:

- **(TS-RD)**
- **(S-RD)**
- **(C-RD)**

Formerly Restricted Data

“Formerly Restricted Data is information that has been removed from the Restricted Data category upon a joint determination by the Department of Energy and DoD. If Formerly Restricted Data appears in a DoD document, place the following marking on the face of the document:

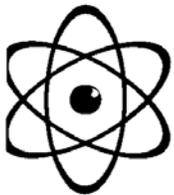
FORMERLY RESTRICTED DATA
Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination. Section 144.b, Atomic Energy Act, 1954



"If the document contains Formerly Restricted Data, do *not* use a "*Declassify on*" line. Formerly Restricted Data is *declassified only upon the joint determination of DOE and DoD*. Mark *portions* containing Formerly Restricted Data as follows:

- (TS-FRD)
- (S-FRD)
- (C-FRD)

Critical Nuclear Weapon Design Information (CNWDI)-----



"CNWDI is a special type of Top Secret and Secret Restricted Data. It refers to information concerning the *theory of operation or design of components of nuclear devices*. If CNWDI appears in a DoD document, this marking goes on its face:

**CRITICAL NUCLEAR WEAPON DESIGN INFORMATION
DOD DIRECTIVE 5210.2 APPLIES**

"The *portion marking* for CNWDI is "(N)." Since CNWDI is a type of Restricted Data, mark portions that contain CNWDI marked as follows:

- (TS-RD)(N)
- (S-RD)(N)

"As you probably suspect already, Doris,

- *Special markings, if they apply, should be placed on the face of a document.*
- **If a special marking appears on the face of a document's component, it should also appear on the face of the document.**

Other Marking Considerations

"You've come this far, Doris. Have you had enough, or are you game to go the rest of the way? There's just Unclassified, public domain, and NATO and foreign government classified left."

"You've kept me on the edge of my seat so far. I can't wait to see how it all turns out!" Doris laughs.

Wholly Unclassified Material-----

"It's home stretch time, then. Hold on! Material that contains *only unclassified information* usually *is not* marked. However, there *are two circumstances* when the markings "UNCLASSIFIED" or "(U)" can be applied:

- When it's important to convey to the user that the information was *reviewed* for possible classification, but it was determined that classification was not *required*.
- When dealing with formerly classified material

Information That Appears In The Public Domain-----

"Material that appears in the *public domain* (for example, articles in magazines or newspapers), *cannot be marked as classified*. If, however, you develop a report that *compares the content* of a newspaper or magazine article *to classified information*, the report, if classified, *can be marked*."

Marking Foreign Government and NATO Information



"Marking foreign government and North Atlantic Treaty Organization (NATO) information can be pretty tricky, Doris. Keep in mind that many of the marking requirements that we've gone over do not apply to documents created by foreign governments and international organizations of governments, such as NATO. For example, other governments may *not* require *portion and page markings*. Another difference concerns *classification designations*. The United States uses three security classification designations: TOP SECRET, SECRET, and CONFIDENTIAL. Many foreign governments and international organizations use a *fourth designation, 'RESTRICTED.'* Appendix F, DoD 5200. 1 -R contains a table that shows foreign government and NATO equivalents of U.S. designations. Here's an extract of Appendix F.

COUNTRY	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Germany	Streng Geheim	Geheim	VS-Vertraulich	
Italy	Segretissimo	Segreto	Riservatissimo	Riservato
Japan	Kimitsu	Gokuhi	Hi	Toriatsukaichui
Spain	Maximo Secreto	Secreto	Confidencial	Diffusion Limitada

Marking Foreign Government Documents-----

"Let's suppose there's an SFC Juan Montoya who is stationed at DIVA's field office in Heidelberg, Germany. He has just received three classified

documents; one from the government of *Germany* and two from the government of *Spain*.

"Juan looks at the document from Germany first. 'Good,' he thinks to himself, 'it's already marked in English. I don't have to do a thing.'

If a classified foreign government document is marked in *English* already you don't have to apply any other markings.

"As Juan looks at one of the documents from the government of Spain he sees the phrase "SECRETO" on it. Juan refers to Appendix F of DOD 5200.1-R. He sees that Spain's marking "SECRETO" is equivalent to our marking "SECRET" Juan writes "SPAIN SECRET"(conspicuously) near the marking 'SECRETO.'

"Juan looks at the other document from the government of Spain. It has 'DIFFUSION LIMITADA!' on its cover. He looks at Appendix F and sees that Spain's classification designation 'DIFFUSION LIMITADA' is equivalent to 'RESTRICTED.' Since our government doesn't have the 'RESTRICTED' designation, he needs to add a marking to show English speaking U.S. personnel what safeguards the document needs. So he puts the following notation on the face of the document:

**SPAIN RESTRICTED INFORMATION
Protect as CONFIDENTIAL - Modified Handling**

"That's about all there is to it, Doris!

- If the *overall marking* of a classified foreign government document is in a *foreign language*, refer to *Appendix F* for our equivalent marking.
- If the equivalent marking is *TOP SECRET*, *SECRET*, or *CONFIDENTIAL*, conspicuously write or stamp the *country name* and the *appropriate classification marking near the foreign language marking*.
- If the equivalent marking is *RESTRICTED*, conspicuously write or stamp

"(Country) RESTRICTED INFORMATION
Protect as CONFIDENTIAL-Modified Handling"

near the foreign language marking.

Marking NATO Documents



"So that's how you would 'translate' the markings of a classified foreign government document for use in our Information Security Program. The same principle applies to *NATO documents*. If the classification markings are in English, you do not have to mark the document further. However,

If the document is marked *NATO RESTRICTED* in *another country's language*, you must place the following notation *on the face of the document*:

TO BE SAFEGUARDED IN ACCORDANCE
WITH USSAN INSTRUCTION 1-69

"This notation alerts a user that the document's safeguarding requirements can be found in *United States Security Authority for North Atlantic Treaty Organization Affairs (USSAN) Instruction 1- 69*. Some components may have additional marking requirements for NATO classified information in their regulations, Doris.

DoD Documents with Foreign Government Information-----

"A DoD classified document that contains foreign government classified information must bear the following notation on its face:



THIS DOCUMENT CONTAINS (Country) INFORMATION.

"This warning alerts a user that the document contains a particular foreign government's information and that the document should *not be provided to nationals of a third country or declassified without the consent of the originator*. If the identity of the foreign government must be *concealed*, the marking is:

THIS DOCUMENT CONTAINS FOREIGN GOVERNMENT INFORMATION.

I

"If your document had portions containing foreign government information, Doris, you would have had to mark them it so as to identify the information.

Portions of DoD documents that contain classified foreign government information must be marked to identify the foreign government information.



"Mark each portion by writing the abbreviation for the foreign country followed by a dash (-) and the classification symbol. For example, (*MEX-C*) alerts a user that the portion contains Confidential information of the government of Mexico. Check the country's abbreviation in a reliable source, such as a dictionary. If the identity of the foreign government must be concealed, use FGI with the applicable classification symbol, for example, (FGI-S).

DoD Documents with NATO Information-----

"The same holds true for *DoD classified documents* that contain *NATO classified information*. In this case mark the *face* of the document as follows:

THIS DOCUMENT CONTAINS NATO (*CLASSIFICATION*) INFORMATION

"These DoD documents must also be *portion marked* to identify the NATO information. For example, a paragraph that contains *NATO SECRET information* is portion marked '(NS).'

DoD Documents with only Foreign Government Restricted/ NATO Restricted Information-----

"What would you do if you had a DoD document that doesn't contain any Top Secret, Secret, or Confidential information but does contain foreign government Restricted or NATO Restricted information?"

If the document contains no U.S. classified information but does contain foreign government *Restricted or NA TO Restricted information...*

- Mark the portions accordingly.
- Mark the page top and bottom:
 "This page contains (Country/NATO) RESTRICTED information."
- Place the following notation on the face of the document:

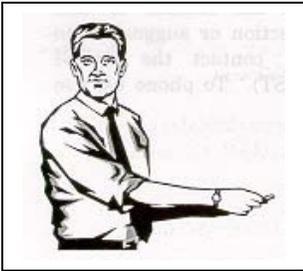
"This document contains (Country/NATO) Restricted information not marked for declassification (date of source) and shall be safeguarded in accordance with USSAN 1-69/DoD 5200.1-R."

"Here's a table that summarizes the requirements for marking NATO and foreign government information, Doris."

Downgrading/ Declassifying Foreign Government/ NATO Information-----

"If the foreign government or NATO does *not* provide downgrading or declassification instructions for the information, treat the information *as if it were marked 'OADR.'* Since the information is not our information, we must obtain the appropriate government's (or international organization's) authorization to lower or remove the classification."

Marking Classified Materials Other Than Documents



"Whew! Free at Last! I didn't think I was going to last through that foreign government and NATO stuff, Mike!"

"I know I told you that was the last of it, Doris. But there is still one teensy-weensy topic left."

"Say your prayers, Security Man! Oh, all right. Go ahead. But if this isn't the last word on marking, it will be *your* last word - on anything!"

"We just need to go over how to mark *materials other than documents.*

We conspicuously mark classified materials with the overall classification designation and when possible the associated markings.

"The *classification markings* should be *conspicuously displayed* on the *classified materials* and their *containers*, if any. The markings can be



stamped, written, or printed on, or affixed by a sticker, decal, or similar device. If it's not practicable to mark the material or container, you can provide *written notification of the classification markings* to be kept with the materials. However, this written notification procedure should be used *only as a last resort!* Remember, the purpose for marking the materials is to ensure that the user, recipient, reader, or whoever realizes that the materials they have are classified. If a big stamp with the classification level on it will work, use it. If you have to attach a label to the item and then stamp the label, do so.



Some items such as 35 mm slides and view-graphs have two groups of people that you must keep informed. The first group is the *audience that views the information as it is projected on a screen*. You must ensure that that group recognizes that the information they are viewing is classified, so put the classification information on the *image area*. The other group of people that you are concerned with is *whoever is handling the slide or the view-graph*. So put the classification designation on the *border of the slide or view-graph* so that person is aware that he or she is holding an item that contains classified information.



"You must also conspicuously mark *magnetic storage media*, the 3 1/2 inch disks (or the 5 1/4 inch disks that some people still use) that contain classified information. This ensures that others realize that the disk contains classified information - and it reminds you too! If you have them, use the small labels (SF 706 for Top Secret, SF 707 for Secret, and SF 708 for Confidential) designed for use on computer disks and similar materials.

Otherwise, take appropriate action to ensure that people will know that the disk contains classified information.



"How would you mark a document that is electronically stored on a disk, Doris?"

"This is just a guess. Electronically?"

"Still awake, eh? Right. You *electronically* mark the portions and then apply the interior page markings, the overall document markings, and the associated markings, if it's feasible. Otherwise *mechanically* place these markings on the document after it is printed.

"Well, Doris, you made it! And probably in record time."

"Don't use the t-word in my presence ever again! My whole morning is gone!" Doris laughs. "Seriously though, Mike, I appreciate your taking the *time* to tutor me in all these marking instructions. How about we do lunch?"

"You bet! And even though it may seem that we've covered marking completely, I'd better point out that the DoD 5200.1-R goes into even greater detail on how to mark various materials. Use it to answer specific questions that you may have about marking a particular item.

"And always remember, Doris, the key to marking is to *identify for others what is classified, at what level, why, and for how long.*"

Summary



In this lesson, you learned about marking requirements for classified documents and materials. We mark the materials to (1) alert the users that they have classified material in their possession, (2) tell the users how they must protect it, (3) show what is classified in the material, (4) identify who classified the information or what source was used to get the classification guidance, (5) show why the information is classified, (6) inform users how long the information is classified, and (7) provide users with any special handling instructions, as appropriate. The parts of a document that must be marked are the portions, the interior pages, the first page, the title page (if any), and the front and back covers (if any). In marking a document, start from the inside and work outward. All portions are marked first (the paragraphs, subparagraphs, illustrative material, captions to the illustrative material, subject or title lines, and headers to major sections), then the interior pages according to the content of the page, then the first page according to the highest level of classification of the information in the entire document, then the title page (if any), and finally the covers (if any). Associated markings provide information other than classification levels: the 'Classified by' line and the 'Classified why' line (for originally classified documents), the 'Derived from' line (for derivatively classified documents), downgrading instructions, the 'Declassify on' line, the agency and office of origin, the date of origin, and warning notices, if any. A component part of a document is marked like a separate document. Unclassified transmittal



letters need only have the overall classification marking (the highest level of classified information contained in the entire package) and a statement that the transmittal letter by itself is unclassified. These items are required only on the face of the transmittal letter. Electronic messages require that the first line of the text have the overall classification of the message; the portions must be marked, and the end of the message must have the 'Derived from' and 'Declassify on' information. A 'working paper' need be marked only with the date and the overall classification; however, it must be protected at its proper level and should be destroyed it as soon as the final product is completed. If a document contains information with special handling or control requirements, the appropriate markings need to be placed on the face of the document and the portions containing the information must be marked. Documents containing foreign government classified information or NATO classified information must be marked to reflect these contents; the appropriate warning notice must appear on the face of the document and the portions containing the information must be marked. Classified materials other than paper documents - and their containers, if any - need to be conspicuously marked to alert people that the materials are classified. Classified materials should always be conspicuously marked so others know what's classified, why it's classified, and how long it's classified. Detailed marking guidance is in DoD 5200.1-R and your component regulations.

REVIEW EXERCISES - Part Two

1. The next page shows a one-page transmittal letter prepared by DIVA's Weapons Systems Division. Use the information below to mark the transmittal letter.

The source of classification for the transmittal letter is another letter whose subject is Review of Raider's Design Specifications (U). The source letter is dated 30 June 1991 with a declassification instruction of 27 May 2000.

From the source letter, you determine that:

The subject is Unclassified.

Paragraph 1 is Unclassified.

Paragraph 2 is Unclassified.

Paragraph 3 is Unclassified.

Attached to the transmittal letter is a document that contains Secret Restricted Data and CNWDL



CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

DEFENSE INTEROPERABILITY VALIDATION AGENCY
4719 DORCHESTER STREET
SPRINGFIELD, VIRGINIA 22150

5 July 1991

MEMORANDUM FOR Personnel of Project V

SUBJECT: Raider Design Specification Review

1. Attached are the design specifications for device Raider. You are responsible for reviewing these specifications to ensure that Raider can operate under all anticipated conditions.
2. Testing continues to take place in the Testing Lab at Ft. Warren.
3. We will quickly respond to any requests for further information concerning Raider's capabilities.

LTC Janet L. Peters
Director, Project V

Attachment
Raider Design Specifications

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

2. Below is the front cover of a report prepared by the RA91 Radar System Project Office, Fort Polk, LA- Use the information to mark the front cover.

Pages 1 through 7 and pages 9 through 11 contain Confidential information that is to be declassified on 25 June 1999.

Page 8 contains Secret information that is to be declassified on 23 April 2002.

Page 12 contains Unclassified information.

Page 15 contains Top Secret Formerly Restricted Data.

The source of classification is the SCG for the RA91 Radar System (U), issued 12 March 1992 by the Electronics Office of DIVA.

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

Final Report: RA91 Radar System Testing

2 October 1994

Prepared by:

RA91 Radar System Project Office
Fort Polk, IA

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

3. The first item of text in a classified electronically transmitted message is the "Subject" line.

True. False.
4. A document contains only Unclassified information. Under what circumstances should it be marked "Unclassified?"

Use the following table to answer questions 5 through 7.

COUNTRY	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Germany	Streng Geheim	Geheim	VS-Vertraulich	
Mexico	Alto Secreto	Secreto	Confidencial	Restringido
NATO	Cosmic Top Secret	NATO Secret	NATO Confidential	NATO Restricted

5. The document on page 4-70 is the front cover of a report provided to the U.S. by the government of Germany. Apply the proper markings.
6. The document on page 4-71 is the front cover of a report provided to the U.S. by the government of Mexico. Apply the proper markings.
7. The document on page 4-72 is the front cover of a report provided to the U.S. by NATO. Apply the proper markings.

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

GEHEIM

Das Unterseeboot in die deutsche Kriegsmarine
Kapitan z.S. Helmut Pumpnickel

Marinehauptquartier BRD

3.6.93

GEHEIM

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

RESTRINGIDO

DEFENSA AEREA EN EL EJERCITO MEXICANO

31 de Augusto 1992

Oficina de la Defensa Aerea
Ministro de Defensa

RESTRINGIDO

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

NATO RESTRICTED

PROTECTING EACH OTHER

30 September 1993

Produced by:

The North Atlantic Treaty Organization

NATO RESTRICTED

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

8. Suppose you receive a document from the government of Italy. It has the markings "TOP SECRET" on it. What markings do you have to apply?

9. Suppose you receive a document from NATO. It is marked "COSMIC TOP SECRET." What markings do you have to apply?

10. You are writing a classified paper on a cooperative weapons program. You extract some information from a document marked NATO CONFIDENTIAL and put it into paragraph 5 of your document. When you mark your document, what must you do concerning the NATO Confidential information?

11. You are writing a document on a cooperative training exercise. The document contains no U.S. classified information. However, you put "Restricted" information from a government of Denmark (DEN) document dated 12 October 1992 into paragraph 12 of your document. When you mark your document, what must you do concerning the Danish information?

12. You are writing a document on a jointly produced weapon. The document contains no U.S. classified information. However, you put NATO "Restricted" information from a NATO document dated 3 April 1996 into paragraph 3 of your document. When you mark your document, what must you do concerning the NATO information?

13. The next page shows a one-page document prepared by XYZ Weapon System Project Office, NAS Lemoore, CA. Use the information below to mark the document.

Paragraph 1 is Unclassified.

Paragraph 2 contains Confidential information extracted from a document furnished by the New Zealand Ministry of Defense.

Paragraph 3 is Secret, declassify 1 Aug 2001.

The sources of classification are:

CNO Letter, 17 Jul 93, subject: Training Operations in New Zealand (U), (Secret, declassify 1 Aug 2001)

SCG for the XYZ Weapon System, 11 July 1992 (Secret, declassify OADR)

Memo from the government of New Zealand (NZ), 26 February 1993 (Confidential, no declassification instructions)



XYZ WEAPON SYSTEM PROJECT OFFICE
NAS LEMOORE, CA

1 October 1993

MEMORANDUM FOR XYZ Weapon System Training Personnel

SUBJECT: Training Operations in New Zealand

1. Training for the XYZ Weapon System will take place in June or July of 1994.
2. The New Zealand government will send 100 troops to partake in the training exercises.
3. Six XYZ Weapon Systems will be deployed to the training sites two weeks prior to training initiation.

LTC Anthony J. Landers
Director, XYZ Weapon System Training

14. Select the true statements concerning marking classified materials.
- a. Classification markings must be placed on the reel of a film but are not necessary for the canister the film is stored in.
 - b. The image area of a classified overhead transparency must contain classification markings.
 - c. Classification markings on materials should be conspicuous.
 - d. The cassette of a classified audio recording does not have to be marked as long as the audio portion contains a warning that the program is classified.

SOLUTIONS AND REFERENCES - Part Two

1. CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

SECRET

DEFENSE INTEROPERABILITY VALIDATION AGENCY
4719 DORCHESTER STREET
SPRINGFIELD, VIRGINIA 22150

5 July 1991

MEMORANDUM FOR Personnel of Project V

SUBJECT: Raider Design Specification Review

1. Attached are the design specifications for device Raider. You are responsible for reviewing these specifications to ensure that Raider can operate under all anticipated conditions.
2. Testing continues to take place in the Testing Lab at Ft. Warren.
3. We will quickly respond to any requests for further information concerning Raider's capabilities.

LTC Janet L. Peters
Director, Project V

***UPON REMOVAL OF ATTACHMENT THIS
DOCUMENT BECOMES UNCLASSIFIED.***

Attachment
Raider Design Specifications

***Critical Nuclear Weapons Design Information
DoD Directive 5210.2 applies.***

RESTRICTED DATA

***This material contains Restricted Data as defined in the
Atomic Energy Act of 1954. Unauthorized disclosure subject
to administrative and criminal sanctions.***

SECRET

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY
(pp. 4-48-49, 52)

Marking Classified Information 4-77

2. CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

TOP SECRET

Final Report: RA91 Radar System Testing (U)

2 October 1994

*Derived from: SCQ, RA91 Radar System (Eq,
Electronics Office.9 DIVA., 12 Mar 92*

FORMERLY RESTRICTED DATA

***Unauthorized disclosure subject to administrative and criminal sanctions. Handle as
Restricted Data in foreign dissemination. Section 144b, Atomic Energy Act of 1954***

Prepared by:

RA91 Radar System Project Office
Fort Polk, LA

TOP SECRET

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

(pp. 4-16,20,28,52)

3. False. The first line of text in a classified electronically transmitted document is the overall classification of the message. (p. 4-50)

4. An unclassified document should be marked "UNCLASSIFIED" when it is important to convey to the reader that the information was reviewed with the possibility of it being classified, but it was determined that classification was not required. Another circumstance is when the document concerns information that was formerly classified (p. 4-54)

GEHEIM

GERMAN SECRET

Das Unterseeboot in die deutsche Kriegsmarine

Kapitan z.S. Helmut Pumpnickel

Marinehauptquartier BRD

3.6.93

GERMAN SECRET

GEHEIM

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY
(pp. 4-55-57, 60)

6. CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

RESTRINGIDO

DEFENSA AEREA EN EL EJERCITO MEXICANO

31 de Augusto 1992

Oficina de la Defensa Aerea
Ministro de Defensa

MEXICO RESTRICTED INFORMATION
Protect as CONFIDENTIAL-Modified Handling

RESTRINGIDO

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY
(pp. 4-55-57, 60)

NATO RESTRICTED

PROTECTING EACH OTHER
30 September 1993

Produced by:

The North Atlantic Treaty Organization

*To be safeguarded in accordance
with USSANZ instruction 1-69.*

NATO RESTRICTED

8. Since the document is already marked in English, you don't have to apply any other markings. (p. 4-56, 60)
9. If a NATO-originated document is marked COSMIC TOP SECRET, NATO SECRET, OR NATO CONFIDENTIAL, you don't have to apply any other markings. (p. 4-57, 60)
10. Portion mark paragraph 5 "(W)" and put the following marking on the face of the document:

"THIS DOCUMENT CONTAINS NATO CONFIDENTIAL INFORMATION." (p.4-59, 60)
11. Portion mark paragraph 12 "(DEN-R)" and apply the following marking to the face of the document:

"This document contains Denmark Restricted information not marked for declassification (source dated 12 Oct 92) and shall be safeguarded in accordance with DoD 5200.1-R" (p. 4-59, 60)
12. Portion mark paragraph 3 "(NR)," and apply the following marking to the face of the document:

"This document contains NATO Restricted information not marked for declassification (source dated 3 April 1996) and shall be safeguarded in accordance with USSAN 1-69" (p. 4-59, 60)

13. CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

SECRET

XYZ WEAPON SYSTEM PROJECT OFFICE
NAS LEMOORE, CA

1 October 1993

MEMORANDUM FOR XYZ Weapon System Training Personnel

SUBJECT: Training Operations in New Zealand (*U*)

1. (*T4*) Training for the XYZ Weapon System will take place in June or July of 1994.
2. (*AW-C*) The New Zealand government will send 100 troops to partake in the training exercises.
3. (*S*) Six XYZ Weapon Systems will be deployed to the training sites two weeks prior to training initiation.

LTC Anthony J. Landers
Director, XYZ Weapon System Training

THIS DOCUMENT CONTAINS NEW ZEALAND INFORMATION

Derived from: Multiple sources

Declassify on: Source marked OADR, date of source 26 Feb 93

SECRET

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY
(pp. 4-20, 26-32, 58, 61)

14.
 - a. False. The containers or holders that we place classified materials into should also be marked.
 - b. True.
 - c. True.
 - d. False. The containers or holders that we place classified materials into should also be marked.

(pp. 4-61-62)

LESSON 5

DERIVATIVE CLASSIFICATION ISSUES



Derivative classification is not cut and dried. Even though you are carrying forward someone else's original classification decisions, you, like the OCA, must constantly use your judgment and apply your professional knowledge to ensure that the classifications you assign are correct. If you make an error in derivatively classifying a document, that error may not end with your document. Someone else may use your document as a source and unwittingly carry forward your error into another document, and still others may carry your error forward from that document into their documents. And so on and on in a ripple of misclassification, which may end in resources squandered in overprotection - or in access to the information by unauthorized persons. When you have completed this lesson, you will be able to do the following:

- * Verify as far as practicable the correct level of classification of portions before marking them.
- * Use only authorized sources for derivative classification.

This lesson contains no classified information. All sample documents contain hypothetical information only. All security markings are for illustration and training purposes only.

Derivative Classification Responsibility

First, let's review what we covered in earlier lessons:

Derivative classification is a determination as to whether information *has already been classified, and, if so, at what level and for how long.*



If so, that classification is *carried forward* to the *new document or product* containing the *information.*

In the DoD there is no such thing as "derivative classification authority." *Authority is assumed.*

Instead, derivative classification is the *responsibility* of all who incorporate, paraphrase, restate, or generate in new form, information that is already classified.

The responsibility is to carry forward *exactly* the *original classification decisions* as to level and duration. In deriving and marking your document, you may not raise or lower an original classification decision or source classification. You may not lengthen or shorten an original duration decision or source duration instruction.

A person with derivative classification responsibility, is *accountable* for the appropriateness of the classifications and markings he or she assigns.

Let's look in again on Mike and Doris. They have finished lunch.



Doris and Mike

"Now that you've eaten, it looks like something's eating you, Mike!" Doris says.

"It's just that I think I may have misled you about how to go about marking that document of yours. Well, not that specific document. It's O.K. But I should have emphasized a few things to you before you started your derivative classification."

"Such as?" Doris asks.

"Look, I know I've taken up your morning, but if you can spare a few more minutes I'd like you to drop by the Security Office and discuss a few things. 11

"O.K., Security Man, if it'll ease your conscience. But this had better be good!"

Is Classified Information Contained or Revealed?

At the Security Office, Mike says, "Let's start simple. If the information in the document I have written *contains* or *reveals* classified information, then we derivatively classify that information *at the same level* as that of the classified information."

"How about an example?" Doris asks.

"Suppose the security classification guide I'm using tells me that the weight of Object X is Secret

information. In my document I include a statement that says 'Object X requires a two-person lift because it weighs 150 pounds.' The statement contains the weight of Object X; therefore, it *contains* Secret information."



Doris

"I thought that's what you meant. I just wanted to be sure. How about a situation where something *reveals* classified information?"

"Sure. Suppose the security classification guide also tells me that the fact that Object X is made up of three components is Unclassified.

"I mention in a paragraph on page one of my document that Object X has three components. According to the guidance, that information is Unclassified. Then on page two of my document I provide the weight of each component. All someone has to do is add the weights of the three components to know how much Object X weighs. Voila! So the two pieces of information *reveal* Secret information."

"I see. Tricky. What if my words don't exactly match up with the words in my sources?" Doris asks.

"Let's take the story of the three little pigs," Mike says. "Suppose a security classification guide tells me that the fact that a pig has hair on its chin is Confidential information. I come to the line in the story where the wolf says, 'Little pig, little pig, let me in' and the pig says, 'Not by the hair on my chinny chin chin.' If I should state, 'The pig vowed by its whiskers not to let the wolf in its house,' the

restated information still reveals the Confidential information. So my wording is 'Confidential' too."

Doris laughs.

"So it's a funny example. But the point is serious. Here's a list of some important points to take back with you."

"I'll add it to my collection," Doris says.

Don't take derivative classification lightly!

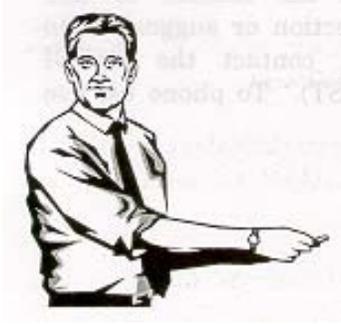
- **You've really got to *think about* what you've written.**
- **Look at it with a *critical eye*.**
- **It's not the words that you use that determine whether or not information is classified, it's what those words convey.**
- **You should *not* develop a document then turn it over to your clerical staff to mark.**
- **Your *subject matter expertise* is required to ensure that appropriate markings are applied.**

Sources Of Instructions

"Mike, so far you've talked about security classification guides in your examples. How come?"

Using a Security Classification Guide

"A security classification guide is the most reliable source of instruction for applying markings to a derivatively classified document, Doris. Security classification guides are issued for classified systems, programs, plans, and projects.



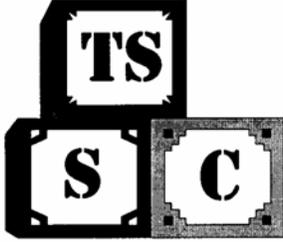
A security classification guide identifies the...

- **Information elements to be protected.**
- **Classification of the information elements.**
- **Reason for the classification of the information elements.**
- **Declassification instructions for each of the classified information elements.**

"Now he tells me! How do I go about finding out if there is a security classification guide for my next project?"

"Look in the Index of Security Classification Guides, DoD) 5200.1-1. The index lists the title of the guide and the office that prepared it. You can request the guide from the Defense Technical Information Center (DTIQ or you can contact the office that prepared it."

"I can see the advantages of using a security classification guide, Mike. But I used classified documents as the sources for my document this morning. Was I wrong?"



Portions are the building blocks of documents

"No, in that case it worked out fine. But the portion markings in source documents are not always *specific enough to permit exact identification* of what's classified and the level - or levels - of classification."

"Not specific enough? I thought I could extract a piece of information from a 'Secret' paragraph in a source document and just mark my paragraph 'Secret' because it contains the same information."

"Maybe, maybe not. When we were marking your document, we began with portions, remember? Portions are the building blocks of documents. But *even smaller units* can contain or reveal classified information.

Segments of a portion such as a sentence can contain or reveal classified information.

"Derivative classification is not a mechanical process and it's not always just a one-to-one proposition. The 'Secret' portion marking in the source document tells you that the *highest level of classified information* in that paragraph is Secret. It's possible, though, that the paragraph also contains Confidential and Unclassified information! Perhaps the information you extracted wasn't Secret after all, but Unclassified. If you marked your report's paragraph 'Secret,' you would be classifying the information too high.

"Let's see what else I have in this folder. This is what I was looking for," Mike says, handing a

printed page to Doris. "It's part of an exercise I use when I'm teaching derivative classification. I think you're ready to give it a try. Just read through the items in the security classification guide and apply it to classify and mark the paragraphs."

Security Classification Guide for Project Gin Rummy

- Everyone is dealt ten cards to start the game – Unclassified
- Aces are worth 15 points – Confidential
- The Queen of Spades is worth 20 points – Secret
- The Ten of Diamonds is worth 5 points – Confidential
- The King of Clubs is wild – Secret

Using the guide, *mark the following document portions:*

1. () At the start of the game the dealer deals everyone ten cards.
2. () Paula was dealt a pair of Jacks and the King of Clubs. This means that she started the game with three of a kind.
3. () When Jim won the first hand, Paula was left with two cards. She had the Ten of Diamonds, worth 5 points, and the Queen of Spades, worth 20 points.

Doris marks the portions (paragraphs).

"Let's see how you did," Mike says.

"I marked the first paragraph (U)," Doris says.

"You're right. The SCG tells you that the information element, 'Everyone is dealt ten cards at the start of the game,' is Unclassified.

"So far, so good. Now how did you mark 'Paula was dealt a pair of Jacks and the King of Clubs. This means that she started the game with three of a kind'?"



"I marked it '(S),' Doris says.

"Right again! This is a good example of information that *reveals* classified information. It's also an example of needing *subject matter* expertise to mark a document. In Gin Rummy, having three of a kind, that is, three of any type of card - two's, six's, etc. - is a good thing. One or two of a kind does you no good. Paula has two Jacks in her hand. Under normal circumstances, she'd need another Jack. But the guide says that the King of Clubs is wild, meaning it can be substituted for any card. The statement that she has three of a kind *reveals* that the King of Clubs is wild, and this is Secret information according to the guide. So you need subject matter expertise - in this case, a knowledge of the rules of Gin Rummy - to realize what is revealed and to correctly mark this portion '(S).'

"How did you mark the third paragraph, 'When Jim won the first hand, Paula was left with two cards. She had the Ten of Diamonds, worth 5 points, and the Queen of Spades, worth 20 points. 'T'

"I marked this one '(S)' too," Doris says. "There are two pieces of classified information in the statement. One is Confidential ('the Ten of Diamonds, worth 5 points'), and the other is Secret ('the Queen of Spades, worth 20 points'). Since the highest level of classification in this portion (paragraph) is Secret, I marked the whole portion '(S).'

the highest classification level on that page, or like marking the face of a document with the highest classification level in the entire document."

"Right on the button, Doris!



When marking a portion assign it the same classification level as the *highest level of classification of any element of information in the portion.*

Using Source Documents

"This brings up another important point:



As a derivative classifier you are responsible for *verifying a piece of information's correct level of classification 'as far as practicable'* before applying a marking.

"You've got to do your best to ensure that the markings you apply are correct. Using a security classification guide is the easiest way. Even then you've got to do a bit of research and some analysis.

"If there is no security classification guide for the information you're working with, then you must use the *portion markings of the source documents* as classification instructions, as you did for the document we marked this morning.

"If portion markings aren't available, use *page markings*. If page markings aren't available, use the *overall marking* of the source or *obtain*

classification guidance from the classifier of the source material.

"Here's an exercise that shows some of the difficulties in trying to accurately mark the portions of a derivative document, when all you have to work from are the portion markings in several source documents.

SITUATION: You need to mark your derivative document and you have no security classification guide. You must obtain your classification instructions from three source documents. The documents contain portions relevant to your document as shown.

1. A memo from the Director of DIVA:

"(U) On 1 April 1999, the R2D2 Avionics test set will be available for use. Eight sets will be deployed to West Coast operations."

2. An information paper:

"(C) Operation and maintenance manuals for the R2D2 Avionics Test Set are currently under development. Naval Weapons Center China Lake has primary responsibility for the development of the manuals. China Lake anticipates publication of the manuals by 1 February 1999."

3. A report:

"(C) Operator and maintenance manuals for the R2D2 Avionics test set will be available by 1 February 1999."

Using the three source portions, derivatively classify *and mark* these paragraphs:

1. () The R2D2 Avionics Test Set will be available for use on 1 April 1999. Eight sets will be deployed to West Coast operations.

2. () Operation and maintenance manuals for the R2D2 Avionics Test Set are being developed and will be published by 1 February 1999.

"How would you start, Doris?"

"Well, looking over the source documents I see that the information in the *Director's memo* is marked '(U).' Since the information in paragraph 1 is essentially the same information, I'd mark it '(U).'"

"Correct. How about paragraph 2?"

"Well, the information in the *information paper* source document is marked (C), so I'd mark it '(C).'"

"Are you sure, Doris? Remember..."

Portion markings indicate the *highest level of classified information contained in or revealed by the portion*. It's possible that the portion also contains *lower levels or unclassified information*.



"Let me take a closer look. Paragraph 2 contains two pieces of information:

- R2D2 Avionics Test Set operator and maintenance manuals are being developed.
- The manuals will be published by 1 February 1999.

"The paragraph in the *information paper* contains the same information. But it also contains a third piece of information:

- China Lake is responsible for the manuals.

"My gosh! Suppose the *only* Confidential information element in the information paper's paragraph is the fact that China Lake has responsibility for the manuals. Then paragraph 2 contains only *Unclassified information!*"

"That's what I wanted you to notice, Doris."

"Wait a minute! The *report source* states that the operator and maintenance manuals for the R2D2 Avionics test set will be available by 1 February 1999 - and indicates that this is Confidential information. So that means *at least one of the* pieces of information in paragraph 2 is Confidential. So I was right to mark it (C)!"

"Yes, but until you *analyzed each element and figured it out*, it was just a lucky guess.

"Let's suppose you had *no other source* to help you decide the correct classification. All you knew for sure was that paragraph 2 contained either Confidential or Unclassified information. What would you do?"

"Well, I'd try to verify the information's classification 'as far as practicable.' If I couldn't resolve it - and since I'm accountable for the markings I apply - I guess I'd mark it '(C).' I'd figure that it was better to call unclassified information classified, than to tell people that classified information was unclassified," says Doris.

"And that's just what our guidance tells us to do.



When in doubt, to ensure adequate protection mark a portion at the highest level of classification it may reasonably contain based on the sources available.

"I hope you've learned from these examples that proper derivative classification takes time, effort, and thought," Mike says.

"Even so, I suppose that after a while, for certain types of information, I won't need to refer to a

security classification guide - or to the portions of source documents. I'll have learned what sorts of things are classified at what levels."

"Doris, you're a movie buff, aren't you?"

"You know it!"

"Who won the Oscar for Best Actress in 1991?"

"Jessica Tandy for *Driving Miss Daisy*."

"Wrong! She won in 1990. Kathy Bates won it in 1991 for her role in *Misery*."

"I knew that! Just a temporary lapse!"

"That's just the type of temporary lapse you'd be liable to make if you relied on your memory and generalizations to apply markings," Mike says. "You must not rely on your memory. And you can't go by general statements like 'the range of a missile is usually classified Secret.' There are always exceptions. Don't get lazy and guess which markings to apply!"



Doris

Your memory and general statements are not authorized sources of instruction or guidance for classifying information. You should use materials such as security classification guides classified source documents project directives memoranda and plans.

"O.K., you've made your point. Well, I must admit I've been enlightened. I appreciate it, Mike. I know it's important to apply accurate markings to classified information. It gets a bit tedious, but that's no excuse for sloppy work. Now point me in the direction of the nearest DoD 5200.1-1."

Summary



In this lesson we went over some of the ways to ensure that derivative documents are classified and marked correctly as far as practicable. We said that information in a derivative document that contains or reveals classified information must be classified and marked at the same level as the level of the classified information. Portions are the building blocks of documents, so it is essential that they be classified and marked correctly. To realize when a document being developed contains or reveals classified information requires constant attention to the relationships among all of the items of information within the document, as well as the application of the developer's subject matter expertise. Only authorized classification sources may be used. Security classification guides provide the best form of guidance and are listed in the *Index of Security Classification Guides*, DoD 5200.1-1. When no guide is available, the next best procedure is to carry classifications forward from the portion markings of source documents. Portion markings reflect the highest level of classification of any information within the portion, so the portion may contain other information elements that are classified at a lower level or not classified at all. When in doubt as to the correct level of classification, to ensure adequate protection mark the portion at the highest level it may reasonably contain based on the sources available.

REVIEW EXERCISES

1. Review the following pieces of classified information:
 - The World Series features the winners of the American League and National League Championships.
 - The World Series is played in October.
 - The World Series winner must win four of seven games

Now select the statements that contain or reveal classified information.

- a. The World Series is the highlight of the baseball season. It takes place in October.
- b. The team that wins the World Series must win the best of seven games.
- c. Only the best umpires are selected to work the World Series.
- d. The opponents in the World Series come from the American League and the National League. To get to the World Series, teams must win their league championships.
- e. The major networks take turns broadcasting the World Series.

2. You are preparing to give a briefing on sources of classification instructions. As part of the briefing you must identify authorized and unauthorized sources of instructions. Next to each of the below items, indicate whether it is an authorized source (A) or an unauthorized one (U).

- _____ a. Memory.
- _____ b. Security classification guide.
- _____ c. Classified document.
- _____ d. General impressions.
- _____ e. Familiarity from having worked with the subject.
- _____ f. Regulation that provides classification guidance.

3. Use the following guidance to portion mark the document on the next page.

Red Riding Hood:

Fact that she has a Grandma	U
Lives 30 minutes walk from Grandma	U
Talks to strangers	C
Meets friends	U
Carries a care package	U
All other information concerning Red Riding Hood	U

Grandma:

Made hood for granddaughter	U
Has been ill	C
Flies a lot	S
Leaves door unlocked	C
All other information concerning Grandma	U

Wolf:

Is hungry	C
Can read	S
Lives in woods	C
Is convincing	U
Becomes impatient	U
All other information concerning the Wolf	U

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

1. Red Riding Hood's grandma loved her very much. In fact, she made the red hood for her granddaughter.
2. Grandma lived 1/2 hour's walk from Red Riding Hood. Red Riding Hood set out to deliver a care package to her grandma.
3. As Red Riding Hood was walking through the woods, she met a wolf. "I've never seen you before. What are you doing here?" asked Red Riding Hood.
4. "I live here. Where are you going?" asked the wolf.
5. Red Riding Hood explained that she was going to visit her grandma. The wolf convinced Red Riding Hood to go off into the woods and pick some flowers for her grandma.
6. As Red Riding Hood went off to pick flowers, the wolf smiled. "I haven't eaten in days. Now I'll have my fill of both Red Riding Hood and her grandma."
7. The wolf went to Grandma's house, knocked on the door, and, when there was no response, walked in.
8. There was a note sitting on the kitchen table. "Feeling much better. Using my frequent flier miles and going to Florida. Be back Saturday."
9. The wolf was disappointed. "I can't wait until Saturday. I'm too hungry. I'll just have to settle for Red Riding Hood."
10. Meanwhile, Red Riding Hood hooked up with two old friends, Hansel and Gretel, and went off to have some fun. The wolf grew impatient and left.

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

4. Portion mark the portions of this one-page document using the three source documents that follow.

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

DEFENSE PRINT PLANT ACTIVITY

30 May 1997

Subject: Fact Sheet on New and Wondrous Paper

1. When this fact sheet is exposed to light, it will become permanently set with the information it contains.
2. Because of the composition of the paper, anything printed on it cannot be reproduced using reproduction equipment currently available.
3. This type of new and wondrous paper can be used for classified defense information, for proprietary information important to a contractor, and for love letters.
4. Unfortunately, this paper is not currently available on the open market.
5. This new paper is, however, expected to be released to the public three years from the date of this memo.
6. So much for the good news. The bad news is that due to inflation, our cost for this fiscal year to buy the paper will go up \$65,000. This represents an average increase of \$3.25 in cost per sheet.
7. Ground Hog Manufacturing has the contract to produce the XP-1. They are currently producing only a small amount of paper. We are negotiating with them to see if they will increase their production. They seem reluctant to do so.
8. We feel, however, that they can be persuaded to increase production in the national interest. We have asked the IRS to look into the situation.

I.M. Sure
Chief, Research Department

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

SECRET

DEFENSE PAPER MILL ACTIVITY
RICHMOND, VA 23297

DPMA-RD

22 February 1995

SUBJECT: New and Wondrous Paper (U)

TO: Defense Print Plant Activity
ATTN: DPPA-SS
Gutenberg, VA 23386

1. (S) One of our contractors is currently producing a new and wondrous type paper. When the paper is exposed to light, whatever is printed on it will become permanently set. It cannot be reproduced using any reproduction equipment available.

2. (U) Uses of this document paper include classified defense information, proprietary information important to a contractor, and love letters sent to anyone that one may choose.

FOR THE DIRECTOR

R.I. Cepaper
Division Chief, Research & Development

Classified by: Report on New Paper, DPMA-RA, 1 Jan 94

Declassify on: OADR

SECRET

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

SECRET

DEFENSE PAPER MILL ACTIVITY
RICHMOND, VA 23297

Memo to all DPMA Chiefs:

1. (S) Ground Hog Manufacturing (GHM) has the contract to produce the XP1. We are currently trying to negotiate with them to produce larger quantities of the paper. At present they are reluctant to increase production, however, we feel sure that GHM can be persuaded to do so in the national interest. We have also asked the IRS to see if it might be in GHM's best interest to increase production.
2. (C) The paper is not currently available to the public but we expect to be releasing this new paper to the public on 30 May 2000.

N.E.W. Sprint
Director

Classified by: Director, DPMA
Declassify on: 1 Aug 2002

SECRET

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

Source #3

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

SECRET

15 March 1995

Sam,

This new paper is great. Here are some figures that I worked up yesterday on production and cost.

This fiscal year cost for total production - \$1,165,000

Last fiscal year cost for total production - \$1,100,000

Net increase -\$ 65,000

This year the cost of each sheet of paper will go up by over \$3.25 over last year.

Joe

P.S. Remember, this cannot be reproduced because of the paper, so if you want another copy you have to type it.

SECRET

5. You are preparing to apply classification markings to a derivatively classified document. You have placed two information elements into paragraph 12 of your document. You look in the applicable SCG and find that both elements are classified; one is Secret, the other is Confidential. You should mark paragraph 12 with the Confidential portion marking. This is because over classification is a primary concern for the Information Security Program.

True. False.

6. The person in the best position to derivatively classify a document is the typist since that person is familiar with the information that is being typed and that person is already working with the document.

True. False.

7. Derivative classification is a responsibility of all who incorporate, paraphrase, restate, or generate in new form classified information.

True. False.

8. Whenever you mark the various parts of your classified document, you must mark them according to the classification level of the information which that particular part _____ or _____ .

9. A security classification guide is the source of classification instruction _____
_____ .

SOLUTIONS AND REFERENCES

1. Based on the classified information that was provided, the following statements contain or reveal classified information.
 - a. The World Series is the highlight of the baseball season. It takes place in October.
 - b. The team that wins the World Series must win the best of seven games (Best of seven games is four of the seven games.)
 - c. The opponents in the World Series come from the American League and the National League. To get to the World Series, teams must win their league championships. (pp. 5-3-5)

2.
 - a. U - unauthorized
 - b. A - authorized
 - c. A - authorized
 - d. U - unauthorized
 - e. U - unauthorized
 - f. A - authorized (p. 5-14)

3. CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

1. (U) Red Riding Hood's grandma loved her very much. In fact, she made the red hood for her granddaughter.
2. (U) Grandma lived 1/2 hour's walk from Red Riding Hood. Red Riding Hood set out to deliver a care package to her grandma.
3. (C) As Red Riding Hood was walking through the woods she met a wolf. "I've never seen you before. What are you doing here?" asked Red Riding Hood.
4. (C) "I live here. Where are you going?" asked the wolf.
5. (U) Red Riding Hood explained that she was going to visit her grandma. The wolf convinced Red Riding Hood to go off into the woods and pick some flowers for her grandma.
6. (C) As Red Riding Hood went off to pick flowers, the wolf smiled. "I haven't eaten in days. Now I'll have my fill of both Red Riding Hood and her grandma."
7. (C) The wolf went to Grandma's house, knocked on the door, and, when there was no response, walked in.
8. (S) There was a note sitting on the kitchen table. "Feeling much better. Using my frequent flier miles and going to Florida. Be back Saturday."
9. (S) The wolf was disappointed. "I can't wait until Saturday. I'm too hungry. I'll just have to settle for Red Riding Hood."
10. (U) Meanwhile, Red Riding Hood hooked up with two old friends, Hansel and Gretel, and went off to have some fun. The wolf grew impatient and left.

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

Paragraph 1 is Unclassified. The classification guidance states the facts that Red Riding Hood has a grandma and that grandma made the hood are both Unclassified information elements.

Paragraph 2 is Unclassified. The classification guidance states the facts that Red Riding lives 30 minutes walking distance from her grandma and that grandma receives care packages are both Unclassified information elements.

Paragraph 3 is Confidential as it reveals that Red Riding Hood talks to strangers.

Paragraph 4 is Confidential because it contains the fact that the wolf lives in the woods. Paragraph 3 tells you that Red Riding Hood was walking through the woods when she met the wolf. Paragraph 4 is the wolf's response to Red Riding Hood's question about where he lives.

Paragraph 5 is Unclassified because the facts that Red Riding Hood has a grandma and that the wolf is convincing are both Unclassified information elements.

Paragraph 6 is Confidential because it reveals that the wolf is hungry. He says he hasn't eaten in days.

Paragraph 7 is Confidential because it reveals that grandma leaves her door unlocked. When there was no answer to his knock, the wolf walked through the door into Grandma's house.

Paragraph 8 is Secret. It reveals two information elements: that grandma has been ill and that grandma flies a lot. The fact that grandma has been ill is Confidential. The fact that grandma flies a lot is Secret. Mark the portion with the highest level of classified information in the portion.

Paragraph 9 is Secret. It contains/reveals two information elements: that the wolf is hungry (Confidential) and that the wolf can read (Secret). Mark the portion with the highest level of classified information in the portion.

Paragraph 10 is Unclassified. The facts that Red Riding Hood meets friends and that the wolf is impatient are both Unclassified.

(pp. 5-3-5, 12)

4. CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

DEFENSE PRINT PLANT ACTIVITY

30 May 1997

Subject: Fact Sheet on New and Wondrous Paper (*E9*)

1. (S) When this fact sheet is exposed to light, it will become permanently set with the information it contains.
2. (S) Because of the composition of the paper, anything printed on it cannot be reproduced using reproduction equipment currently available.
3. (U) This type of new and wondrous paper can be used for classified defense information, for proprietary information important to a contractor, and for love letters.
4. (C) Unfortunately, this paper is not currently available on the open market.
5. (C) This new paper is, however, expected to be released to the public three years from the date of this memo.
6. (S) So much for the good news. The bad news is that due to inflation, our cost for this fiscal year to buy the paper will go up \$65,000. This represents an average increase of \$3.25 in cost per sheet.
7. (S) Ground Hog Manufacturing has the contract to produce the XP-1. They are currently producing only a small amount of paper. We are negotiating with them to see if they will increase their production. They seem reluctant to do so.
8. (S) We feel, however, that they can be persuaded to increase production in the national interest. We have asked the IRS to look into the situation.

I.M. Sure
Chief, Research Department

CLASSIFICATION MARKINGS ARE FOR TRAINING PURPOSES ONLY

Subject line is Unclassified based on guidance from subject line of Source 1.

Paragraph I is Secret based on the guidance of Paragraph 1, Source 1. No other document contains information concerning the element, so the portion is marked (S).

Paragraph 2 is Secret based on the guidance of Paragraph 1, Source 1 and the last paragraph of Source 3. Note that Source 3 does not contain portion markings. Sometimes you'll encounter documents that are not marked with all required markings. If portion markings are not available, use page markings as guidance.

Paragraph 3 is Unclassified based on guidance in Paragraph 2, Source 1.

Paragraph 4 is Confidential based on the guidance in Paragraph 2, Source 2.

Paragraph 5 is Confidential based on guidance in Paragraph 2, Source 2 and the date of your document.

Paragraph 6 is Secret based on information contained in Source 3.

Paragraph 7 is Secret based on Paragraph 1, Source I and on Paragraph 1, Source 2.

Paragraph 8 is Secret based on Paragraph 1, Source 2.

(pp. 5-3-5, 10-11, 13)

5. False. We mark a portion to indicate the highest level of classification of the information contained in it. A weakness within the system is that not all information in the portion might be at the highest classification level and, therefore, the potential exists that in the future anyone extracting information from the portion could conceivably be classifying an item of information at a higher level than it really is.
(p. 5-12)
6. False. The person doing derivative classification should be the subject matter expert.
(p. 5-5)
7. True. (p. 5-2)
8. contains
reveals (pp. 5-3-5)
9. most reliable (p. 5-6)

LESSON 6

EFFECTIVE SECURITY PRACTICES



handling classified information
in the workplace

In your workplace you and your co-workers have a set of job responsibilities. You have to follow all sorts of procedures from ordering supplies and sending mail to making coffee. The workplace that handles classified information needs to establish special procedures to avoid unauthorized disclosure of classified information and to deter anyone from removing classified information without authorization.

In this lesson, you'll learn about handling classified information in the workplace. We'll tell you who classified information custodians are and identify some of their responsibilities. We'll discuss protecting information when it has been removed from storage, handling office materials that contain classified information, using secure telephone circuits for classified discussions, seeking approval for taking classified materials home to work on, reproducing classified information, securing the workplace at the end of the day, and handling working papers. At the end of this lesson, you will be able to do the following:

- Recognize the responsibilities of those who handle classified materials in the workplace.
- Use Standard Forms 701, 702, 703, 704, and 705 under appropriate circumstances in the workplace.

- Properly handle office supplies and work materials that contain classified information.
- Identify precautions in the use of a secure communication circuit.
- Identify the requirements for taking classified materials home to work on.
- Identify requirements for reproduction of classified information.
- Properly handle working papers.



Responsibilities of Custodians

Rich Martin is having lunch in the cafeteria and is reading *The Washington Post* when he hears, "Hi, Rich. Mind if I join you?"

"Well if it isn't Wally Chin! Sure. Pull up a chair."

"Everything OK with your division?" Wally asks.

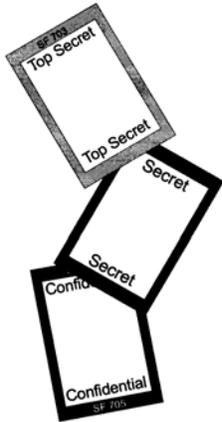
"Yeah, I think so. You know, working in an office that handles classified information is certainly different from being in one that doesn't. There's a whole new set of responsibilities. It seems like the first thing I have to get through to people is that when they are in possession of classified information, they are the *custodians* of that information. And as custodians, they have certain responsibilities.



Responsibilities of Classified Information Custodians

Persons who have possession of or who are otherwise charged with safeguarding classified materials are responsible for...

- * Providing protection for such information at all times.
- * Ensuring that classified information is locked in appropriate security equipment whenever it is not in use or under direct supervision of authorized persons.
- * Verifying a person's need-to-know and clearance before providing that person with any classified information.
- * Following procedures to ensure that unauthorized persons do not gain access to the classified information.



"I explain to them that when their supervisor hands them a Confidential document to use as reference material while they are working on a project, they become the custodian for the document. So it's up to them to ensure that anyone who is not *authorized* access to the information in the document does not *get* access to the document. And while they are actually working with the document, they must *keep it under their direct control - under* constant surveillance. And that when they are *not* working with the document, they should *lock it up* in an approved storage container or facility or *keep it under constant surveillance* – or they should ask another person who is authorized access to the material (properly cleared with a need to know) to *watch over* the materials."

"Right, Rich. You and I have security-related job responsibilities, so we think about security a lot. But the technical staff is wrapped up with the nuts and bolts of their projects. It's obvious to us what a custodian of classified materials must do to protect them, but it's not obvious to others. They need reminders and procedures to make security a habit."

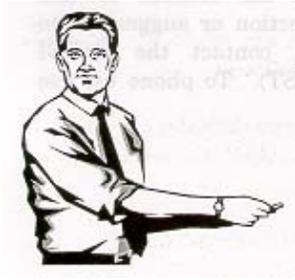
SF 703, 704, and 705 - Cover Sheets

"True, Wally. When I first came to the Weapons System Division I put up *security posters* to remind people to always protect the classified materials in their possession. And we try to encourage good security practices and to reinforce them."

"Such as?" Wally asks.

"For starters, we remind them to place *cover sheets* on the documents when they take them out of storage.

And we make sure that they know that the cover sheet they need to use will *vary with the classification level of the document* that they are handling.



The Three Cover Sheets

Standard Form 703 (Orange) - Top Secret documents

Standard Form 704 (Red) - Secret documents

Standard Form 705 (Blue) - Confidential documents

"I remind our people that cover sheets serve two purposes: they *block the classified information from view* so no one can read it and, more important, they *remind the person working with the document that they have classified material* in their work area. I emphasize that they should block the classified document *immediately* when someone who is not authorized access to the information comes by."

Office Supplies and Work Materials

"Keeping an eye on classified documents is probably job one," Wally says. "But I also remind people to protect other items in the office that contain classified information. They need to remember that..."

Preliminary drafts worksheets printer ribbons and other materials containing classified information shall either be destroyed immediately after they have served their purpose or shall be given the same classification and secure handling as the classified information they contain.



"I remind folks that these are preliminary products or means to a final product, not a final product, and that they should *destroy them properly once they have served their purpose*. For instance, I tell our clerical people to destroy right away any drafts they may have worked up when creating a classified document. And that printer ribbon, too. I stress that until they actually destroy the materials, though, they need to protect them - either keep them under *constant surveillance* or secure them in the *proper container*.

"And I point out other materials in the office that they may have to protect. For instance, a 'post-it' note placed on a classified document may pick up the imprint of the information on the adhesive. I remind them to properly destroy the note as soon as possible - or protect it properly. And I challenge them to find other items that could pose a problem. When they do, I make sure to tell them they're great!"

Classified Discussions on the Telephone



"And how about reminding them not to discuss classified information on their regular office telephones?" Rich says. "I must sound like a record: 'Discuss classified information only over phones with approved secure communications circuits.' Remember when we had just one secure telephone for all of DIVA? It took an act of Congress to get access to it! Now so many of us have a STU-111 (Secure Telephone Unit) that finding a secure phone is no big deal."

"But," Wally says, "just having a STU-III is not enough. They need to be briefed on how it works. I've met people who think that just because their telephone

is a STU-III it's always secure! They think they can just make a call and start talking classified! We need to make sure that every STU-III user knows how to use it properly. And that they know who is nearby when they're using it! They may forget that others in the office can hear their end of the conversation if they are not careful.

Working with Classified Materials at Home



"I met one guy," Rich says, "who was working on a classified project and didn't see why he couldn't stick classified papers in his briefcase and take them home. It took fifteen minutes to convince him that he needed special authorization to remove classified information from the workplace to work on it at home. "I explained to him that for Secret and Confidential materials the authorization has to come from the head of a DoD Component or that person's single designee at the headquarters or major command level - in our case General Kent. For Top Secret materials the authorization has to come from one of the four Secretaries (Defense, Air Force, Army, or Navy), a combatant commander, or a Senior Agency Official for the Component. I told him that even if he did get authorization to take work home, he'd have to have a GSA-approved security container to store the information in when it was not in use."

"Yeah," Wally says, "And not only that, I'm not sure why anyone would want to take classified materials home to work on. It's hard enough to protect the materials here at work, let alone protect them at home!"

If you need to work with classified materials at home you must...

- Get authorization from:
- for Top Secret:
SECDEF, SECAF, SECARMY, SECNAV; Combatant Commander; or
Senior Agency Official of Component
- for Secret:
Head of DoD Component; or Designee at Headquarters or Major
Command.
- Have a GSA approved security container at home.
- Protect the materials at all times.

"Rich, that's enough shop talk for one lunch! If we don't get onto the Redskins or my Bermuda grass, I'm outa here!"

Rich laughs. "OK, Wally. How's your Bermuda grass?" With that, Rich and Wally discuss the woes of trying to maintain a lawn in Northern Virginia.

Reproduction Limitations

Rich returns to his office. Before long, Denise Torrez knocks at his door.

"Hi, Denise. How'd the review of your control systems go this morning?" Rich asks.

"Everything was fine. Hey, listen. Have you seen Major Jenkins? I need to get him to get some

additional data for a project we're working on. And by the way, where's the copier? I need to make a copy of this Secret document and give it to Sue over at the Operations Office."



Denise Torrez

"Haven't seen the Major. I just got back from lunch. I ran into Wally Chin from the Security Office. I'll bet the only security topic we *didn't* cover was reproduction of classified information."

"Too bad," Denise replies. "Want to go over it now? This seems like a great time for a review. I know that any office that reproduces classified materials has to set up procedures to ensure that originals and copies are properly protected. But aren't there some special circumstances when you need to do more than just run the copy machine?"

Yes, the originator must be contacted to authorize the reproduction of the classified information if it is marked:

Reproduction requires approval of originator or higher DoD authority.

"There is no specified method for getting this approval, so just use your best judgment. Use a phone, send a letter, send a FAX, or whatever will work best.

"But it doesn't stop there, Denise. People who receive the copies have to take precautions when dealing with them," Rich says. "They've got to remember that..."

All copies of classified documents reproduced for any purpose including those incorporated in a working paper are subject to the same controls prescribed for the document from which the reproduction is made.

"So if the *originals* were accounted for in an accountability system, the *copies* must be too. And make sure that the copies are *marked*, so those who handle the copies will see that they have classified materials in their possession.



Denise and Rich

"What's more, Denise," Rich goes on, "we at DIVA have had to find out what vulnerabilities and weaknesses are inherent in the copiers that we use. We studied hard to find out how the copiers worked. We needed to find whether any images were retained within the copier after the copying. If images were being left within the machines, we would have had to put the copier inside a secure area or take whatever actions would erase or eliminate the retained images. And we would have had to make our people aware of the vulnerabilities and the preventive measures."

"Are these the 'latent images' that I keep hearing about?" Denise asks.

"Yes, a latent image is one copier vulnerability. The machine retains an image and places that image on the following page - or on a number of following pages. In most cases, running a number of blank copies through the machine will take care of this problem."

SF 701 End-of-Day Security Check

Let's leave Rich and Denise, and talk about security checks. Each activity that processes or stores classified information must establish a system of security checks at the close of each working day. *Standard Form 701, Activity Security Checklist* is used to record these checks. A sample SF 701 is on the next page.



Note especially that this end-of-day check involves more than just verifying that the security container is properly locked. When you perform this check, in addition to checking the container, you should *check around your work area* to include your desk, your inbox, your out-box, your desk top, the trash can, the copier (if there is one located in your work area) and any other place that classified materials *might inadvertently be left*. And you should perform the check if you work *after hours*, or on *weekends* and *holidays*, and access classified materials. The idea is to ensure that you have not inadvertently left classified materials *unsecured*.

SF 702 - Security Container Check Sheet

All vaults, secure rooms, and containers used for the storage of classified material must be secured at the end of each workday. *Standard Form 702, Security Container Check Sheet* is used to record this. A sample SF 702 is shown on the next page.



The SF 702 is also used to record your *opening and closing of the container*. Although the DoD regulation does not specify that you must do this, it's a good idea to fill out the form every time you take an action with the container - whenever you open it, lock it, and check it to verify that it's locked. Some people fill out the form only in the morning when they first unlock the container and in the afternoon when they lock it for the last time that day. There are no specific prohibitions on doing it this way. But when you look at the functions for the form you can see that the benefits gained by filling it out each time you take an action with the container outweigh the few seconds it takes to fill out the form.



The SF 702 serves two functions. First, it is a *record* of what actions have been taken with the container. You can use this record in a number of ways. If there is an open container violation, the form helps to narrow the scope of the inquiry. The form can also give you an idea of the use of the container. Second, the form serves as a sort of reverse *reminder* to take certain actions with the container. You take an action, you fill out the form. You take an action, you fill out the form. You take an action, you fill out the form. Before long the behavior has become a habit. And this is one habit you'll be glad you have.

Finally, if you work at your office *after hours*, or on *weekends* and *holidays*, and you open your container, you need to complete the SF 702.

Handling Working Papers



"Working papers" are classified documents and materials that are created in preparing a finished document. They are the drafts, notes, and other items you make when you are developing a document. Working papers are not final products. They only lead to a final product.

DoD 5200. 1-R recognizes that requiring people to put all of the security markings (portions markings, applicable associated markings, etc.) on a working paper would impose an administrative burden. So the regulation allows you to place only the *overall classification marking* at the top and bottom of each page of the working paper and to *date* the working paper. No other markings are required. As with other preliminary materials, you should get rid of (properly

destroy) each working paper *as soon as it has served its purpose*. To ensure that working papers are destroyed promptly, DoD 5200.1-R imposes limitations on how long you can label a draft, note, etc. a "working paper."

Working papers that contain classified information should be handled in the same manner as a *finished document* when...

- * Released outside the activity**
- * Retained more than 180 days from date of origin**



Suppose, for example, you are writing a classified report to your commanding officer on a project. Since it's almost impossible to just sit down and create the report in its final form on the first try, you end up writing a number of drafts of the report until you get it into its final form for submission to your commander. You can simply mark each page of your drafts with the overall classification of the report at the top and bottom and place on it the date that you wrote the draft. You are not required to put portion markings on the drafts nor are you required to place the associated markings on it. (However, even though you are not required to do so, you may find that you are better off doing so since you will need to place the portion markings and associated markings on the final version anyway. And if you have those markings on the drafts already, you won't have to go back and do research to find out what the proper portion markings and associated markings are for the final version.) As soon as you have completed the final version, properly destroy those drafts. Keep in mind, though, that if you should send the draft to another activity you will have to place all of the final markings on that draft. And if that draft is kept more than 180 days, you will need to put all of the final markings on it.

Summary



In this lesson, you learned about practices required in workplaces that deal with classified information. You learned that anyone who possesses classified information is considered a classified information custodian. Custodians of classified information have safeguarding responsibilities, such as keeping it under constant surveillance or locking it up in a proper storage container or facility and ensuring that only authorized persons get access to it. Cover sheets -specific to the level of classification of the document covered - are used to block the view of classified documents from unauthorized persons and to remind the authorized user to monitor the documents while in use. Office supplies and work materials that contain classified information should be destroyed as soon as possible after they have served their purposes or protected properly. It is essential to follow proper procedures when using the STU-111 to discuss classified information and to ensure that unauthorized persons do not overhear classified conversations. Classified material may be worked on at home only if authorization at the required level is obtained, there is a GSA-approved security container at home, and the materials are protected at all times. Copies of classified information must be marked, controlled, and protected like the originals, and copier vulnerabilities must be overcome. SF 701 records end of-day security checks, while SF 702 records the opening, closing and end-of-day securing of the security container. A working paper need be marked only with the overall classification and the date; it should be destroyed as soon as it has served its purpose. It should be fully marked and handled as a finished document when released outside the facility or retained more than 180 days from its date of origin.

REVIEW EXERCISES

1. Enter the appropriate cover sheets.
 - a. Confidential document _____
 - b. Secret document _____
 - c. Top Secret document _____
2. Circle the letter of each true statement.
 - a. Custodians of classified information should verify a person's need-to-know and clearance before providing him or her classified information.
 - b. Classified information may never be discussed over the telephone.
 - c. A printer ribbon used in the development of a Secret document should be safeguarded like the Secret document.
 - d. Local installation commanders can authorize working at home with Secret materials.
3. If a classified document is removed from a security container, it must be under your _____ at all times.
4. SF 701 records the _____ made at the _____ of each day.
5. Circle the letter of each true statement.
 - a. Rules to reproduce classified information must be posted at all copiers.
 - b. Copies of classified documents must be controlled like the originals.
 - c. A designated official must approve requests to copy Secret information.
 - d. Specific copiers must be designated to reproduce classified information.
6. If you work with classified materials in your office during the weekend, you do not need to complete the SF 701 when you finish for the day.

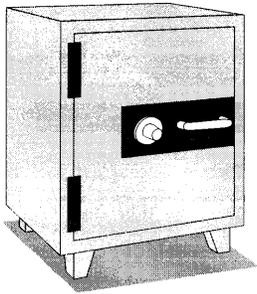
True False.
7. SF 702 records the securing of _____, _____, and _____ at the _____ of each _____ day.
8. A working paper is controlled as a finished document when it is released _____ or retained more than _____ days.

SOLUTIONS AND REFERENCES

1.
 - a. Confidential documents - Standard Form 705
 - b. Secret documents - Standard Form 704
 - c. Top Secret documents - Standard Form 703 (p. 6-5)
2.
 - a. True. (p. 6-3)
 - b. False. Classified information can be discussed over secure phone lines. (pp. 6-6-7)
 - c. True. (pp. 6-5-6)
 - d. False. DoD Component heads or their single designees at the headquarters or major command level must authorize working at home with Secret and Confidential materials. (pp. 6-7-8)
3. "constant surveillance" or "direct control." (p. 6-4)
4. SF 701 records the security checks performed at the end of each work day. These checks are conducted to ensure that no classified materials are left out at the end of the day. (pp. 6-10-12)
5.
 - a. False. This is a good idea, but it is not required.
 - b. True. (pp. 6-9-10)
 - c. False. Reproduction approval officials are not required. The only time you would need to get approval is when the originator of the document requires prior approval for reproduction.
 - d. False. This is a good idea, but it is not required.
6. False. People must complete the SF 701 if they work after hours, on weekends, or holidays and access classified materials. (p. 6-12)
7. The SF 702 records the securing of vaults, containers, and secure rooms at the end of each work day. (p. 6-12)
8. outside the facility, 180. (p. 6-15)

LESSON 7

SAFEKEEPING AND STORAGE



Since most classified information spends far more time not being used than being used, the safekeeping and storage of classified information is extremely important. And sometimes the measures that the Government takes to safeguard classified information are surprising. Did you know, for instance, that of the two approved standalone containers for Secret information, one provides little protection against forced entry - and the other provides none at all? In this lesson, we'll explore the rationale behind this apparent lack of security: the concept of minimum risk. We'll also explore the literal "nuts and bolts" of security - the physical equipment and devices used to store classified information. We'll see when to use them, how to procure them, and how to keep track of the level of classified in each of them. We'll talk about the locks and locking devices that secure them and how to handle the combinations for them. We'll wind up with a few words on repairing them and on safeguarding classified information in foreign countries. At the end of this lesson, you will be able to do the following:

- Identify the types of threats that security containers and facilities for classified storage are designed to protect against.
- State the principle of minimum risk.



Lt. Col. Bill Timmons

- Identify storage requirements for the different levels of classified information.
- Select the locks used for protecting bulky classified materials and state the procedures used with the locks.
- Select and procure appropriate storage equipment for classified information.
- State the procedures for designating containers.
- List the conditions that require changing a combination.
- Identify properly restored security equipment. Lt. Col. Bill Timmons
- List the methods of safeguarding classified information in foreign countries.

Storage equipment and procedures seldom change, so people tend to take them for granted and often become careless about their use. This is no less a problem for DIVA than for any other organization or agency.

To reduce the danger of such carelessness, Lt. Col. Bill Timmons, Chief of the Security Branch, routinely assigns a new person to the job of overseeing the procedures for use and security of storage containers within DIVA. Mike Carson, a new hire, was recently appointed to replace Wally Chin for these duties.

Let's look in on their meeting in Wally's office.

Types of Threats

"Mike," Wally says, "the first thing to keep in mind is that we try to provide protection against two types of threats.

We try to protect against...

- **Inadvertent disclosure**
- **Deliberate attempts to gain access**



Mike knew that inadvertent disclosure was when classified information is disclosed *unintentionally*. "It seems to me," says Mike, "that inadvertent disclosure would most likely occur when classified documents or materials are in use. Isn't that why we use cover sheets? So that no unauthorized person - even someone who doesn't mean to - can look down at an open document on a desk and see classified information not intended for his eyes?"

"That's true," says Wally. "Inadvertent disclosure can even occur while a person is removing a classified document from a storage container or replacing it. But imagine how much inadvertent disclosure there would be if classified information were stored in unlocked, easily accessible containers! Unauthorized persons could accidentally open a file with classified while innocently searching for unclassified materials. Secure containers prevent this threat."

"I can see that," Mike says, "But what about *deliberate* attempts to gain access? Why doesn't everyone use the best safe available?"

"Actual dollar *costs* limit the practicality of that approach," says Wally. "Besides, *no container exists that can defend against a determined effort to gain access.*"

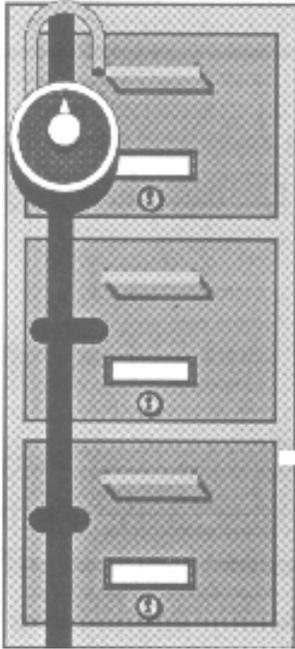


"Faced with these real world considerations, the *Government does not seek absolute physical security of all classified information.* Instead, the Government relies on the fact that a person who wants to gain illegal access to classified information *does not want to leave evidence* that the information has been compromised. For one thing, discovery of the compromise would bring on an investigation and the possibility of apprehension. Then, too, when the Government detects a compromise, the information usually loses its value, since the Government can take action to counteract the damage. And so we focus on *deterrence through probable detection.* For one thing, we use safeguards that would show, *by the evidence left,* that a breach in security has occurred.

Minimum Risk

"At the same time, though, we don't want to make it easy to get at classified information! If all we cared about were the evidence left, we could just blow up a balloon around the information every night when we left! What we want is protection that *makes a forced attempt to gain unauthorized access obvious* and that *substantially prolongs a more subtle attempt,* such as manipulating the combination dial.

With enough delay, the attempt will be thwarted by the arrival of installation personnel.



"Since we are *act* seeking *absolute security*, we are willing to take certain risks. Security of classified information may be compared to the safety of the car that you drive. Most of us do not select the absolute 'safest' car on the road. We compromise. Big cars are usually safer than small ones, but most of us don't buy the biggest car because of parking, maneuverability, and cost.

"Within the constraints of our needs, desires, and funds, we set an *acceptable level of risk* or *IniniM11772 risk* that we will have an accident or be injured in an accident.

The same is true for security of classified information. Our main goal," Wally continues, "is to provide a minimum risk that deliberate attempts to gain access will be successful.

"We base the *level of the risk* on the *level of classification* of the information that we are protecting. The *higher* the classification of the material, the *lower* the risk we are willing to take. And so the *higher* the classification, the *more stringent* is the physical protection standard for that material."

MINIMUM RISK

- * **Based on level of classification**
- * **Local situations can influence how much risk is taken**

"Does that mean that the same information may be protected in different ways at two different locations?" asks Mike.

"That's exactly right," says Wally.

Storage methods vary according to the *nature and size of the activity* its *mission* and the *level and type of classified information*.

"The effectiveness of the storage methods may be equal even though the methods themselves are different."

"I'm not sure what you mean by that," Mike replies.



"Well, for example, at one installation they may be storing Confidential documents in a GSA-approved security container that is located in a locked office with no alarms or any other security measures to protect the container. At another installation, the same document might be stored in a lock bar cabinet that is located in a locked office that is protected with an alarm system as well as a magnetic badge reader. Both systems do the job."

"And notice that they both use *several* security measures. You should not use just a security container by itself when securing classified materials. Storage procedures should incorporate other physical security elements, such as locked doors, location of containers, and container records."

Mike says, "Still, there are times when a container can be used by itself, right? So doesn't there have to be some uniformity in the protection they provide? Don't they have to meet some sort of standards?"

Standards for Storage Equipment

"You bet they do, Mike."

There is a security container in the office and Wally walks over to it.

"This cabinet had to meet the *General Services Administration's* (GSA) criteria for storage equipment used for classified information."



Wally Chin

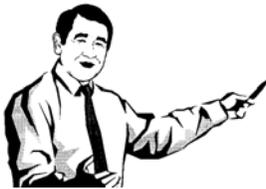
The GSA establishes and publishes minimum standards, specifications, and supply schedules for:

- Containers
- Vault doors
- Modular Vaults
- Alarm systems
- and
- Associated security devices suitable for the storage and protection of classified information.

"GSA writes the specifications for the containers, then the container manufacturers submit their products for testing against the standards. If the product meets the specifications, GSA certifies it. GSA does the same for vault doors and for modular vaults.

"Alarm systems and associated security devices that are used to protect classified information should also meet standards set by GSA. Associated security devices are biometric machines used to determine if a person is authorized access to the classified materials - fingerprint readers, palm geometry readers, retinal eye scanners, etc. GSA is currently updating these specifications. When they are finalized, GSA plans to implement testing and certification procedures.

"And take a look at this," Wally says, pointing to the label affixed to the *outside of the locking drawer*.



General Services Administration
Approved Security Container

"When you see this GSA *approval* label you know that the cabinet was manufactured *after 1962*. That's when GSA formalized the certification program and started placing this label on storage equipment authorized for classified materials."

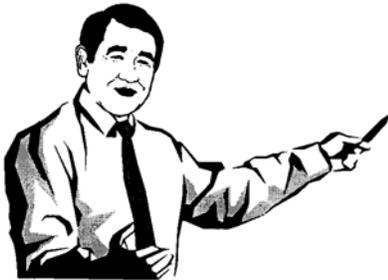
Mike sees a second label located on the *side of the container's locking drawer*. "What's this, Wally?"

THIS IS A U.S. GOVERNMENT CLASS 6 CABINET WHICH HAS BEEN APPROVED BY GSA UNDER FEDERAL SPECIFICATION AA-F-358G. IT AFFORDS THE FOLLOWING PROTECTION:

- 20 MAN-HOURS AGAINST SURREPTITIOUS ENTRY
- 30 MAN-MINUTES AGAINST COVERT ENTRY
- 0 MAN-MINUTES AGAINST FORCED ENTRY

"It's a GSA *test certification* label, Mike. With older equipment you sometimes find it on the inside wall. Notice that the label shows *zero man-minutes against forced entry*. Remember what I said earlier about deterrence through probable detection? When individuals (or governments) want illegal access to classified information, they usually want that access to occur in such a way that the authorized holder of the information does not know that the information was compromised. We say they want the entry to be *covert* or *surreptitious*, an entry that does not leave physical evidence. So even though the cabinet itself can be broken into in nothing flat, it is a rare situation when someone uses a sledge hammer to open it to get at classified materials!

"And here's the *identification* label," Wally says. "It contains four items of information.



- 1. Cabinet Model**
- 2. Serial Number**
- 3. Year of Manufacture**
- 4. Contract Number**

"It's important to know that this information can be found on this third label," says Wally, "because every once in a while we receive notices about taking certain actions with containers. And the criteria that the notices use to identify the affected containers are the data on this label."

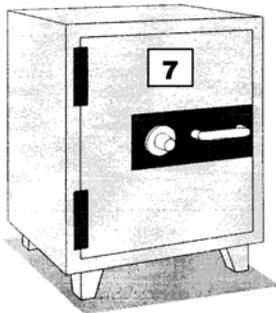
"Is there a way for a visitor to know the classification of material stored in any container simply by looking at it?" Mike asks.

"No," says Wally. "For one thing, it's acceptable to store Secret and Confidential documents in Top Secret storage devices. So it's conceivable that a container in which it's O.K. to store Top Secret materials might only contain a Confidential document. Then, too, heads of DoD Components may establish more stringent standards. Thus standards may vary among components. If that weren't enough, it is also *prohibited* to indicate the authorized level of storage on the outside of a container!"

Storage Requirements for Classified Information

"I haven't thought a lot about the container that I use to store my Secret documents," says Mike. "I guess I just assume that it meets the standards for Secret storage."

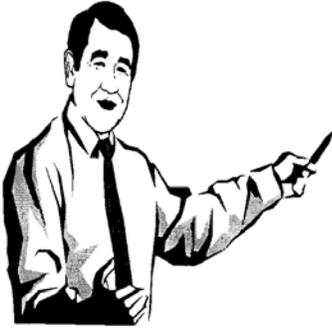
"Can you describe the container and its locking mechanism?" asks Wally.



"It's the gray safe in my office. It has a sticker with the number 7 on the outside. It has a 3-position combination lock. I'm pretty sure that there's a test certification label inside."

"Good old number 7!" says Wally. "It meets the container standards for storage of Top Secret information."

"I know it's been some time since you studied the minimum requirements for storing classified materials. Let me review them with you."



Top Secret information can be stored in a...

- GSA-approved security container with supplemental controls
- Vault (meeting DoD standards) with IDS
- GSA-approved modular vault with IDS
- Secure room (meeting DoD standards) with IDS

"IDS stands for *intrusion detection system*. An IDS is an electronic alarm system that operates by detecting motion, heat, sound, or other disturbance in the protected area. Note that if you store *Top Secret* materials in a GSA-approved security container, *supplemental controls* must be applied.

Supplemental Controls for
GSA-Approved Security Container
Storing Top Secret Information

One of the following must be applied in addition to the container itself.

1. A location under continuous protection by cleared guards or duty personnel
2. Inspection of the container once every 2 hours by cleared guards or duty personnel
3. An IDS which meets the standards specified in DoD 5200.1-R
4. Security-in-depth if the container has the Mas-Hamilton X-07 lock

"You can also use a vault, a GSA-approved modular vault, or a secure room to store Top Secret material.

Top Secret Storage – Compartments

A vault must meet the specifications noted in DoD 5200.1 -R *and be* protected by IDS or be under constant surveillance.

A GSA-approved modular vault must be protected by IDS or be under constant surveillance.

A secure room must meet the specifications noted in DoD 5200. 1-R *and be* protected by IDS or be under constant surveillance.

Mike asks, "What about Secret information? Does it have to be stored exactly like Top Secret?"

"The requirements are not as stringent," Wally replies. "Secret information is not as sensitive as Top Secret information, so we are willing to take a little more risk with it."

Secret information can be stored in...

- The same manner prescribed for Top Secret storage
- GSA approved security container or vault without supplemental controls
- A secure room (meeting standards established prior to 1 Oct 95 by the head of the DoD Component concerned)
- Until 1 Oct 2002, a steel filing cabinet with a built-in three position changeable combination lock, with supplemental controls
- Until 1 Oct 2002, a steel filing cabinet equipped with a steel lock bar secured by a GSA-approved changeable combination lock, with supplemental controls



"The two steel filing cabinets with their locking hardware are the containers that the Government used to store classified materials *prior to the GSA approved container program*. And remember, I said that this program started *in 1962*, so these cabinets are *very old equipment*. Even though DoD activities have until *October 2002* to get rid of them, DIVA has phased out most of them already.

"Confidential materials can be stored in the same containers or facilities as Secret materials and do not require supplemental controls."

Minimum Storage Requirements

Top Secret	Secret	Confidential
<ul style="list-style-type: none"> • GSA approved container with supplemental controls • Vault with IDS • GSA approved modular vault with IDS • Secure room with IDS 	<ul style="list-style-type: none"> • Same as TS • GSA approved container or vault without supplemental controls • Secure room approved by Component Head • prior to Oct 95 • Non-GSA approved steel filing cabinet with supplemental controls (until Oct 2002) • Lock-bar cabinet with supplemental controls (until Oct 2002) 	<ul style="list-style-type: none"> • Same as Secret without supplemental controls

Storing Bulky Materials

"What about storing bulky classified items, like equipment?" Mike asks. "I know we don't have any here at DIVA, but how is it stored?"

"Good question," Wally replies. "Bulky materials, other than those classified Top Secret are stored in areas that can be secured with special padlocks.

Storage of Secret and Confidential Bulky Material

Bulky materials will be stored in areas that have access opening secured by GSA-approved changeable combination padlocks or key-operated padlocks with high security cylinders.



"The *combination padlocks* must be of the Federal Specification FF-P110 series. The padlock that currently meets the specification is the *Sargent & Greenleaf model 8077AC*. If you use a *key-operated padlock*, it must be a shrouded shackle padlock, which meets Military Specification P-43607. The key-operated padlock that currently meets the specification is the *Sargent & Greenleaf model 833*.

"And if a *key-operated padlock* is used, the keys must be *treated as classified material equal to the classification of the material being protected*. And administrative procedures for the control and accounting of the keys and locks must be established, such as appointing a key control custodian, regular inventorying of keys and locks, regular rotation of locks, and signing for keys. The 5200.1-R does not specify all of the administrative

procedures, but the procedures for any good key control system would be applicable."

Procurement of New Storage Equipment

"Suppose I need a new security container," Mike says. "Where do I look to find out what's available?"

Wally answers, "If you are going to purchase a new security container, you need to use the GSA Federal Supply Schedule.

Procurement of New Storage Equipment

New security storage equipment must be procured from those items listed on the GSA Federal Supply Schedule. Exceptions may be made by heads of DoD Components, with notification to OASD(C31).

"The *Federal Supply Schedule (FSS) for Miscellaneous Furniture* lists the different types of containers and the various configurations (each designed for a different purpose). Read the descriptions carefully. It is easy to make a mistake and order the wrong type of container. The FSS also provides instructions for ordering."

Designations and Combinations

As Mike and Wally continue their rounds they come upon an office with the remnants of a small party that had been held earlier in the day. Wally tells

Mike, "This is a good time to explain about *designations* and *combinations*.

"Make a note about that container in the corner, the one with the red number on the side. One of your first duties after this briefing can be to see that the combination on the lock is changed.

"You're already aware that there can be no external indication of the classification level of materials stored in a container. However, containers can be *identified* to tell them apart. Each container may be labeled on the outside with a *number* or *symbol*. At DIVA we use numbers.



For identification purposes...

Each vault or container may be given an external number or symbol.

"Each container has been assigned a level of classification to be stored in it. Only information of the assigned and lower levels may be stored in it. As you carry out your new duties you will become familiar with the designation of each classified material storage container within DIVA.

"One reason that you need to know about each container is so that you can ensure that the combination is changed at the right times. One of your responsibilities is to help people change combinations of locks when necessary. For example, until noon today, Frank Lewis was authorized access to the classified information in container '4.' However, he was transferred to another job - hence the party - and no longer requires that access.

"An important part of your job will be to maintain the records of the *combination of the lock*, the *location of the container*, and the *names, addresses and telephone numbers of the people who know the combination.*"

Once the combination has been changed and made known to authorized individuals, record the information on a *Standard Form 700, Container Information*. Remember that the combination has the *same security classification* as the information in the container. Thus any *record of the combination* must be stored in a *container approved to store material with that level of classification* or a higher level."

"I can see why combinations should be changed when persons are reassigned and no longer require access to the materials," says Mike. "What other events require combination changes?"

"Several conditions require changing combinations.

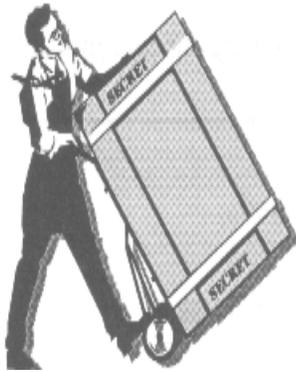
Combinations shall be changed...

- When the container or padlock is first placed *in* use.
- Whenever an individual knowing the combination *no* longer requires access or is no longer authorized access.
- When the combination has been subject to possible compromise.
- When the container or padlock is taken out of service.

"When a container is first brought into an office, the combination on the lock will be 50-25-50. Be sure that you remind people that '50-25-50' is *a standard*

setting and that they have to put on their own unique combination right away. And Mike, remember when we talked about using a combination padlock for the storage of bulky items? All of the procedures I just mentioned concerning changing combinations apply to those padlocks also. (The standard setting for the padlock is '10-20-30.)

Repair of Damaged Security Containers



"Mike, your new responsibility also involves attention to *repair of damaged equipment*. When containers or locks are damaged it can often be more economical to repair the damage or replace damaged parts rather than replace the whole piece of equipment."

"I've never seen any damaged equipment before. What type of damage occurs?" asks Mike.

"Equipment does not fail often," replies Wally. "However, the most usual problem is a *lock failing to open properly*."

"Replacement of damaged or altered parts is fairly cut and dried. For example, a damaged lock can be replaced with a currently authorized lock. The equipment is then considered restored to its original state of security.

... Repairing security containers is not so simple. The repair standards can be found in DoD 5200.1-R. *If you wish to continue to use a damaged container as a GSA-approved one, you must ensure that the container is repaired in the specified manner. In making repairs to security containers, the following general rules apply.*

Repair of Damaged Security Containers

- Only *authorized persons*, cleared or continuously escorted, may make repairs.
- To be considered repaired, strict *standards must* be met.
- If repair standards are not met, the Test Certification *Label and the GSA approval label must be removed.*
- A container not meeting repair standards may be used only for *unclassified* materials and must be so *marked on the front.*

Safeguarding Classified in Foreign Countries

Mike does not have to *safeguard classified information in foreign countries.* However, you may be called upon to do just that. Be aware that U.S. classified materials should be retained in foreign countries only when *absolutely necessary.*

Classified material in a foreign country that is not authorized for release to that country may be stored...

- At a U.S. military installation, embassy, or consulate
- At a building used exclusively by U.S. government tenants if the building is under 24-hour control by U.S. government personnel
- At a building not used exclusively by U.S. Government tenants if the information is stored in GSA-approved containers and
 - a. under 24-hour U.S. control by a U.S. Government activity (when the host government does not control the building)
 - b. in a locked room or area to which only U.S. personnel have access (when the host government controls the building)

Control procedures for information that has been authorized for release will be specified in the appropriate agreement.

Summary



We have discussed safekeeping and storage of classified information. Containers and storage facilities provide protection against inadvertent disclosure and deliberate attempts to gain access. Since there is no entirely secure container and since costs to provide the best security container across the board are too high, we do not seek absolute security. Instead, we rely on deterrence through probable detection, knowing that those who are most likely to try to gain unauthorized access to classified material want to avoid discovery. We seek minimum risk, and set a level of protection appropriate for each level of classification. The specific conditions at an activity also affect the amount of risk taken. The General Services Administration (GSA) sets the security standards for containers, vault doors, modular vaults, alarm systems, and associated security devices. GSA approved containers bear an approval label, test certification label, and identification label. Top Secret information may be stored only in a GSA approved security container with supplemental controls, a vault or secure room that meets DoD standards and has an intrusion detection system (IDS), or a GSA-approved modular vault with IDS. Secret material may be stored in the same manner as Top Secret information, in a GSA-approved container or vault without supplemental controls, in a secure room that meets appropriate standards, and, until 1 Oct 2002, in a steel filing cabinet secured with either an authorized built-in



combination lock or a lock bar with authorized combination lock when supplemental controls are also provided. Confidential information may be stored in the same containers or facilities as Secret information but does not require supplemental controls. Bulky materials are stored in areas secured with either the Sargent & Greenleaf 8077AC combination padlock or the Sargent & Greenleaf 833 key-operated padlock. New security containers are procured using the Federal Supply Schedule for Miscellaneous Furniture. Security containers may not be marked to show the level of classification they contain, but may be identified by a number or symbol. A combination used in securing classified material has the same classification as the most sensitive information it protects, and any record of the combination must be stored according to that classification. Combinations must be changed when the container or padlock is first placed in use, whenever an individual knowing the combination no longer requires access or is no longer authorized access, when the combination has been subject to possible compromise, and when the container or padlock is taken out of service. Only authorized persons may repair damaged containers and if strict standards are not met, the GSA approval and test certification labels must be removed and the container used to store unclassified materials only and so marked. Classified information in a foreign country may be stored at a U.S. military installation, embassy, or consulate; at a building used only by U.S. government tenants if it is constantly controlled by U.S. personnel; or at a building used by non-U.S. tenants if the information is stored in GSA approved containers and either under 24-hour control by a U.S. activity (if the host government does not control the building), or in a locked room or area to which only U.S. personnel have access (if the host government controls the building).

REVIEW EXERCISES

1. The Information Security Program seeks to provide protection against what two threats?
 - a. _____
 - b. _____
2. Minimum risk acknowledges that it is practically impossible to provide security against all attempts to gain illegal access to classified information. Instead, we try to keep the risk of illegal access to a minimum. We base the level of risk that we are willing to take on the _____ of the information we are trying to protect. In addition, _____ can influence how much risk is taken.
3. The storage methods for classified information vary among activities. List three factors that influence the methods of storage.
 - a. _____
 - b. _____
 - c. _____
4. Name the five types of equipment for which the General Services Administration publishes minimum standards.
 - a. _____
 - b. _____
 - c. _____
 - d. _____
 - e. _____

5. The three labels that can be found on a GSA-approved security container are the GSA approval label, the _____ and the _____.
6. The four types of containers or areas that are acceptable for storage of Top Secret information are:
- a. _____
 - b. _____
 - c. _____
 - d. _____
7. The five types of containers or areas acceptable for storage of Secret information are:
- a. _____
 - b. _____
 - c. _____
 - d. _____
 - e. _____
8. A key-operated lock is used in the storage of Secret bulky material. The lock's key must also be treated as if it were classified Secret.
- True False
9. You are going to procure new storage equipment. The _____ lists those items that you can procure.
10. Storage containers will display a label indicating the level of classified information stored in the container.
- True False

11. The four occasions when lock combinations should be changed are:
- a. _____
 - b. _____
 - c. _____
 - d. _____
12. A GSA-approved security container has been damaged. To be considered repaired, strict standards must be met. If repair standards are not met, the _____
_____ and the _____ must be removed. A container not meeting repair standards may be used only for storage of _____ .
13. U.S. Government classified information in a foreign country may be stored in any structure as long as that structure has a GSA-approved security container.

True False

SOLUTIONS AND REFERENCES

1. a. Inadvertent disclosure
b. Deliberate attempts to gain access (p. 7-3)
2. level of classification
local situations (p. 7-5)
3. a. Nature and size of the activity
b. Mission of the activity
c. Level and type of classified information (p. 7-6)
4. a. Containers
b. Vault doors
c. Modular vaults
d. Alarm systems
e. Associated security devices (p. 7-7)
5. test certification label
identification label (p. 7-9)
6. a. A GSA-approved security container with supplemental controls
b. A vault with IDS
c. A GSA-approved modular vault with IDS
d. A secure room with IDS (p. 7-11)

7.
 - a. Those that meet Top Secret storage standards
 - b. GSA approved security container or vault w/o supplemental controls
 - c. Secure rooms(meeting Component standards established prior to 1 Oct 95)
 - d. Steel filing cabinet with a built-in three-position changeable combination lock, with supplemental controls
 - e. Lock bar filing cabinet secured by a GSA approved changeable combination lock, with supplemental controls (p. 7-13)
8. True. (p. 7-14)
9. Federal Supply Schedule (p. 7-15)
10. False. (p. 7-16)
11.
 - a. When the container or padlock is placed in use
 - b. When a person who knows the combination no longer needs access.
 - c. When the combination has been subject to possible compromise
 - d. When the container or padlock is taken out of service. (p. 7-17)
12. test certification label
 GSA approval label
 unclassified materials (p. 7-19)
13. False. U.S. classified in a foreign country may be stored only at:
 - a. A U.S. military installation, US embassy or consulate
 - b. At a building used exclusively by U.S. government tenants if the building is under 24-hour control by U.S. government personnel.
 - c. At a building not used exclusively by U.S. Government tenants with other restrictions dependent upon whether or not the host government controls the building. (p.7-19)

LESSON 8

TRANSMISSION AND TRANSPORTATION

Classified materials usually don't stay put. Sooner or later, something comes up that calls for them to be sent somewhere else. And whenever classified information is removed from a work area, the risk of loss or compromise increases. To minimize this risk, we need to follow the special rules for the *Transmission and Transportation* of classified information. In this lesson, we'll go over the authorized methods for sending classified information, how to prepare it for transmission, and the special requirements for hand carrying it.



At the end of this lesson, you will be able to do the following:

Identify the authorized methods for the *Transmission and Transportation* of classified information.

Determine if classified information has been properly prepared for sending.

Identify the procedures for hand carrying classified information.

Identify the additional procedures for hand carrying classified information aboard a commercial airline.

Methods of Transmitting Classified Information		
Top Secret	Secret	Confidential
<p><u>Defense Courier Service (DCS)¹</u> Authorized Component courier service</p> <p><u>Department of State courier system²</u> US military and US civilian employees. All hand carriers must be appropriately cleared with a need-to-know.</p> <p><u>DoD contractor employees within the US & Territories only and, for TS, with authorization from the appropriate Cognizant Security Agency (CSA). All hand carriers must be appropriately cleared with a need-to-know. CSA authorization not required to hand carry S material.</u></p> <p><u>Cryptographic system authorized by NSA (e.g. STU-III)</u></p> <p><u>Protected Distribution System meeting NACSI 4009 standards</u></p>	<p>Same methods as Top Secret except no DCS³</p> <p>-Unless COMSEC or SCI, or -DCS has given prior approval, or -US control cannot be ensured</p> <p><u>Registered mail⁴</u> -within and between US and Puerto Rico -to APO or FPO address if mail always under US control</p> <p><u>US and Canadian Registered Mail⁴ with registered mail receipt between US and Canadian installations in US and Canada</u></p> <p><u>USPS Express Mail⁵ within and between US and Puerto Rico</u></p> <p><u>GSA contractor for overnight delivery (currently FEDEX⁶) within and between US and Territories</u></p> <p><u>Protective Security Service (PSS)⁷ within US, when size, bulk, weight, or escort considerations dictate</u></p> <p><u>Appropriately cleared vehicle operator, officer of a ship, pilot of an aircraft or a US or US-contract vehicle, USN ship, civil-service operated USN ship or US registry ship (must be kept under observation or authorized storage)</u></p>	<p>Same methods as Secret</p> <p><u>Registered mail⁴</u> -to APO/FPO outside US and Territories -when uncertain if location within US -to contractor or other Executive Branch agency, as appropriate</p> <p><u>First Class Mail⁸ between DoD activities within US and Territories only. Put "Do Not Forward" on outer wrapper.</u></p> <p><u>Certified Mail⁴ to contractor or other Executive Branch agency, as appropriate</u></p> <p><u>Constant Surveillance Service (CSS) within US, when size, bulk, weight, nature, or escort considerations dictate</u></p> <p><u>Commander/master of US registry ship (must be US citizen)</u></p>

¹DCS will not transport chemicals, explosives, or contraband.

²The Department of State courier system uses diplomatic pouches. DoD and State have an agreement by which DoD will transport State materials into places that DoD has a system but State does not, and vice versa.

³Due to volume and costs DCS does not routinely transport Secret or Confidential materials. They will, however, transport all COMSEC and SCI materials and any other classified materials for which an agreement has been made, for example, special access program (SAP) information. And they will transport Secret or Confidential materials if US custody of the materials will not be maintained throughout the entire transportation process using another means. It is the sender's responsibility to research how materials are handled using other means.

⁴Registered or certified mail should be used only when less expensive authorized methods are unavailable.

⁵Use USPS Express Mail only when it is the most effective means considering security, time, cost and accountability. Don't execute the "Waiver of Signature and Indemnity," nor use street-side collection boxes, nor use it for APO/FPO addresses.

⁶When using FEDEX, be sure an authorized person is available to receive delivery. Do not execute the "Release Signature upon receipt" block and do not use street-side collection boxes. FEDEX is not authorized for COMSEC, NATO, and foreign government information. Applicable postal regulations must be met.

⁷PSS is a contracted service that requires the carrier to provide dual drivers, continuous escorting of the materials, and other security measures. The company must have a Secret facility clearance issued under the National Industrial Security Program (NISP). Military Traffic Management Command (MTMC) can tell you which companies in your area provide PSS.

⁸Don't use First Class Mail to send any classified materials to contractors or other Executive Branch agencies.

Authorized Methods

Tim Evans of DIVA's Intelligence Systems Division needs to send a three-page Secret document to DIVA's field office at Edwards Air Force Base. Tim usually hands off tasks like this to Pam Leyland, a member of the support staff. But Pam's out with the flu, so it's up to him to send the document to Edwards.



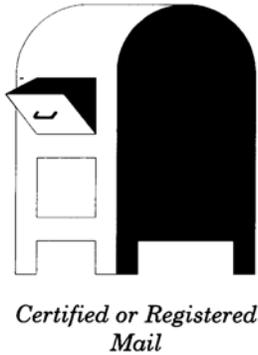
Tim remembers that Pam once gave him a handout listing the *authorized methods of transmitting classified information*. He finds it in his desk and reads it, but he is uncertain about some of the requirements. He asks around and gets advice on the methods, but he's not sure that the advice is accurate. So he decides to call DIVA's Security Office. His call is put through to Mike Carson. Mike says he will be right over.

"Now," says Mike, seated in Tim's office. "What can I clear up about the chart?"

"Well, the chart says that I can send Secret materials to an APO or FPO address as long as the mail does not pass out of US control. Whose responsibility is it to find out how the mail is handled?"

"It's the *sender's responsibility*, and it's not an easy task," Mike says. "You can try to contact the security folks stationed in the country that you're sending the materials to, or you can try the post office. They may be able to help you."

"O.K. Next question. The chart indicates that I can use Constant Surveillance Service to send



Confidential materials. Will the company that provides CSS have a *facility clearance*?"

"Not necessarily. They may have one because of some other contract. But they are *not required to have a facility clearance simply to provide CSS.*"

"And the last question. I notice that the chart says that when I send Confidential materials to my contractor or to another Executive Branch agency I must use registered mail, as appropriate, or certified mail, as appropriate. How do I know when it's appropriate?"

"They will tell you," Mike answers. "What's important to remember is that you must use, *at a minimum, certified mail* to send the materials to your contractor or another Executive Branch agency. You find out *from your contractor or the agency* if it must be sent through *registered mail.*"

Preparing Classified Information for Transport

"Thanks, Mike. I appreciate the information. I've decided that U.S. *Registered Mail* is the best way to get this Secret document to Edwards Air Force Base. Can you help me prepare it for mailing?"

Before Packaging

"Before we get into packaging, Tim, let's make sure a few other things have been dealt with. Are you sending a *transmittal letter* with the document?"

"Yes," Tim replies. "And I've checked to see that the *transmittal letter* is properly *marked*. The *Secret document* has the necessary *markings* on it too."

Double Wrapping-----

"Great! Now let's talk about packaging. The requirement is...

When size permits classified items should be transmitted in two non-transparent sealed envelopes or similar wrappings.



Tim takes two envelopes out of his desk drawer.

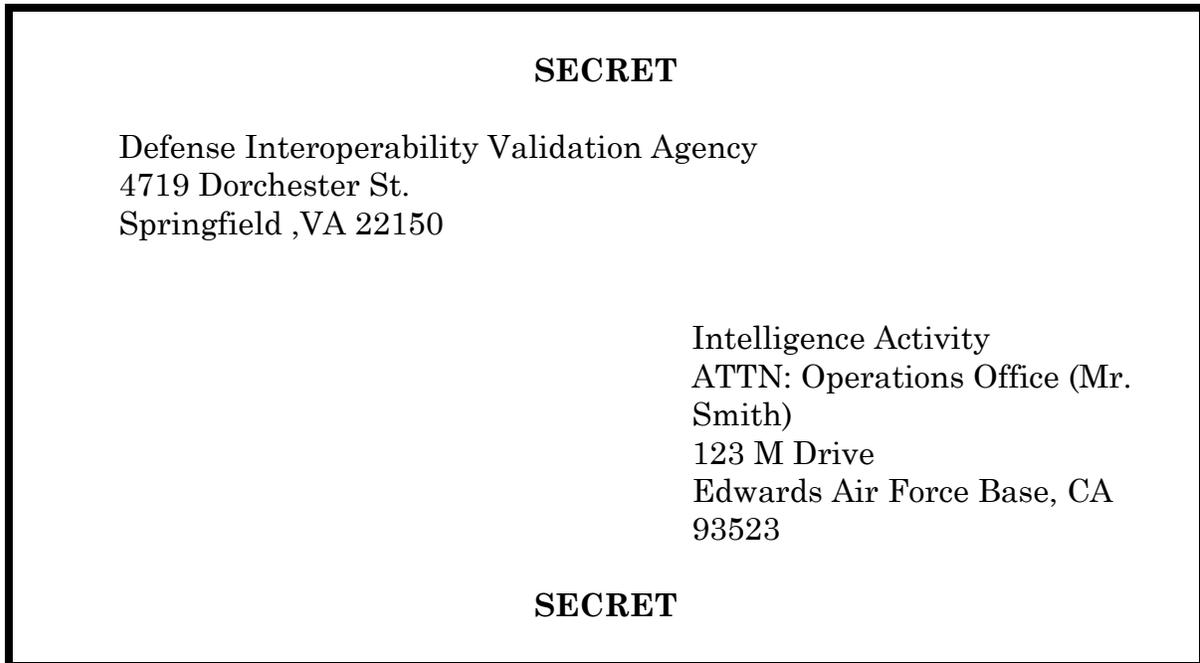
"Let's check out these envelopes," Mike says. "They must be *strong enough* to withstand normal mail handling and *opaque* so no one can read what's inside. These look O.K., but there might be a problem. I'll show you later what I mean.

The Inner Envelope-----

"Do the inner envelope first. You need to...

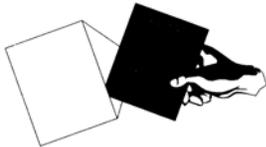
- Address the envelope to an official government activity or *DoD* contractor.
- Put your office's return address on the envelope.
- Conspicuously mark the envelope with the highest level of classified information it contains.
- Place any applicable special markings such as "Restricted Data" on the envelope.
- Carefully seal the envelope to minimize the possibility of access without leaving evidence of tampering.

Tim's *inner envelope* looks like this:



"Was it O.K. to put Mr. Smith's name on the envelope?" Tim asks.

"Yes," Mike replies, "you can put a *person's name on the inner envelope*, but *not* on the outer envelope."



"Now put your document and transmittal letter in the envelope. You may want to fold the document inward so the text can't be read through the envelope. If you have to, wrap your document in a blank sheet of paper." Tim puts the materials in the inner envelope.

"Suppose your document was classified Confidential instead of Secret. But your transmittal letter contained Secret information. How would you mark the inner envelope?"

"I'd mark it SECRET since the *highest level of classified information in the envelope is Secret.*"

"Right. *Always* mark the *inner envelope* with the *highest level of classified information it contains*. And try to avoid mailing documents of different classification levels in one package. If you must,

though, mark the inner envelope with the highest classification of the contents. What would you do if the document contained Restricted Data?"

"I'd put 'Restricted Data' on the inner envelope," Tim says.

The Outer Envelope

"Let's move on to the outer envelope," Mike says. "Here's what you need to do..."

*Address the envelope to an official government activity or DoD contractor not to an individual. However, you can use office code numbers or phrases, such as **"Attention: Research Department."***

Put your office's return address on the envelope.

Don't put any markings or notations on the outer envelope that indicate that its contents are classified.

Carefully seal the envelope to minimize the possibility of access without leaving evidence of tampering.

Tim's outer envelope looks like this:

Defense Interoperability Validation Agency
4719 Dorchester St.
Springfield, VA 22150

Intelligence Activity
ATTN: Operations Office
123 M Drive
Edwards Air Force Base, CA 93523

"Why the prohibition on putting a person's name on the outer envelope?" Tim asks.



"People tend to treat mail with a person's name on it as personal mail," Mike answers. "If the addressee is not there at the time of delivery, they may place the package on that person's desk - or worse, they might forward the mail to the addressee at another organization! We want the *receiving organization to open the outer envelope upon receipt*. When they get to the second envelope and see the classification markings, they will know how to treat the package."

Tim puts the inner envelope in the outer envelope.

"O.K., Tim. Before you seal the outer envelope, take a close look. Can you see the classification markings on the inner envelope as you look at the outer envelope?"

"If I look real hard I can see the word 'Secret'."

"This is that potential problem that I mentioned earlier," Mike says.

If the inner envelope's classification markings show through the outer envelope wrap *the inner envelope with enough paper to prevent the markings from showing through*.

Tim wrapped the inner envelope in two sheets of paper, placed it all in the outer envelope, and carefully sealed the outer envelope.

Mike says, "Your document is properly packaged -good to go via U.S. Registered Mail!"

Other Packaging Requirements-----

"Thanks, Mike. Now that I've done it, it seems pretty easy. But what if something like that," Tim says as he points to his radio, "was classified and I had to it to send it to Edwards instead of this 3-page document?"

"Good question, Tim. Here's a chart that covers packaging classified items.

Packaging Classified Items

- **If a classified item is too large to be transmitted in envelopes or similar wrappings *enclose it* in two nontransparent sealed containers such as boxes or heavy wrappings.**
- **If a classified item is an internal component of a packageable item of equipment the outside shell or body may be considered as the inner *enclosure provided* it does not reveal classified information.**
- **If the classified item is an inaccessible internal component of a bulky item of equipment that is not reasonably packageable**
- **the outside or body of the item may be considered to be a sufficient enclosure provided the shell or body does not reveal classified information.**
- **If the classified item is not reasonably packageable and the shell or body is classified it shall be concealed with a nontransparent covering that will hide all classified features.**
- **Specialized shipping containers including closed cargo transporters may be used instead of the packaging cited above. In such cases the container will be considered the outer wrapping or cover.**

"I think I need some help here," says Tim. "I'm not sure what you mean by the third item on the list, 'If a classified item is an inaccessible internal component of a bulky item that is not reasonably packageable,' and so forth."

"Well, for example, let's say you have a classified hard drive that is not removable. If the outside of the computer doesn't reveal any classified information, then the computer itself can be considered a sufficient enclosure. So you wouldn't have to wrap the computer.

"And as for the next item on the list, if you have a piece of equipment that is configured in such a way that the outside reveals classified information - for example the shape might be classified - and the item is not easily packageable, cover it in such a way that the classified information would not be discernible."

When packaging a classified item, ensure that...

- The package is wrapped so that no classified information is revealed.
- The packaging is strong enough to provide protection in transit.
- The classified item can't break out of its package.
- The package is wrapped so that you can tell if it's been tampered with.

"Thanks for all the help with getting classified information prepared for shipment," Tim says.

"No problem, Tim. But you'd better get your package down to the mailroom if you want them to send it today! I'll walk to the elevator with you."

Hand Carrying Classified Information

When we use the term "hand carry" we are not referring to a designated courier whose job is to routinely hand carry classified materials. Instead, we use "hand carry" to refer to an *appropriately cleared U.S. government or U.S. contractor employee personally transporting classified information for which he or she has a need-to-know.*

To learn more about hand carrying, let's look in on Mike Carson as he arrives at the Security Office.

Determine Need

"Hi, Jackie. Any messages?" Mike asks Jackie Hernandez, the Security Office's secretary.



"No. But don't forget the staff meeting this afternoon. Did you get everything taken care of up in Intelligence?" Jackie asks.

"Piece of cake. Tim Evans just needed some advice for how to send a Secret document by registered mail. I'm just glad he didn't ask about hand carrying the thing. I'm so tired today, I'm not sure I could have told him how to do it"

"Well, if Tim had needed advice on hand carrying information, you could have stayed here and answered the phones and I would have gone up to Intelligence to advise him," Jackie teases. "After all, I have picked up a few things in my two years here!"

"O.K., wise one, what would you have told Tim about hand carrying classified information?"

"Well, first I'd have said that hand carrying classified information should be done only as a last resort.

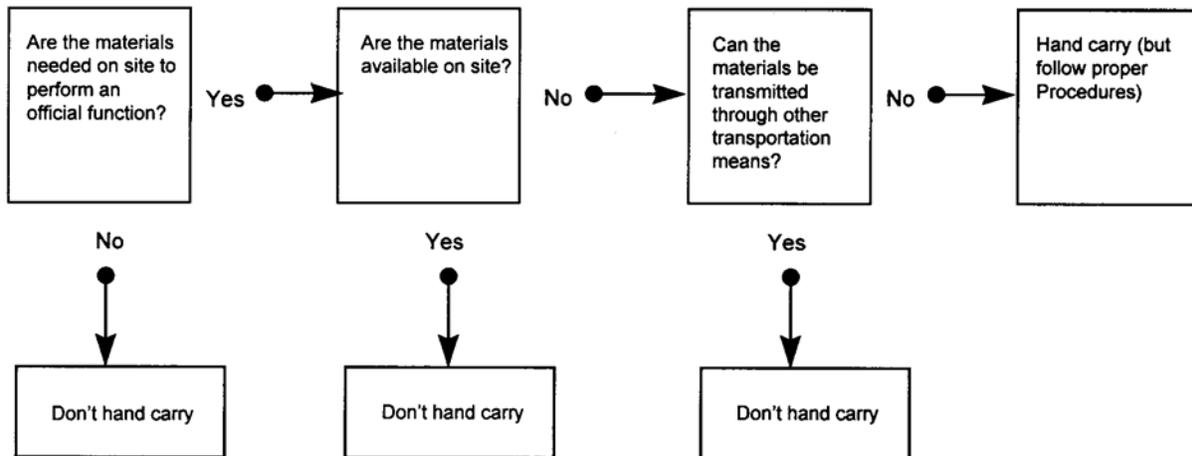
Before hand carrying or escorting classified information is authorized the following questions must be answered...

Are the materials *needed at the destination to perform an official function?*

Are the materials *already* available at the destination?

Can the materials be transmitted to the destination *in time* by *another authorized method?*

Determining Need to Hand Carry



"So before authorizing the hand carrying of classified information, the responsible official has to determine that in this particular instance the traveler requires the classified information at the destination to perform official duties, that it is unavailable there, and that it can't be transmitted by another authorized method in time for the traveler's use there."

Traveler's Responsibilities

"Very good, Jackie. Now, suppose the chief of the Security Branch has told Tim it's O.K. to hand carry the Secret document to the Pentagon. What's next?"

"I'd say that he must have *written authorization*. It varies according to the type of transportation used.

Written authorization for hand carrying classified materials can be:

- **Travel orders** (*not* for travel on commercial airlines)
- **DD Form 2501** (*not* for travel on commercial airlines)
- **Letter of authorization** (*required* for commercial airlines)

"What we in this office issue - his *travel orders* or a *DD Form 2501*, 'Courier Authorization Card' - would be enough unless he's flying. Then he'd need a *letter of authorization*.

COURIER AUTHORIZATION		SERIAL NUMBER AD 00000	
1. ISSUE DATE		2. EXPIRATION DATE	
3. NAME (Last, first, middle initial)			
4. RANK OR GRADE			
5. AUTHORITY			
6. CERTIFICATION			
7. ORGANIZATION			
8. SECURITY INCIDENTS			
9. DUTY PHONE NUMBER			
10. APPROVAL			
a. NAME		c. SIGNATURE	
b. TITLE		SAMPLE	

DD Form 2501, MAR 88

THIS CARD IS THE PROPERTY OF THE U. S. GOVERNMENT. ANY COUNTERFEITING, ALTERATION, OR ABUSE OF IT IS A VIOLATION OF SECTION 494, TITLE 18, U. S. CODE.

If found, drop in any mailbox.

Postmaster - Return to:

TAKE THE FOLLOWING PRECAUTIONS WHILE IN TRANSIT

- Keep material in your personal custody at all times.
- Store material overnight in U.S. Government or cleared contractor facility.
- Allow only cleared individuals, with a need to know, access to the material.
- Use the most direct route.
- Do not discuss or view classified material in public.
- Immediately report security incidents to the numbers listed in item 10 of this form.

DD Form 2501 Reverse, MAR 88

front **back**

Sample DD Form 2501

"Then Tim would have to be *briefed on his responsibilities as a hand carrier.*"



"What would you include in the briefing if Tim had to make an overnight stop on the way to the Pentagon?"

"I'd point out that he'll need to *make arrangements to store the package overnight* with either a *government facility* or a *cleared contractor with storage capability*. He would *not* be authorized to give it to the motel clerk to put in the motel safe for the night!"

"Does the document need to be prepared any special way for hand carrying?"

"No. It has to be double wrapped - placed in two envelopes and addressed just as though he was going to mail it."

"Suppose he wants to carry the classified materials in his *briefcase*, what would you tell him?" Mike asks.

"If it has a *lock*, he can. He would just have to prepare an *inner envelope* like we do for all classified materials being mailed, put it in his briefcase, and lock it. The *briefcase* would be considered the *outer wrapper.*"



"You're doing great so far, Jackie! Anything else?"

"Sure," she says. "The package must *remain in his personal possession or be under his constant surveillance*. So if he stops for a bite to eat along the way, he *can't leave the package unattended* in his car and go into the restaurant. He has to take it with him. And the classified information mustn't be

read, studied, displayed or used in public, so he can't go over the document at the restaurant table either!

"That about covers his responsibilities. And if you're tired again, Mike Carson, and need to remember the rules for hand carrying, just refer to my chart!" Jackie laughs. "Here's a copy for your personal use with my compliments."

Hand Carrying Classified Information

- Individuals hand carrying classified materials will be briefed on their responsibilities.
- *Written authorization is required.*
- Overnight storage is authorized only at a US government facility or cleared contractor *with storage capability.*
- Materials must be double wrapped. (Locked briefcase can serve as the outer wrapper.)
- The classified information must remain in their personal possession or under their *constant surveillance.*
- The classified information must not be read studied displayed or used in public.
- The information must never be left unattended.

Hand Carrying Aboard Commercial Passenger Aircraft

"Thanks. Still, that was pretty easy. Suppose Tim had to get on a TWA flight and go out to California with his Secret document. What would you say?"

"Still not convinced that I know this stuff, are you? I'd start by reminding him that, as for any hand carrying, an appropriate official must determine the

need for the hand carrying. Tim must need the document for official use when he gets to California, it must not already be available there, and there must be insufficient time to get it there by another authorized method.

"I'd go on to say that there are some additional restrictions and procedures when classified information is to be hand carried aboard a commercial aircraft."

"Why?" Mike asks.

"Because of the threat of hijacking and the danger of weapons and explosives being taken or placed aboard aircraft."

"Can you think of any specific restrictions?"

"Sure. Just give me a minute."

"Hey, maybe I've stumped you!" Mike says.

"No way! Here goes.

When classified information is hand carried aboard commercial passenger aircraft all airlines involved shall be U.S. carriers.

Foreign carriers may be used only *when no U.S. carrier is available*. The information must remain in the custody and physical control of the U.S. escort at all times.

"O.K.," Mike says, "let's say we have Tim from Intelligence to the point where the situation is urgent and the chief of the Security Branch has

given verbal approval for Tim to take his Secret document to California and back on TWA, which is a U.S. carrier. Now what?"

"Tim needs to make sure he carries two other items on the plane in addition to his classified package.

When hand carrying classified information on a commercial flight the traveler must possess...

- **A suitable ID card**
- **A letter authorizing that person to hand carry classified information**

"The ID card must contain his *photograph*, descriptive data (*date of birth, height, weight*), and *his signature*.

Military personnel can use their DD Form 2, Armed (or Uniformed) Services Identification Card. *Government employees*, such as Tim, can present the official identification issued to them by their agency. *Contractor personnel* ID cards must contain the name of the employing contractor or be marked 'Contractor'."

"Tell me more about the *letter of authorization*," Mike says.

"The person traveling carries the *original* authorization letter. And the traveler should *carry sufficient copies to provide one to each airline involved*; the traveler retains the original. In addition

The **letter of authorization** will...

- Be prepared on letterhead stationery of the agency or contractor authorizing the carrying of classified material.
- Give the full name of the individual and his or her employing agency or company.
- Describe the type of identification the individual will present.
- Describe the material being carried (for example three sealed packages 9" x 8" x 24" addressee and addresser).
- Identify the point of departure destination and known transfer points.
- Carry a date *of* issue and an expiration date.
- Carry the name, title, and signature of the official issuing the letter.
- Carry the name *of* the government agency designated to confirm the letter *of authorization and* its telephone number. The telephone number shall be an official U.S. Government *number*.

**Defense Interoperability Validation Agency
4719 Dorchester Street
Springfield
Virginia 12345-6789**

Security Office
[Name and address of airline]

23 March 1997

SUBJECT: Letter of Authorization

To Whom It May Concern:

1. Mr. Timothy R. Evans from the Intelligence Systems Division of the Defense Interoperability Validation Agency is authorized to carry classified materials as described in this correspondence.

2. Mr. Evans will have the following in his possession:

a. Identification card (OF 55
US Government Identification)

b. One sealed envelope:

(1) 9 inches X 12 inches X 2 inches

(2) Addressee is Satellite Intelligence Agency, 12345 Arterial Way, San Bemadino
California 98765-4321

(3) Addresser is Defense Interoperability Validation Agency, Intelligence Systems, Division, 4719
Dorchester Street, Springfield, Virginia 12345-6789

3. Mr. Evans will be departing Dulles International Airport on 24 March 1997 and is scheduled to transfer at O'Hare International Airport with a final destination of Los Angeles International Airport.

4. Point of Contact for this matter is Mrs. Sheila Harrington
Defense Interoperability Validation Agency Security Office
COMM (703) 555-1234.

5. This authorization to transport the above-described classified materials will expire on 27 March 1997.

Lt Col William Timmons
Chief, Security Branch
Defense Interoperability Validation Agency

Sample Letter of Authorization

Transmission and Transportation

8-19

"Should Tim make any special arrangements with the airline?"
Mike prompts.



"Yes," Jackie says. "He should coordinate with airline officials to ensure that arrangements for transporting the classified information are *in line with DoD and FAA guidance*. And he needs to find out what *documentation* they require him to carry."

"Right on the button, Jackie! Now let's change the situation a little. What if, instead of a 3-page document, Tim's package contains a *300-page document*?"

"There are guidelines for that situation too.

Classified documents concealed in envelopes and transported via commercial aircraft should not be held together by metal *bindings* or anything that may arouse suspicion or be mistaken as *contraband*. Avoid giving airline officials a reason to visually inspect the package.

"Tim would carry the envelope in his locked briefcase and proceed as he normally would through ticketing and boarding. At the security check he can open his briefcase and allow it to be inspected. He needs to stay on his toes in case the screening officials decide to inspect the envelope itself.



The screening officials may check the envelope by X-ray machine flexing feel and weight but they *cannot open* the envelope.

"Right," Mike says. "They can't have access to the information, so they *must not be allowed to open the envelope*. Well, I've learned a lot today."

"That my hanging around this office for over two years has allowed me to pick up on security issues and procedures?" Jackie asks.

"I learned that if I'm too tired to do my job, I'll just refer people to you!"

"You're impossible! Now why don't we go to lunch and talk about that staff meeting this afternoon?"

"Good idea. I could eat a 300-page document!"

Summary

In this lesson, you learned what needs to be done to transmit and transport classified information.

You learned that Top Secret information may be sent by the Defense Courier Service (DCS); by a component courier system; by U.S. military and U.S. civilian hand carriers (appropriately cleared and with a need-to-know); by DoD contractor employees (appropriately cleared and with a need-to-know) hand carrying the material within the U.S. and its territories with authorization from the appropriate cognizant security office (CSA); by an NSA-authorized cryptographic system, such as the STU-III; and by a Protected Distribution System.



Secret information may be sent by the same methods as Top Secret (but by DCS only in certain cases); by U.S. Registered Mail within and between

the U.S. and Puerto Rico and, if under U.S. control, to an APO/FPO address; by U.S. and Canadian Registered Mail with receipt between their installations in the two countries; by USPS Express Mail within and between the U.S. and Puerto Rico; by FEDEX within and between the U.S. and its territories; by Protective Security Service (PSS) for special shipments within the U.S.; and by certain cleared officers of U.S.-related vehicles, vessels and aircraft.

Confidential information may be sent by the same methods as Secret and by U.S. Registered Mail to an APOTPO address outside the U.S. and its territories, when the destination may lie outside the U.S., and to a contractor or another Executive Branch agency, as appropriate; by U.S. First Class Mail between DoD activities within the U.S. and its territories only; by U.S. Certified Mail to a contractor or another Executive Branch agency, as appropriate; by Constant Surveillance Service (CSS) for special shipments within the U.S., and by a U.S. citizen who commands a U.S. registry ship.

You also learned that a transmittal letter, if used, must be properly marked, as must the classified material. In almost every case you must double wrap the materials for transport, usually in two substantial, opaque envelopes, as follows:

Inner envelope
<ul style="list-style-type: none">• Return address• Recipient's address (a person's name may be included)• Classification markings• Caveats (as appropriate)• Seal envelope in such a way that tampering can be detected

Outer envelope
<ul style="list-style-type: none">• Return address• Recipient's address (do <i>not</i> include a person's name)• Seal envelope in such a way that tampering can be detected



Classified items too large for envelopes are double packaged so as to prevent revealing the classified information, protect the items in transit, keep them contained, and enable discovery of tampering.

We concluded with hand carrying classified information. The traveler should not hand carry the materials unless they are needed at the destination to perform an official function, are unavailable at the destination, and can't be transmitted there by another authorized method in time for the traveler's use. If the determination is made to hand carry the classified materials, the following procedures apply.

Prior to leaving:	While traveling:	Also, if traveling by a commercial aircraft:
<ul style="list-style-type: none"> ● Obtain written authorization <ul style="list-style-type: none"> (1) Travel orders, (2) DD Form 2501, or (3) Letter of authorization. ● Get briefing. ● Make arrangements for overnight storage (if applicable). ● Double wrap materials. 	<ul style="list-style-type: none"> ● Keep materials in your personal possession or under your constant surveillance. ● Do not read, study, display, or use the materials in public. ● Never leave materials unattended. 	<ul style="list-style-type: none"> ● Ensure that all airlines involved are U.S. carriers, or that no U.S. carrier is available before using a foreign carrier. ● Coordinate with the airlines. ● Have in your possession: <ul style="list-style-type: none"> (1) Military/government ID (2) Letter of authorization. ● Allow airline/airport officials to inspect outside of package. ● Don't bind material with metal straps or otherwise cause airline/airport officials to be suspicious or want to inspect inside the package. ● Allow airline/airport officials to X-ray, flex, feel, and weigh the package but don't allow them access to the information.

REVIEW EXERCISES

1. Write in the highest level of classification of information that that can be transported by each method ("TS," "S" or "C").
 - ___ a. U.S. Registered Mail
 - ___ b. U.S. First Class Mail
 - ___ c. U.S. Express Mail
 - ___ d. U.S. Certified Mail
 - ___ e. U.S. Military employees traveling on a commercial aircraft
 - ___ f. Commercial carriers that provide a Constant Surveillance Service
 - ___ g. Defense Courier Service
 - ___ h. U.S. Government employee traveling by surface transportation
 - ___ i. NSA cryptographic system
2. What industrial security agency's authorization is required before a DoD contractor employee may transport Top Secret information?
3. When may you transmit Top Secret information by the U.S. postal system?
 - a. When DCS is not available.
 - b. At any time it is deemed necessary by the commanding officer.
 - c. Under all circumstances.
 - d. Under no circumstances.
4. You are sending Confidential information via U.S. First Class Mail. What special endorsement (or phrase) must appear on the outer envelope?

SOLUTIONS AND REFERENCES

1. S a. U.S. Registered Mail
C b. U.S. First Class Mail
S c. U.S. Express Mail
C d. U.S. Certified Mail
TS e. U.S. Military employees traveling on a commercial aircraft
C f. Commercial carriers that provide Constant Surveillance Service
TS g. Defense Courier Service
TS h. U.S. Government employee traveling by surface transportation
TS i. NSA cryptographic system (p. 8-2)
2. The appropriate cognizant security agency. (p. 8-2)
3. d. (p. 8-2)
4. Do Not Forward. (p. 8-2)
5. False. (p. 8-2)
6. DCS will transport all COMSEC and SCI materials as well as all SAP materials if the program has an agreement with them and if it cannot be ensured that with other authorized methods the materials will stay within U.S. control throughout the entire transport. (p. 8-2)
7. (pp. 8-5 and 7)

SECRET

Defense Interoperability Validation Agency
4719 Dorchester St.
Springfield, VA 12345

Defense Engineering Activity
ATTN: Testing Laboratory (Sam Jones)
Hamilton Building, Bay N
Richmond, VA 23297

Formerly Restricted Data

SECRET

Defense Interoperability Validation Agency
4719 Dorchester St.
Springfield, VA 12345

Defense Engineering Activity
ATTN: Testing Laboratory
Hamilton Building, Bay N
Richmond, VA 23297

8. Although the outer shell is a sufficient enclosure to shield the classified information, the computer should be packaged to protect it from damage during transport. (p. 8-10)
9. True. (p. 8-14)
10.
 - a. Letter of authorization
 - b. Travel orders
 - c. DD Form 2501 (p. 8-13)
11. You must have a letter of authorization when you are hand carrying classified materials on a commercial airline. (p. 8-13)
12. No. (p. 8-14)
13.
 - a. False.
 - b. True.
 - c. True.
 - d. True. (pp. 8-16-20)

LESSON 9

DISPOSAL AND DESTRUCTION



Sooner or later all classified materials that an organization holds are either transferred or destroyed. Unfortunately destroying often happens later not sooner. People often hold on to classified materials for no good reason - and for many bad ones. Part of your job is to make destruction an integral part of security. And timely destruction should not be a hard sell. In fact, destroying classified information should be everyone's most pleasant security task - after all, each item destroyed is one less item to worry about. No one will have to store it, re-mark it, inventory it, check it out, check it in, or transmit it ever again!

At the end of this lesson, you will be able to do the following:

- List reasons why people don't destroy the materials that should be destroyed.
- Identify why it's important to destroy classified materials when necessary.
- Assist others in developing techniques to help identify what should be destroyed.
- Identify what should be destroyed.

- Identify who should conduct the destruction of classified materials.
- List appropriate methods for the destruction of classified materials.
- State the problems associated with destroying particular materials.
- Promote the effective disposition of classified materials through the identification of the procedures for conducting destruction.



Disposal vs. Retention



Admit it! You still have report cards from elementary school stuffed in an old shoe box somewhere in your house. You've probably got a deflated basketball tucked away in your basement and an unopened wedding gift from Aunt Sarah and Uncle Bob under the pile of clothes you've been meaning to give to Goodwill.

Why do we continue to hold on to things that no longer serve a purpose in our lives? Well, for one thing, we keep personal items for sentimental reasons. We also tend to hold on to things in the workplace - and not for sentimental reasons. That's what we're here to explore - why we don't dispose of classified items that are no longer essential to the operation of our workplace.

Let's begin our discussion of disposal vs. retention by identifying reasons why we might hold on to classified items. We'll look in on Anne Perkins of DIVA's Security Office as she drops by Margaret Collier's office. Margaret works in DIVA's Weapons Systems Division. She also happens to be Anne's sister-in-law.

Why We Hold On To Unneeded Classified Items-----

"Hi, Margaret," Anne says. "I just wanted to drop these clothes off for the kids."

"Thanks, Anne. Kids grow so fast. I wonder if anyone actually buys children's clothes. Seems like the kids get hand-me-downs, fill them out, hand them off, and get handed down to again!"

"I know the feeling. So how are you?" Anne asks.

"Very busy. Look at this office. It's a mess. If I ever get a spare moment, I'll do some spring cleaning."

"I hate to tell you this," Anne says, "but it's now September!"

"So I'll be a few months early," Margaret laughs.

"Well, when you start cleaning house, be sure to think about the classified materials you use in your work. You should get rid of what you don't need."

"From sister-in-law bearing gifts to Deputy Chief of the Security Branch in record time," Margaret says.



Anne Perkins Margaret Collier

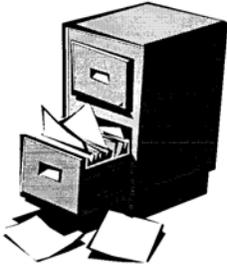
"I guess I did bring my security soapbox. But you wouldn't believe what a hassle it is getting people to dispose of classified information they don't need. If only they'd realize the drawbacks - even dangers - of not getting rid of it when they should!"

"Anne, maybe people just don't know when they *can* dispose of their classified information."

"Too true. Many people look at a classified document and read, 'Declassify on: OADR.' They know that OADR means 'Originating Agency's Determination Required.' They know they have to check with the originating agency before *declassifying* it, so they jump to the conclusion that they have to contact the originating agency and get its approval before they can *destroy* it. Which of course is wrong! But maybe no one has ever told them that *if records management rules don't require you to retain a document - and if it no longer serves an operational purpose - it can be and should be disposed of!*

"Or maybe you look at a document and say to yourself, 'I haven't opened it in two years but I'd better hold on to it, just in case.' Sound familiar?"

"I refuse to answer on the grounds that I may have several long-unopened classified documents," Margaret replies.



"So that's another reason people hold on to classified materials. *They think they'll need it in the future.* It's a valid reason. But what people don't understand is that if everyone followed the proper records management procedures, they could obtain another copy in the future because the file copy would be retained in the originator's system.

"What really gets to me though is that some people hold on to classified materials because they think the more they have, the more important they are. *ney let their egos get in the way.* And others think they can *justify manning requirements* by having a lot of classified information in their workplace."

"You won't get an argument from me on either of those," Margaret says. "I work with a few people like that. But in my case, I have to admit that I *don't know how to go about destroying classified materials* and I *don't even know what I should destroy and what I shouldn't!*"

"That's the big one, all right. The main reason people don't dispose of their classified materials is *their workplace has not established a program to help them identify what should be destroyed and to assist them in the actual destruction methods.*

"Maybe I should talk with Troy Walker. He has security-related responsibilities for this division. He needs to review the division's classified information disposal program. I'm sure you folks

have a program. It just doesn't seem to be understood or followed."

"Anne, don't judge everyone around here by me. A lot of conscientious people work here."

"I know," Anne replies. "I just want to check with Troy."

As Anne heads over to Troy's office, let's summarize the reasons we hold on to classified items.

Reasons we hold on to classified items include...

- **We are unaware that the item may be disposed of.**
- **We believe that we will need the item in the future.**
- **We believe the destruction process is inconvenient or we don't know how to do it.**
- **Our egos get in the way.**
- **We think we can use the items to justify manning.**
- **Our workplace does not have an established program to dispose of classified items.**

Why We Should Dispose of Unneeded Classified Items-----

The discussion between Anne and Margaret centered on reasons people tend to hang on to classified information. Now let's look at some reasons why we should dispose of classified items after they have served their purpose.

Reasons to dispose of classified items include...

- To reduce holdings
- To free up storage space
- To save resources and money
- To reduce risk of compromise



These are good reasons to get rid of classified documents and materials as soon as we have no operational need for them, especially the last two.

There are security costs associated with maintaining classified items. These costs are in dollars and time. It follows, then, that the less classified information you have to maintain, the lower your security costs.

And let's get back to that classified document that has been sitting around for two years without being opened. That document may no longer be important to operational requirements, but it's still got classified information in it. As long as we have the document, the potential for compromising the information in it exists. It requires protection. If the document had been destroyed, no compromise can occur from an unauthorized disclosure and no protection would have been required.

And related to this, it's possible that "out of sight, out of mind" might apply. If this is true, the likelihood of an undiscovered compromise increases.

Techniques for Helping People Reduce Holdings

Anne arrives at Troy's office. She fills him in on her recent discussion.

"I'm sorry to hear of the things you've told me," Troy says. "I'll certainly keep them in mind. I know we've had a lot of new hires lately and with all the events taking place recently, perhaps I've slipped in ensuring that our classified materials disposal program is working."



"What kind of things do you do in your program?"

"Well, for one thing we make *assistance visits to the various offices*. These visits can be formal or informal. Sometimes they are based on a formal inspection, like an IG inspection; at other times, they may be simply a visit to an office to answer a question or solve a problem. Anyway, while we're at the office, we look *at their files*. If we see an old document that doesn't seem to have any use, we ask them why they are keeping it. We can't tell someone that they don't need a document for their job; that's a decision they have to make. But *we challenge people and make them account for what they have*. By questioning their holding on to a document we hope that they will realize that they might not need that item after all."

"Anything else?" Anne asks.

"We try to *consolidate holdings*," Troy says. "We try to get co-workers to *share classified documents* instead of each having a separate copy of a document. And we *establish central libraries* where documents and materials can be kept."

"And of course we take part in the *annual clean-out day*," Troy continues. "As you know, each activity must establish at least one clean-out day a year. We try to get people to spend a portion of the day identifying classified items no longer needed and then destroying them."

"Do you use review sheets?" asks Anne.

"I'm not familiar with those," Troy says.



"What you do is attach a *review sheet* to each classified item. These sheets don't have to be anything elaborate. Anytime someone uses the item, they simply fill out the sheet, maybe just initials and the date. If you see that no one has looked at the item for, let's say, the last two years, you would have a pretty good indicator that the office needs to review whether or not they need to retain that item!"

"Sounds like a good idea," Troy says.

"How about the *availability of destruction equipment*?" asks Anne. "We know that if it's inconvenient to destroy the classified materials, people probably won't do it."

"We've bought a number of shredders in the past year and we've tried to place them in convenient locations," Troy says. "But you raise another issue too. I've been remiss in not *briefing our people on how to properly operate the equipment*. I suppose there are some people who are afraid of the equipment. I'll need to start a training program so people get familiar with using it."

"Thanks for the new ideas, Anne. I'm going to make an effort to improve our disposal program."

"Glad to hear it, Troy. And if I can help you, just give me a call."

As Anne heads back to her office, let's list the techniques that she and Troy talked about for helping people to reduce their classified holdings.

Some ways to reduce classified holdings...

- **Make assistance visits.**
- **Consolidate holdings.**
- **Make disposal of classified part of the *annual* clean-out day.**
- **Attach review sheets to documents to monitor use.**
- **Increase availability of destruction equipment.**
- **Familiarize people with the use of destruction equipment.**

What Should Be Destroyed?

You should destroy those classified materials that are non-record files for you and for which you have no operational need.



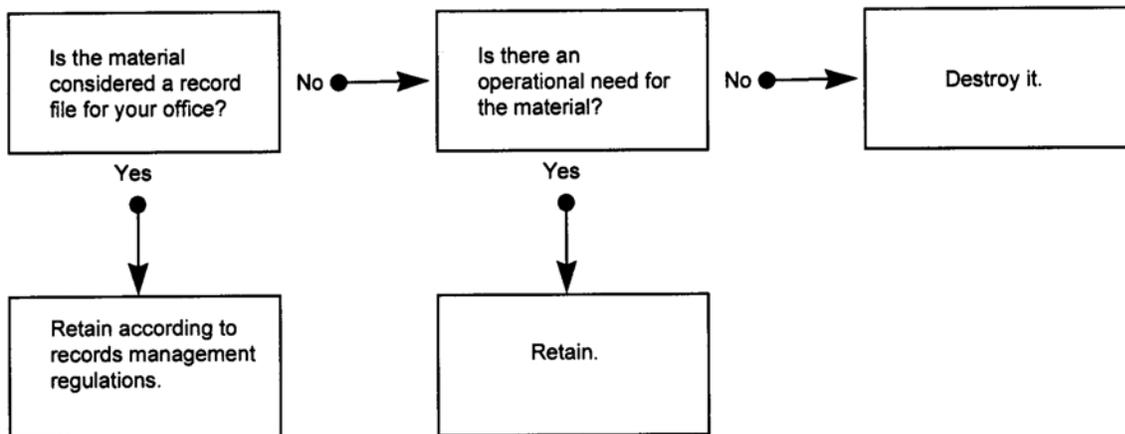
Classified documents and materials should be destroyed immediately if...

- **they are non-record files and**
- **there is no operational need for them.**

If the materials are *record files* for you, records management regulations determine how long you must maintain the files. We'll discuss record files and non-record files shortly. For now, just note...

Some classified materials *can't* be destroyed *even though they no longer serve an operational need.*

Deciding What To Destroy



Record files vs. Non-record files

Check with your *records management office* or *information resource management office* to find out exactly what documents are *record files for your office* and what documents are *non-record files for your office*.

As a general rule of thumb, files that are *generated or created by your office* - documents, memos, etc. - would be considered *record files for your office*. These record files, *whether classified or unclassified*, are *subject to records management regulations*, and you are *required to keep them for specified periods*.

If you have a copy of a *document that some other office or activity created*, then that copy is probably considered a *non-record file* for you. You can destroy any *non-record file as soon as it has served its intended purpose*.

Historical Records



Some classified documents are considered *records of significant historical value* and must *never be destroyed*. Again, your organization's records management or information resource management people can help you identify such records. Historical records are a subset of record files, so *all historical records are record files*. If records with permanent historical value are destroyed, the person responsible may be *fined up to \$5,000 and sentenced up to 5 years in prison*.

Who Can Destroy Classified Materials?

As Anne is returning to the Security Office, she meets Margaret in the hallway.

"Hi, Margaret."

"I'm glad I ran into you, Anne! I was just now reading this Confidential document that I received from the Defense Testing Agency, and it dawned on me that I really didn't have an operational need to keep it. After our talk about people unnecessarily holding on to materials, I thought I should get rid of it. Well, just as I was thinking about this, Bob from our Operations Office came by and said that he was going to the shredder on the next floor to destroy a bunch of documents. He asked if I had any documents that I wanted destroyed. I was just about to hand him this document, when I had

second thoughts. Would it have been O.K. to give it to him to destroy?"

"What's his *clearance level*?" asks Anne.

"Top Secret."

"Would he have any *need-to-know* for the information in the document?"

"No, he wouldn't. This document is on a project that his office doesn't do any work for, and the subject is outside the scope of his work."

"Then you did the right thing," says Anne. "People often forget that the rules of access apply even to classified materials that are about to be destroyed. *Clearance* and *need-to-know* must be *enforced* until the materials are in such a state that *no discernible information can be extracted from the residue.*"

Not everyone is permitted to destroy classified materials. There are three general categories of authorized personnel.



People authorized to destroy classified materials include...

- Custodians/users
- Designated individuals
- Specified control officers

These three categories of people are authorized to destroy classified materials because through their *job functions* they are *authorized access to the materials*. The objective is to limit access to the materials to those who require the access. *Custodians or users* are already authorized access to the materials, so they can destroy the materials. *Designated individuals*, properly cleared, may be

assigned the destruction task for an activity and, because of their assignment, require access. Some activities have a central destruction facility, and allow only designated people to destroy classified materials. *Specified control officers* are people responsible for accounting for classified information. Their job is to track and ensure control over the classified materials assigned to their organization -either the entire activity, or just their office. Since they are authorized access to the materials, they are authorized to destroy them.

Methods of Destruction

Now that we've discussed why classified materials should be destroyed and who may destroy them, let's discuss how they may be destroyed.

Classified items must be destroyed in a way that ensures that *the classified information can't be recognized or reconstructed*. Several methods are authorized. Whatever destruction method you use, it *should not harm or injure anyone*.



Destruction Methods

- **Burning**
- **Shredding**
- **Pulverizing**
- **Pulping**
- **Melting**
- **Chemical decomposition**
- **Mutilation to preclude recognition**

Burning



Burning is an authorized method for destroying classified materials, but there are three areas of concern with it. First, you must ensure that the burning is lawful. You can't just burn classified material wherever and whenever you feel like burning it. Not all locales allow the burning of refuse. And many that do permit burning may have passed environmental protection laws. For example, you might be required to use only facilities that produce emissions that meet strict air quality standards. Second, regardless of what equipment you use, such as a hospital incinerator or a hotel furnace, you must ensure that there is no unauthorized access to the materials while you are destroying them. Third, you must ensure that the burning is complete. Rake or stir the ashes to turn up any unburned material with discernible classified information. If you find any, burn it up.

Shredding



More and more people are using *shredders* as the destruction equipment of choice. They are relatively *cheap* (compared to an incinerator) and they are convenient. Your *Agency or Component headquarters sets the standards for shredders*. The key specification is the size that the shredder chops the materials down to. All shredders must have *cross-cut* capability to cut the material into confetti like bits, not just into long strips. Any shredder that cuts the materials into 1132" by 112" pieces will meet most Component requirements. No *information should be discernible from the pieces*. You should follow three procedures when using a shredder. First, *remove all staples and paper clips* from the documents. These materials will nick the shredder blades and eventually cause the shredder to "go out of spec." Second, *use the "secure volume" concept: Shred 20 or more pages at the same time*. The greater the volume of the bits produced, the

lower the chance that the classified information can be reconstructed.



The secure volume concept requires that you...

- Destroy 20 or more similar pages of classified paper at the same time

or

- Add sufficient similar types of unclassified pages to the classified document to arrive at the 20 page count

Third, *check the insides of the shredder after you use it.* Larger pieces may get stuck on the sides or they may slip through. And while you're in there, check the blades to ensure that they have not been dulled.

Pulverizing

A pulverizer grinds the materials into small pieces and pushes the pieces through a screen. The size of *the holes in the screen* through which the materials pass determines whether or not that pulverizer is an authorized one. *The Components set the standards.* You should not simply shove materials into a pulverizer and walk away. As with a shredder, after you have completed the process, you should *check the interior to ensure all materials have been properly destroyed.*

Pulping

Pulpers, like pulverizers, grind the materials into bits. However, a pulper adds water to the materials before it pushes them through a screen. The *size of the holes in the screen* determines whether or not the pulper is authorized. *Your Component headquarters sets the standards.* Again, like

shredders and pulverizers, you should *check the interior after the destruction process is completed*. Pulpers process only paper, so don't include microforms, microfiche, paper clips, staples, etc.

Other Destruction Methods

Other destruction methods, such as chemical decomposition and melting, are not as common as the ones we've discussed. Whatever the method used, the process should produce a residue from which no classified information can be gleaned.

Destroying Problem Materials

Certain materials can present problems in the destruction process because of their composition. Let's look at different types of materials and see how they are destroyed.

Microforms and Microfiche



Microforms and microfiche may be *burned*, if you have an incinerator designed to handle the *toxic emissions* created. These materials may also be *shredded*, but the plastic-like substance can cause the shredder to jam. And it is difficult to shred the classified information beyond discerning since it is imprinted on tiny areas that may not always be destroyed even by an authorized cross-cut shredder. An alternative method is to use *chemicals to decompose the imprints*. If you use a corrosive chemical, such as an acid, be sure that you take precautions to prevent injury while using it. For example, use protective eyewear and gloves. Also beware of inhaling toxic chemical fumes.

Typewriter Ribbons



Typewriter ribbons can be burned. However, you should not simply throw the entire ribbon cartridge into the furnace or incinerator. Before you start the process, you should *break apart the cartridge and cut the ribbon core into sections.* Then throw the *ribbon sections into the furnace.* Throwing the entire cartridge into the furnace could lead to a meltdown of the cartridge around the ribbon core, which could leave the core intact. An alternative method for destruction is to *shred* the ribbon. Here also, you need to *break apart the cartridge and cut the ribbon core.* Then *place the ribbon pieces between two sheets of paper* before placing them into the shredder. Both processes are long and dirty.

Videotapes



Videotapes can be *burned* or *degaussed* (demagnetized). If you burn your videotapes, you must ensure that the destruction equipment can safely handle any toxic emissions that could occur. Sometimes, instead of destroying videotape, you may want to erase the classified information on it and reuse the videotape. A good rule of thumb is, if you put classified information on videotape, treat that videotape as classified until you physically destroy the tape. However, there are occasions when you want to reuse it and handle it as an unclassified tape. To do this, you need to degauss (demagnetize) the tape. Degaussing, however, presents another problem. The magnetic properties of the videotape of the 1990's differ markedly from the low energy ferrous oxide coating of the 1960's and 1970's. Today's high-energy materials may or may not be adequately erased by today's degaussers. *Before you degauss videotape in order to declassify it, check with your Component headquarters or with the National Security Agency (NSA) for information on suitable equipment.*

Computer Disks



The computer magnetic storage media that most of us use is the floppy *disk* (5 1/4" or 3 1/2"). You can *burn* it, *degauss* it, or *overwrite* it. As with videotapes, a good rule of thumb is once you put classified information on a floppy, treat it as classified until you physically destroy it. If you *burn* your floppy disks ensure that the equipment you use can safely handle any *toxic emissions* that may occur. Like videotapes, when you want to *reuse* the disk but treat it as *unclassified*, *degauss* it. *Check with your Component headquarters or with NSA* for suitable equipment. *Overwriting is* another way to remove information from a floppy disk, but overwriting can inadvertently leave information on the disk. Again, *check with your Component headquarters or with NSA* on how to overwrite and on the limitations of overwriting.

Destruction at DIVA



As part of his decision to improve DIVA's disposal and destruction program for classified materials, Troy Walker has decided to see what Buzz Bradshaw, a co-worker, knows about disposal and destruction procedures.

"Hey, Buzz, it may seem like I'm giving you a pop quiz on security, but I'm not. I'm just trying to get a feel for what people know and don't know, so I know what to work on."

"It's O.K., Troy. Sometimes we tech folks get so wrapped up in our specifications and calculations we can lose sight of security."

"That's my concern all right. Since you are one of the people in the division designated to destroy classified materials, I want to go over the procedures with you. Maybe provide some refresher training if necessary."



"Check me out!" Buzz says.

"First, how do you know when you should destroy a particular document?"

"Well, if it's a non-record document for us and if I have no operational need for it, I earmark it for destruction."

"What about record files?" asks Troy.

"Then I follow the records management regulations on how long to retain them in my files."

"Good! Now take me through how you go about destroying the document."

"I protect it according to its classification level. I don't allow just anyone to handle or look at the document, only those with the proper clearance and need-to-know. So I'm very careful with our materials even at the shredder. After I finish the shredding, I always open it to check inside to make sure there are no large pieces stuck on the sides or still in the shredder."

"Well, Buzz, if this was a quiz, you'd get an A+'. Now if you have a little more time, maybe you can tell me what you think your co-workers know or need to know about the disposal and destruction process." And with that, Buzz and Troy got into a lengthy discussion of classified materials disposal and destruction.

Summary

In this lesson, you learned about the disposal and destruction of classified information. We identified reasons why people hang on to classified material needlessly: they don't know they can destroy it; they think they'll need it in the future; they think destroying it is inconvenient; they don't know how to destroy it; they think it makes them important and "most important" they don't have an established program for disposing of it. We looked at the reasons why we should dispose of classified material as soon as possible: to reduce the amount of it on hand; which in turn frees up storage space, saves resources, and reduces the risk of compromising it. We described techniques to help people reduce classified holdings: making assistance visits, consolidating holdings through sharing and central storage, including classified material during the annual clean-out day, attaching review sheets to classified materials to monitor use, increasing the availability of destruction equipment and familiarizing people with its use. We identified what should be destroyed: non-record files that no longer serve an operational need. We pointed out the three types of people authorized to destroy classified materials: the custodians /users, designated individuals, and specified control officers. We identified authorized destruction methods, the primary ones being burning, shredding, pulverizing, and pulping. We looked at ways to destroy problem items; microforms, microfiche, typewriter ribbons, videotapes, and computer disks. And we discussed protecting the materials while in the destruction process and checking to ensure that all materials have been properly destroyed.



REVIEW EXERCISES

1.
 - a. What is the primary reason people do not dispose of their classified holdings even when there is no need to retain them?
 - b. List three other reasons why people might hold on to classified materials that they should dispose of.
 1. _____
 2. _____
 3. _____
2. People should dispose of their unnecessary classified materials in order to reduce holdings, free up storage space, save on resources, and

3. You can reduce classified holdings with an annual _____ .
4. Classified materials should be destroyed immediately if:
 - a. they are non-record files and have no operational function.
 - b. they have historical significance but have no operational function.
 - c. they are non-record files and have an operational function.
 - d. they are record files but have no operational function.
5. Classified documents are exempt from records management procedures.
True. False.
6. The Operations Office has a Secret document, "European Theater Armor Tactics," but no operational need for it. Who is not permitted to destroy it?
 - a. Wilfred, who works in the Operations Office as the classified materials control officer.
 - b. Jennifer, who works in the Operations Office as the support officer for tactical operations in Europe.
 - c. Jim, who works in the Facilities Office as the activity's designated destruction official.
 - d. Bob, who works in the Transportation Office as the activity's automobile mechanic.

7. The four commonly used methods for destroying classified materials are:
- _____
 - _____
 - _____
 - _____
8. The burning of classified materials is exempt from environmental regulations because destroying them is essential to the national security.
True. False.
9. Sarah has a non-record one-page Confidential document for which her office has no functional need. She burns the document in her ashtray. To see whether the burn is complete, she stirs the ashes. No classified information can be discerned. Besides safety and fire-marshall violations, Sarah has also committed a security violation.

True. False.
10. The "secure volume concept." requires that you shred _____ or more similar pages of classified or unclassified paper at the same time.
11. When destroying classified materials you must (1) ensure that no unauthorized access to the materials occurs during the destruction and (2) after destruction, check _____

12. You may destroy classified material using any pulverizer or pulper that meets UL standards.

True. False.
13. The two common methods for destroying typewriter ribbons both require that you first _____
14. The three methods for destroying floppy disks are and _____ ,
_____ , _____ .

SOLUTIONS AND REFERENCES

1. a. Their workplace does not have an established program to help them identify what should be destroyed and help them destroy it. (P. 9-5)
b. Unaware that an item can be disposed of
Believe that they will need the item in the future
Destruction is an inconvenience
Not sure how to do it
Ego gets in the way
Think they can use the items to justify manning (p. 9-6)
2. reduce the risk of compromise. (p. 9-7)
3. clean-out day. (pp. 9-9, 10)
4. a. (p. 9-10)
5. False. (p. 9-11)
6. d. (pp. 9-13-14)
7. a. burning.
b. shredding.
c. pulverizing.
d. pulping. (pp. 9-15-16)
8. False. (p. 9-15)
9. False. (pp. 9-13, 15)
10. 20. (pp. 9-15-16)
11. to ensure all materials are properly destroyed. (pp. 9-14-17)
12. False. (p. 9-16)
13. break apart the cartridge. (p. 9-18)
14. burning, degaussing, and overwriting. (P. 9-19)

Index

A

addressing packages see transmitting/transporting
annual clean-out day. 9-9
Assistant Secretary of Defense for Command, Control,
Communications, and Intelligence [ASD(C³I)]. 1-9; 1-11

B

back cover markings
see marking
burning (destruction method). 9-15

C

caption markings see marking
"classified by" line see marking
"classified why" line see marking
classification
 approving of assignment. 2-13
 assigning level. 2-9
 challenge to. 2-8; 2-14
 communicating decision for. 2-10
 derivative
 definition of. 2-11; 4-4
 process of. 2-12; 5-3
 responsibility for. 2-11; 5-2
 using source documents. 5-10
 policy for duration of. 3-2
 original
 definition of. 2-3; 4-4
 process of. 2-6
 setting duration for. 2-9; 3-7
 tentative. 2-13
 types of. 2-3

classification categories. 2-7
classification levels. 2-2
classification policy of EO. 1-5
classified information
 definition of. 1-3
 designation of. 2-2
combinations, changing of. 7-17
Communications Security (COMSEC).
 1-7
containers
 see GSA approved security container and storage
 equipment
CONFIDENTIAL
 definition of. 2-2
 marking. 4-5
 storage requirements for. 7-13
 symbol for. 4-5
 transmitting/transporting methods.
 8-2
control markings
 see marking
copying classified
 see reproduction
cover markings
 see marking
Critical Nuclear Weapons Design Information
(CNWDI)
 definition of. 4-53
 marking of. 4-53
custodian
 definition of. 6-3
 responsibilities of. 6-3

D

DD Forms
see forms

declassification

- automatic. 3-9
- authority to conduct. 3-3
- changes to. 3-16
- definition of. 3-3
- extending. 3-17
- foreign government information. 3-15
- mandatory review. 3-13
- methods of. 3-9 OADR. 3-15
- OCA's options. 3-7
- of old information. 3-15
- re-evaluation. 3-12
- scheduled. 3-9
- systematic review. 3-12

"declassify on" line see marking

derivative classification see classification

"derived from" line see marking

destruction

- authorized destruction personnel. 9-13
- historical records. 9-12
- methods of. 9-14
- non-record files. 9-11
- problem materials. 9-17
- reasons to. 9-7
- record files. 9-11

disk destruction. 9-19

DoD 5200. 1 -R. 1 -11

downgrade

- authority to. 3-3
- automatic. 3-5
- definition of. 3-3
- extending. 3-17
- marking for. 3-5
- upon reconsideration. 3-5

downgrading instructions
see marking

E

Executive Orders

10290. 1-5

12958. 1-5

DoD implementation of. 1 -11

F

Federal Supply Schedule (FSS). 7-15

first page markings
see marking

foreign government information
declassification of. 3-15
inside US document. 4-58
marking of. 4-55

Formerly Restricted Data (FRD)

definition of. 1-6

declassification of. 3-6

marking of. 4-13; 4-51

forms

DD Form 2501. 8-13

SF 311. 1-9

SF 700. 7-17

SF 701. 6-10

SF 702. 6-12

SF 703. 6-4

SF 704. 6-4

SF 705. 6-4

front cover markings
see marking

G

GSA approved security container
characteristics of. 7-7

H

hand carrying classified materials
see transmitting/transporting

header markings
see marking

historical records
automatic declassification of. 3-9
non-destruction of. 9-12 "25-year rule." 3-9

I

illustration markings
see marking

inadvertent disclosure. 7-3

Information Security Program, purpose for. 1-4

Information Security Oversight Office (ISOO). 1-8

interior page markings
see marking

L

letter of authorization. 8-13" B-17

lock bar cabinet. 7-14

M

mandatory declassification review
see declassification

marking
agency information. 4-21; 4-24; 4-32
associated markings. 4-20
caption. 4-7
classified by" line. 4-21- 4-22
classified why" line. 4-1 -1 4-22
CNWDL 4-53
component parts. 4-34
control markings. 4-13 covers. 4-6; 4-18
date. 4-24; 4-32

"declassify on" line. 4-21; 4-23-1 4-26
"derived from" line. 4-21; 4-26

downgrading instructions. 4-21; 4-22; 4-26
face of document. 4-20
first page. 4-6; 4-16
Formerly Restricted Data. 4-13; 4-51
foreign government information. 4-55; 4-58; 4-60
headers. 4-7
illustrations. 4-7
interior pages. 4-6; 4-14
materials other than documents. 4-61
messages. 4-50
NATO information. 4-57; 4-59; 4-60
office of origin. 4-21; 4-24; 4-32
overall classification. 4-16
paragraphs. 4-7
portions. 4-6; 4-7
process summarization. 4-35
public domain information. 4-54
purpose for. 4-3
Restricted Data. 4-13; 4-51
subject lines. 4-7
subparagraphs. 4-7
titles. 4-7 title pages. 4-6; 4-18
transmittal letters. 4-48
unabbreviated. 4-5
warning notices. 4-13; 4-21; 4-24" 4-32; 4-51
wholly unclassified materials. 4-54
working papers. 4-51; 6-14

message markings
see marking

microform/microfiche destruction. 9-17

minimum risk. 7-4

N

National Security Council (NSC). 1-8

North Atlantic Treaty Organization (NATO)
markings. 4-57
markings when used inside US document. 4-59

O

office of origin markings
see marking

office supplies and work materials, handling of.
6-5

OMB Directive 1. 1-8

original classification
see classification

original classification authority
definition for. 2-3
delegation of. 2-4
responsibility of. 2-4
training of. 2-5

Originating Agency Determination Required (OADR)
see declassification

overall classification markings
see marking

P

preparing packages for transport
see transmitting/transporting

paragraph markings
see marking

portion markings
see marking

pulping (destruction method). 9-16

pulverizing (destruction method). 9-16

record files. 9-11

reducing holdings. 9-10

regrading. 3-17

R

reproduction of classified
approval for. 6-9 control of. 6-9
limitations on. 6-8

Restricted Data (RD)
definition for. 1-6
declassification of. 3-6
markings for. 4-13; 4-51

S

Sargent & Greenleaf 8077AC. 7-14
Sargent & Greenleaf 833. 7-14

SECRET
definition for. 2-2
markings for. 4-5
storage requirements for. 7-12
symbol for. 4-5
transmitting/transporting methods for. 8-2

secure telephone
see telephone

security manager responsibilities. 1-12

senior agency officials responsibilities. 1-12

Sensitive Compartmented Information (SCI). 1-7

SF 311
see forms

shredding (destruction method). 9-15

source documents, use of. 5-10

Special Access Program (SAP). 1-7

steel filing cabinet. 7-14

storage equipment
changing combinations. 7-17
designation of. 7-15
Federal Supply Schedule (FSS). 7-15
procurement of. 7-15
repair of. 7-18
supplemental controls for. 7-11

storage requirements
bulky materials. 7-14
CONFIDENTIAL. 7-13
overseas. 7-19
SECRET. 7-12
TOP SECRET. 7-11

storage standards. 7-7

STU-III
see telephone

subject line markings
see marking

subparagraph markings
see marking

systematic review
see declassification

T

telephone
using the STU-111. 6-6

title markings
see marking

title page markings
see marking

TOP SECRET
definition for. 2-2
marking of. 4-5
storage requirements for. 7-11
symbol for. 4-5
transmitting/transporting methods. 8-2

transfer of responsibility for declassification
official. 3-18
unofficial. 3-19

transmittal letter markings
see marking

transmitting/transporting classified materials
addressing packages. 8-5; 8-7
DD Form 2501. B-13
hand carrying requirements. 8-11
hand carrying summarization. 8-23
letter of authorization. 8-13; 8-17
methods for. 8-2
preparing packages for. 8-4

"25 year rule." 3-9

typewriter ribbon destruction. 9-18

U

UNCLASSIFIED
marking for. 4-5
symbol for. 4-5

V

videotape destruction. 9-18

W

warning notices
see marking

working papers
definition for. 6-14
handling of. 6-14
marking of. 4-51; 6-15

working with classified at home. 6-7