THE NATIONAL ACADEMIES

OFFICE OF PROGRAM SECURITY

DERIVATIVE CLASSIFICATION AND MARKING TRAINING

Revised January 2022

OSEC OFFICE OF PROGRAM SECURITY

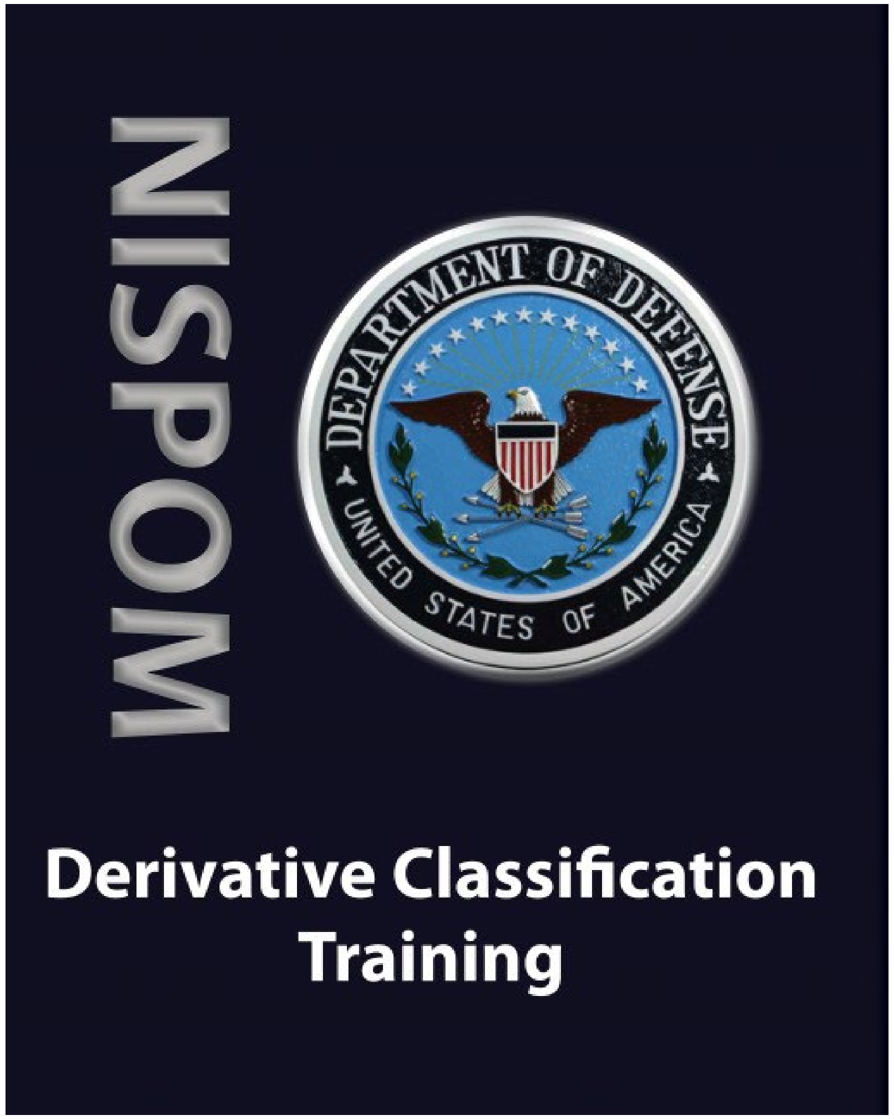
The National Academies of
SCIENCES • ENGINEERING • MEDICINE

WHY IS THIS TRAINING SO IMPORTANT TO NATIONAL ACADEMIES STAFF

- It’s a DOD Training Requirement
- Security Classification Review
- Good Information Stewardship

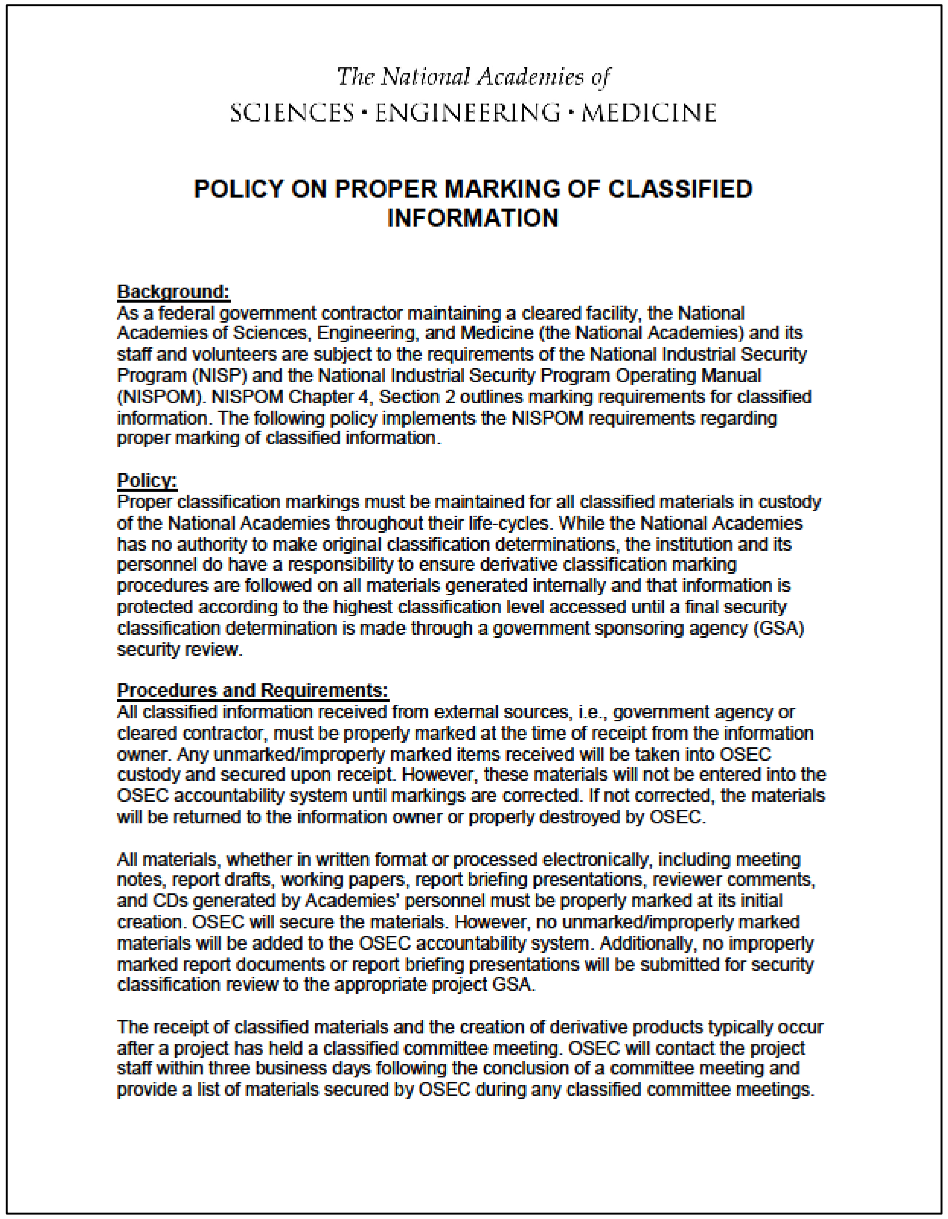
DERIVATIVE CLASSIFICATION TRAINING REQUIREMENT

- NISPOM 4-102 outlines derivative classification responsibilities for all cleared individuals.
- The Defense Security Service (DSS) also requires derivative classification training for all individuals that access export-controlled/ITAR information, Safeguards Information (SGI), and Sensitive Security Information (SSI).
- In addition to an Initial Derivative Classification Training, cleared individuals must complete a Refresher Training every two years.
- Training is available in-person through the Office of Program Security or online through DSS.
- Individuals due for Initial or Refresher Training will be contacted by OSEC to complete this training.



MARKING POLICY

- **In compliance with NISPOM Chapter 4, Section 2, the National Academies established the Policy on Proper Marking of Classified Information.**
- **Under the policy:**
  - All electronic and hardcopy documents received from external sources must be properly marked at the time of receipt.
  - All electronic and hardcopy documents produced by Academies' personnel and volunteers (including meeting notes, report drafts, working papers, report briefing presentations, reviewer comments, etc.) must be properly marked at its initial creation.
  - All unmarked/improperly marked electronic and hardcopy documents will be properly **destroyed** or **returned** to the information owner **7 business days after receipt or after committee meeting.**



The National Academies of
SCIENCES · ENGINEERING · MEDICINE

POLICY ON PROPER MARKING OF CLASSIFIED INFORMATION

Background:
As a federal government contractor maintaining a cleared facility, the National Academies of Sciences, Engineering, and Medicine (the National Academies) and its staff and volunteers are subject to the requirements of the National Industrial Security Program (NISP) and the National Industrial Security Program Operating Manual (NISPOM). NISPOM Chapter 4, Section 2 outlines marking requirements for classified information. The following policy implements the NISPOM requirements regarding proper marking of classified information.

Policy:
Proper classification markings must be maintained for all classified materials in custody of the National Academies throughout their life-cycles. While the National Academies has no authority to make original classification determinations, the institution and its personnel do have a responsibility to ensure derivative classification marking procedures are followed on all materials generated internally and that information is protected according to the highest classification level accessed until a final security classification determination is made through a government sponsoring agency (GSA) security review.

Procedures and Requirements:
All classified information received from external sources, i.e., government agency or cleared contractor, must be properly marked at the time of receipt from the information owner. Any unmarked/improperly marked items received will be taken into OSEC custody and secured upon receipt. However, these materials will not be entered into the OSEC accountability system until markings are corrected. If not corrected, the materials will be returned to the information owner or properly destroyed by OSEC.

All materials, whether in written format or processed electronically, including meeting notes, report drafts, working papers, report briefing presentations, reviewer comments, and CDs generated by Academies' personnel must be properly marked at its initial creation. OSEC will secure the materials. However, no unmarked/improperly marked materials will be added to the OSEC accountability system. Additionally, no improperly marked report documents or report briefing presentations will be submitted for security classification review to the appropriate project GSA.

The receipt of classified materials and the creation of derivative products typically occur after a project has held a classified committee meeting. OSEC will contact the project staff within three business days following the conclusion of a committee meeting and provide a list of materials secured by OSEC during any classified committee meetings.

Objectives

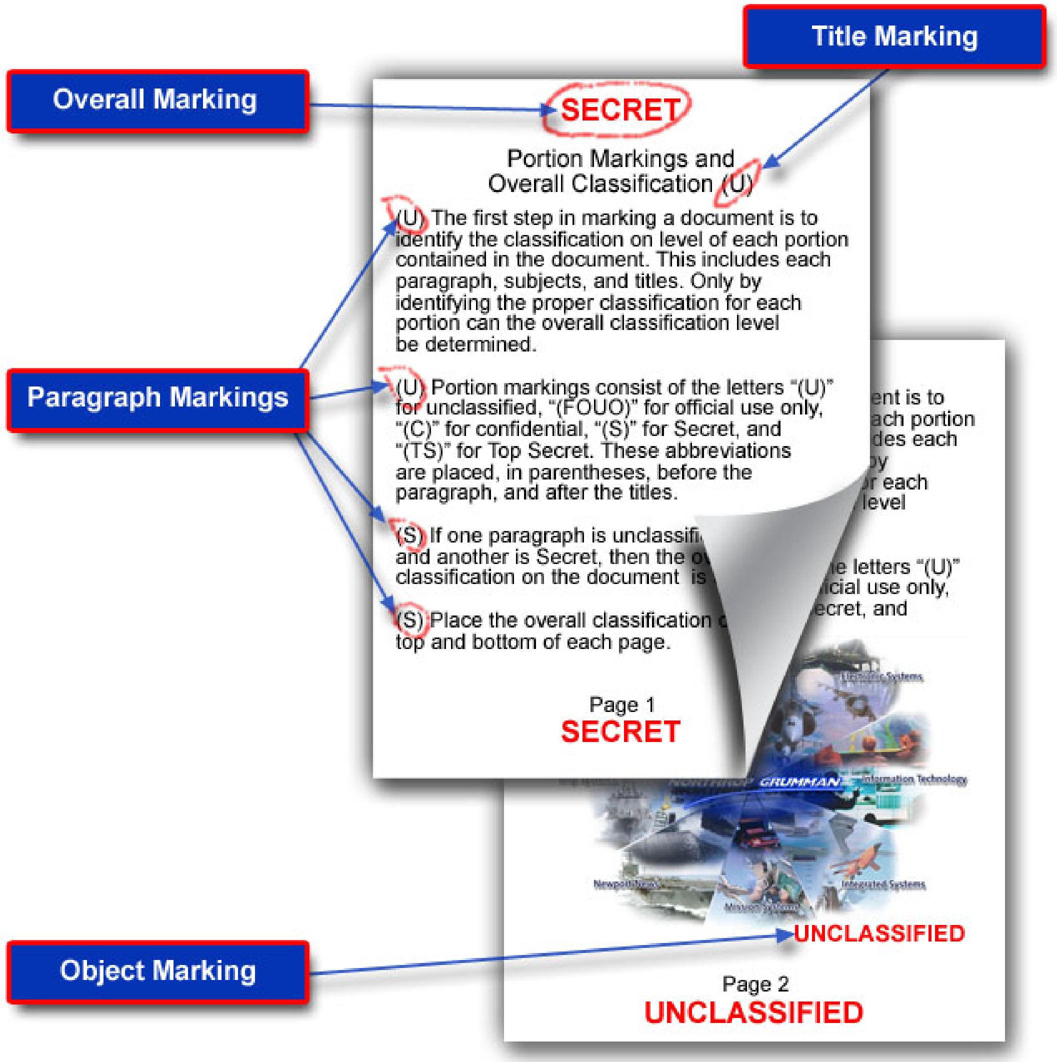
- Classification Levels
- Classification Authorities
- Authorized Classification Sources
- Principles of Derivative Classification
- Identification and Markings
- Duration Of Classification
- Classification Prohibitions and Limitations Classification Levels
- Sanctions, and
- Classification Challenges.

DERIVATIVE VS. ORIGINAL CLASSIFICATION

- **Original Classification**
  - The initial decision about what information should be classified. This authority is granted only a limited number of government officials.
- **Derivative Classification**
  - The process of using *existing* classified information to create new material, and marking that newly-developed material consistent with the classification markings that apply to the source information.
- **All cleared personnel who use or reference material from classified sources are Derivative Classifiers.**

**** Copying or duplicating existing classified information is not derivative classification.**

(NISPOM 4-101; 4-102; 4-104; ISL 2013-16 – Revised 12/04/13)



SECRET

Portion Markings and Overall Classification (U)

(U) The first step in marking a document is to identify the classification on level of each portion contained in the document. This includes each paragraph, subjects, and titles. Only by identifying the proper classification for each portion can the overall classification level be determined.

(U) Portion markings consist of the letters "(U)" for unclassified, "(FOUO)" for official use only, "(C)" for confidential, "(S)" for Secret, and "(TS)" for Top Secret. These abbreviations are placed, in parentheses, before the paragraph, and after the titles.

(S) If one paragraph is unclassifi and another is Secret, then the o classification on the document is

(S) Place the overall classification c top and bottom of each page.

Page 1
SECRET

UNCLASSIFIED

Page 2
UNCLASSIFIED

INTRODUCTION

- In the course of working with classified information, individuals sometimes generate or create new documents/materials based on that classified information.
- Individuals must carefully analyze their work product to determine what classified information it contains or reveals.
- They must ensure that the information in the new material is identified as classified by applying the appropriate markings to the material.
- These individuals are responsible for maintaining the protection of that classified information. These individuals are called DERIVATIVE CLASSIFIERS.

CLASSIFIED INFORMATION – DEPARTMENT OF DEFENSE; INTELLIGENCE COMMUNITY

- **There are three distinct classification levels within the Department of Defense system**
  - **Top Secret** – Information that if compromised can cause exceptionally grave damage.
  - **Secret** – Information that if compromised can cause serious damage.
  - **Confidential** – Information that may cause damage.
- **These types of classified information are usually described as “collateral” information**
- **The Intelligence Community may identify additional access restrictions through compartmentalization.**
  - **SCI** – Sensitive Compartmented Information is information derived from intelligence sources and methods.

(Executive Order 13526; ICD 704)

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE ★ UNITED STATES OF AMERICA ★

SUBJECT CATEGORIES OF CLASSIFIED INFORMATION

- **Section 1.4 of Executive Order (E.O.) 13526, "Classified National Security Information"**
  - a. Military plans, weapons systems, 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, technological, or economic matters relating to the national security, which includes defense against transnational terrorism
  - f. United States Government programs for safeguarding nuclear materials or facilities
  - g. Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism
  - h. Weapons of mass destruction

UNCLASSIFIED CONTROLLED INFORMATION

- Export Controlled / International Traffic in Arms Regulations (ITAR)
- Sensitive Security Information (SSI)
- Safeguards Information (SGI)
- Controlled But Unclassified (CUI)
- Proprietary
- Other FOIA exempt categories

RESPONSIBILITIES OF DERIVATIVE CLASSIFIERS

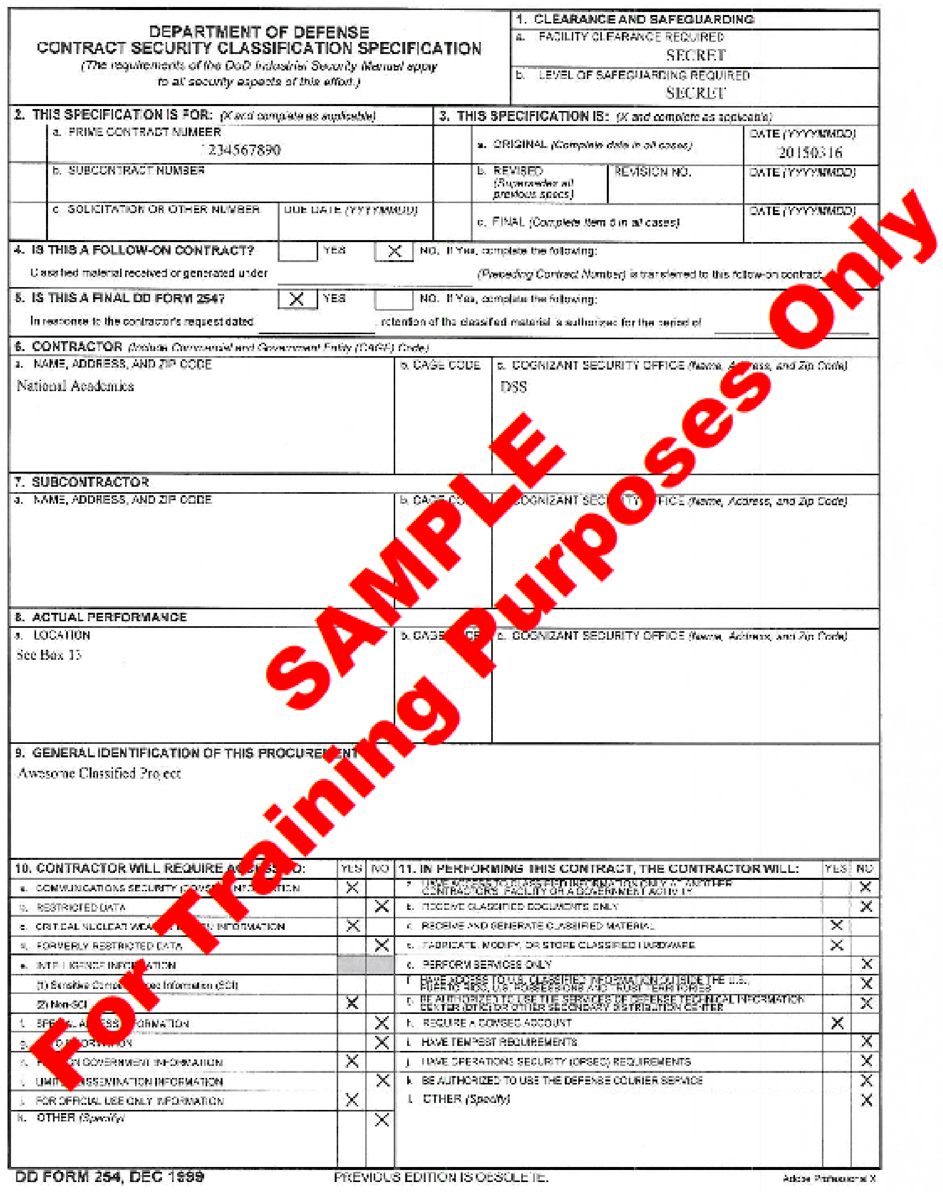
- **Observe and respect the original classification authority's decision**
- **Use only authorized sources to determine derivative classification**
- **Accurately mark derivatively classified materials according to the highest level of classified information contained in the new document**
- **Complete Required training**
  - Once every two years
  - Derivative classifiers who do not receive such mandatory training at least once every two years shall have their authority to apply derivative classification markings suspended until they have received such training.

AUTHORIZED SOURCES FOR DERIVATIVE CLASSIFICATION

- **There are only three authorized sources for derivative classification:**
  - **Security Classification Guide (SCG)** - An SCG is a collection of precise, comprehensive guidance about a specific program, system, operation, or weapon system telling what elements of information are classified. For each element of information, the SCG includes its classification level, the reasons for that classification, and information about when that classification will be downgraded or terminated. For this reason, SCGs are the primary source for derivative classification.
  - **An existing, properly marked source document** from which information is extracted, paraphrased, restated, and/or generated in a new form for inclusion in another document. You must carry the classification of that existing material forward into your new end product.
  - **DD Form 254, the DoD Contract Security Classification Specification** - DD Form 254 provides classification guidance to contractors performing on classified contracts. It informs them of the level of information they will need to access, the required level of security clearance for access, and the performance requirements; for example, safeguarding and special security requirements.
- **To ensure that the original classification of information is maintained, derivative classifiers must use only authorized sources of classification guidance to derivatively classify information. While it might be tempting, derivative classifiers must not rely on their memories or general rules about classification.**

SAMPLE DD254

- “Contract Security Classification Specification”
- See Handout
- Something RSO must review carefully as it has critical security guidance information
- The types of DD254’s we receive have not had detailed marking information but it might so it is important that RSO are fully aware of the terms and details of their classified contract and DD254 Contract security specification



DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION
(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)

1. CLEARANCE AND SAFEGUARDING
a. FACILITY CLEARANCE REQUIRED: SECRET
b. LEVEL OF SAFEGUARDING REQUIRED: SECRET

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*	3. THIS SPECIFICATION IS: *(X and complete as applicable)*
a. PRIME CONTRACT NUMBER 1234567890	a. ORIGINAL *(Complete date in all cases)* — DATE (YYYYMMDD) 20150316
b. SUBCONTRACT NUMBER	b. REVISED *(Supersedes all previous specs)* — REVISION NO. — DATE (YYYYMMDD)
c. SOLICITATION OR OTHER NUMBER — DUE DATE (YYYYMMDD)	c. FINAL *(Complete Item 5 in all cases)* — DATE (YYYYMMDD)

4. IS THIS A FOLLOW-ON CONTRACT? □ YES ☒ NO. If Yes, complete the following:
Classified material received or generated under ________ *(Preceding Contract Number)* is transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 254? ☒ YES □ NO. If Yes, complete the following:
In response to the contractor's request dated ________, retention of the classified material is authorized for the period of ________

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE National Academics	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)* DSS

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

8. ACTUAL PERFORMANCE

a. LOCATION See Box 13	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT
Awesome Classified Project

10. CONTRACTOR WILL REQUIRE ACCESS TO:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	X	
b. RESTRICTED DATA		X
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	X	
d. FORMERLY RESTRICTED DATA		X
e. INTELLIGENCE INFORMATION		
(1) Sensitive Compartmented Information (SCI)		
(2) Non-SCI	X	
f. SPECIAL ACCESS INFORMATION		X
g. NATO INFORMATION		X
h. FOREIGN GOVERNMENT INFORMATION	X	
i. LIMITED DISSEMINATION INFORMATION		X
j. FOR OFFICIAL USE ONLY INFORMATION	X	
k. OTHER *(Specify)*		X

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		X
b. RECEIVE CLASSIFIED DOCUMENTS ONLY		X
c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	X	
d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	X	
e. PERFORM SERVICES ONLY		X
f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		X
g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		X
h. REQUIRE A COMSEC ACCOUNT	X	
i. HAVE TEMPEST REQUIREMENTS		X
j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		X
k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		X
l. OTHER *(Specify)*		X

DD FORM 254, DEC 1999 — PREVIOUS EDITION IS OBSOLETE. — Adobe Professional X

SAMPLE
For Training Purposes Only

EXAMPLES OF UNAUTHORIZED SOURCES OF CLASSIFICATION

Examples of unauthorized sources of classification:

- ☒ **Memory: "I remember that project was classified Secret 5 years ago, so it must be Secret now."**
- ☒ **Unconfirmed source: "Someone told me this document can be declassified."**
- ☒ **Just because: "I am going to classify this document Top Secret because that is how we have always done it."**
- ☒ **Media/Internet: "I saw it on the news last night so it must be declassified."**

CLASSIFIED INFORMATION IN THE PUBLIC DOMAIN

Never

Comment,

Confirm, or

Deny

references to Classified Activities in the Public Domain.

Classified information in the public domain is still CLASSIFED!

You should never comment on or further disseminate this type of information. You are recognized as a knowledgeable expert and comments you make could be very damaging to national security.

DERIVATIVE CLASSIFICATION PROCESS

- Analyze
- Use Only Authorized Sources
- If Needed Seek Additional Guidance
- Mark Classified Material Properly

THREE WAYS DERIVATIVE CLASSIFIERS EXTRACT CONTENT

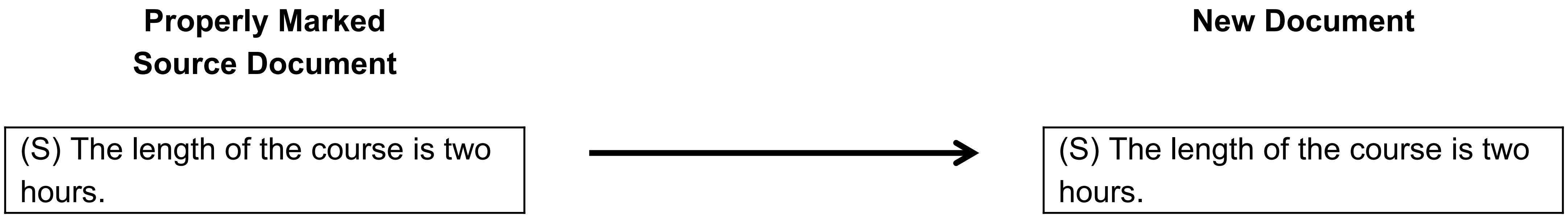
- Extracting occurs when information is taken directly from an authorized classification guidance source and is stated verbatim in a new or different document.
- Paraphrasing or restating occurs when information is taken from an authorized source and is re-worded in a new or different document. Derivative classifiers must be careful when paraphrasing or restating information to ensure that the classification has not been changed in the process.
- Generating is when information is taken from an authorized source and generated into another form or medium, such as a video, DVD, or CD.

** Copying or duplicating existing classified information is not derivative classification.

"CONTAINED IN"

The concept of "contained in" applies when derivative classifiers incorporate classified information from an authorized source into a new document, and no additional interpretation or analysis is needed to determine the classification of that information. In other words, when classified information in a new document is contained in the authorized source, the new document's classification is derived directly from the classification of that source. The concept of "contained in" can apply when the information is extracted word-for-word or when the information is paraphrased or restated from the existing content.

"CONTAINED IN"



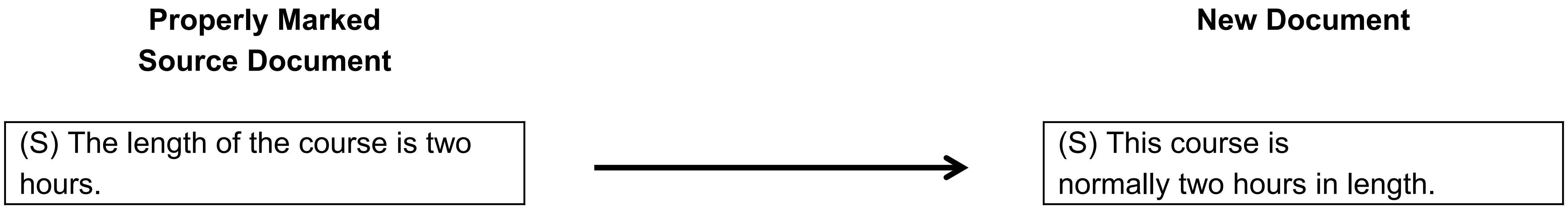
Properly Marked Source Document

(S) The length of the course is two hours.

New Document

(S) The length of the course is two hours.

- **In this example, the classification guidance is a properly marked source document. It contains classified information that has been extracted word-for-word into the new document. Because the information contained in the classification source was Secret, you must classify the new document Secret.**



Properly Marked Source Document

(S) The length of the course is two hours.

New Document

(S) This course is normally two hours in length.

- **Here, the information from the classified source is paraphrased and incorporated in the new document. Even though it is worded differently, the information in the new document is contained in the classified source, where it is Secret. Therefore, you must classify the new document Secret.**

“CONTAINED IN”

Security Classification Guide

	U	*C*	*S*	*TS*
length of course			X	

New Document

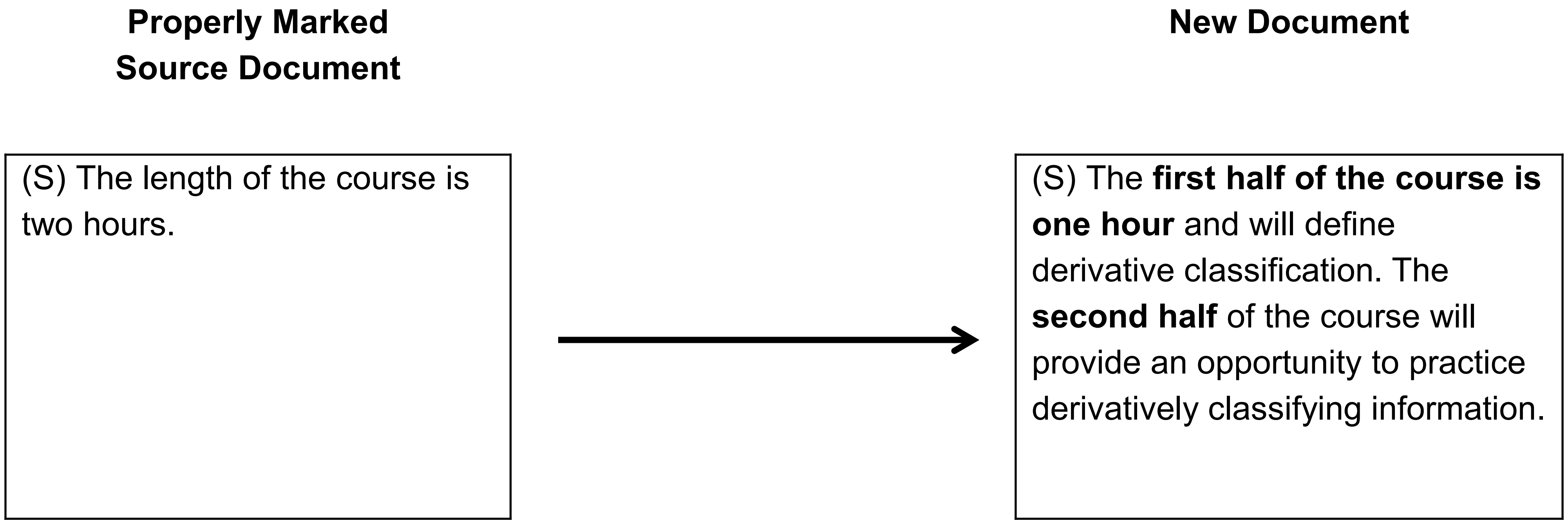
(S) This course is normally two hours in length.

- **This SCG provides that the information about the length of the course is classified Secret. Because you have stated this exact information in your new document, you must apply this Secret classification as dictated by the SCG.**

“REVEALED BY”

The concept of "revealed by" applies when derivative classifiers incorporate classified information from an authorized source into a new document that is *not* clearly or explicitly stated in the source document. However, a reader can *deduce* the classified information from the new document by performing some level of additional interpretation or analysis. In this sense, the classified nature of the information in the new document is *revealed by* analysis of its contents, so it will need to be marked in accordance with that classification.

“REVEALED BY”



Properly Marked Source Document

(S) The length of the course is two hours.

New Document

(S) The **first half of the course is one hour** and will define derivative classification. The **second half** of the course will provide an opportunity to practice derivatively classifying information.

- **The properly marked source document contains some Secret information. Your new document does not contain that same information. However, the information in your new document will allow a reader to deduce the classified information.**
  - If the first half of the course is one hour long, it follows that the second half would be the same length -- one hour. Since the course has two one-hour halves, it must be two hours long. This information is classified Secret according to the properly marked source document, so you must apply the same classification markings to the information in your new document.

REVEALED BY

Security Classification Guide

	U	*C*	*S*	*TS*
length of course			X	

New Document

(S) The **first half of the course is one hour** and will define derivative classification. The **second half** of the course will provide an opportunity to practice derivatively classifying information.

- **The concept of "revealed by" also applies when you are using an SCG as classification guidance. You need to look at what information can be deduced from what you have included in your new material and check whether that information is itself listed as classified in an SCG**

CLASSIFICATION BY COMPILATION

- **Sometimes combining two or more pieces of unclassified information can result in an aggregate that is classified. This occurrence is called compilation, or aggregation.**
- **Classification by compilation involves combining or associating unclassified individual elements of information to reveal an additional association or relationship that warrants a classified level of protection.**
- **Classification by compilation is not the norm when derivatively classifying information but it does happen.**
- **There are some special procedures to follow whenever you classify information by compilation.**
  - First, you must place a clearly-worded explanation of the basis for classification by compilation on the face of the new document or include it in the text.
  - You must also mark each element of information individually according to its classified content. This will allow subsequent derivative classifiers to use the individual elements at their original classification level.

CLASSIFICATION BY COMPILATION

Security Classification Guide

	U	*C*	*S*	*TS*
3.3.2.8 Single theater-wide operation failure report, outage report, problem report, or investigation report	X			
3.3.2.9 Compilation of two or more theater-wide operation failure reports, outage reports, problem reports, or investigation reports within the same document			X	

CLASSIFICATION BY COMPILATION

SECRET

(U) Investigation Report

(U) Table of Contents

(U) Introduction……………………………………………1
(U)* Theater-wide outage report………………………...2
(U)* Theater-wide problem report……………………....3

*Note that the compilation of two or more theater-wide operation failure reports, outage reports, problem reports, or investigation reports within the same document is classified as Secret.

SECRET

SEEKING FURTHER GUIDANCE

- **Remember, as a derivative classifier, you are not authorized to make original classification decisions. Rather, your duty is to derivatively classify new documents based on classification guidance and to seek clarification or further direction when the classification guidance is in question.**
- **If the classification in the existing content seems incorrect or there is conflicting guidance from authorized sources, you are required to seek further guidance.**
- **Some issues may lead you to believe that an existing document is incorrectly marked:**
  - These include the level of classification, the duration of the classification, special control requirements, and outdated classification guidance. When there is a conflict between an existing document and an SCG, the SCG takes precedence.
  - When you are unsure of how to mark the new document, personnel should contact their Facility Security Officer (FSO).
- **When in doubt, you should always seek additional guidance rather than guess or speculate how to mark the new document. Remember, your derivative classification determinations may have far-reaching effects on national security and the efficient use of resources.**

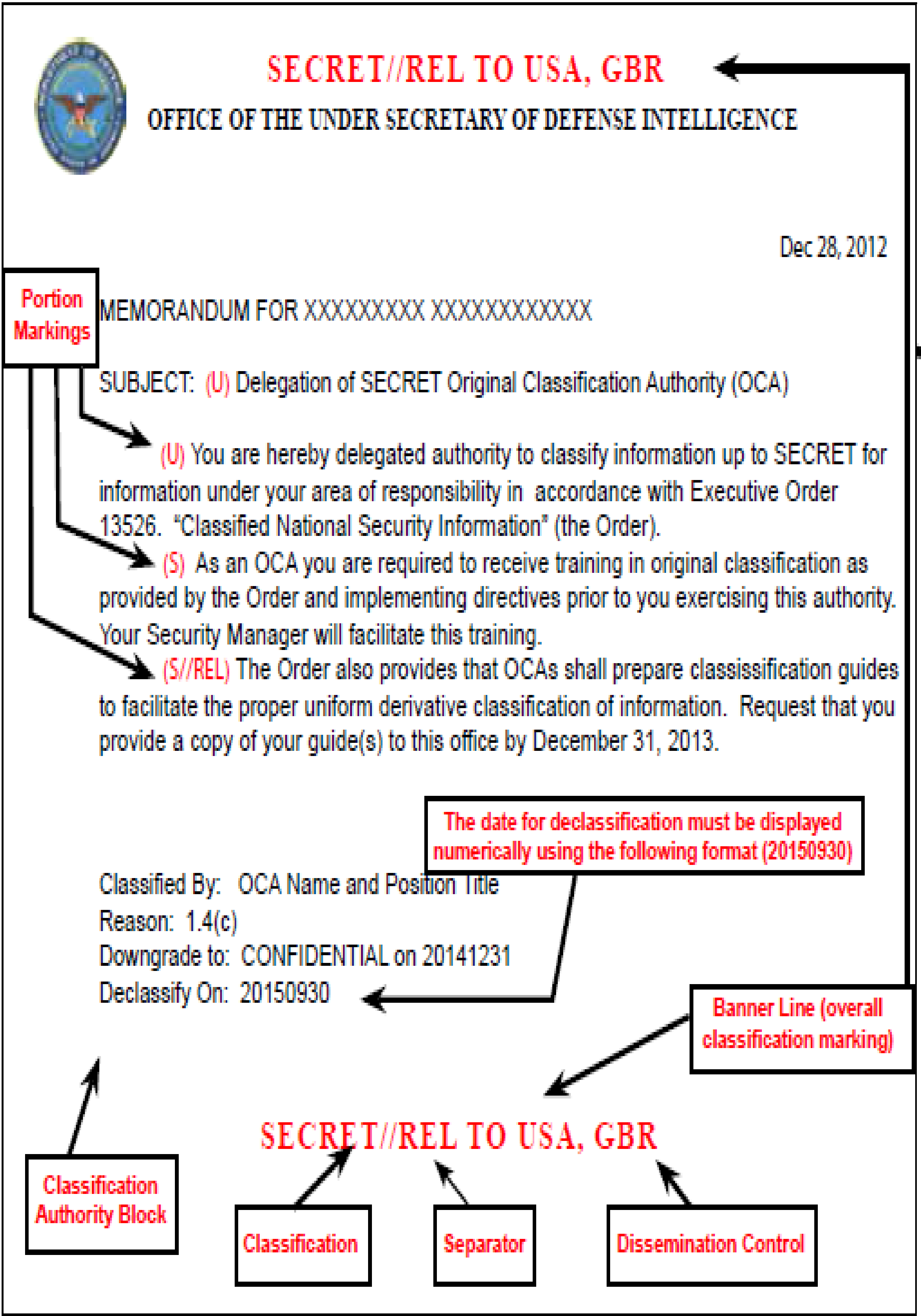
MARKING CLASSIFIED DOCUMENTS

Marking is the principal way of letting holders of information know the specific protection requirements for that information. Markings and designations serve several purposes; specifically, they:

- **Alert holders to the presence of classified information, information protected under the Freedom of Information Act (FOIA), and technical information with restrictions on its dissemination**
- **Identify, as specifically as possible, the exact information needing protection**
- **Indicate the level of classification and any other markings for control of the information**
- **Provide guidance on information sharing**
- **Provide guidance on downgrading (if any) and declassification**
- **Give information on the source(s) and reason(s) for classification or other restrictions**
- **Warn holders of special access, control, or safeguarding requirements**

MARKING CLASSIFIED DOCUMENTS

- You are going to encounter a couple types of documents when you start derivatively classifying. Originally classified documents, derivatively classified documents, and classified figures.



SECRET//REL TO USA, GBR

OFFICE OF THE UNDER SECRETARY OF DEFENSE INTELLIGENCE

Dec 28, 2012

Portion Markings

MEMORANDUM FOR XXXXXXXXX XXXXXXXXXXXX

SUBJECT: (U) Delegation of SECRET Original Classification Authority (OCA)

(U) You are hereby delegated authority to classify information up to SECRET for information under your area of responsibility in accordance with Executive Order 13526. "Classified National Security Information" (the Order).

(S) As an OCA you are required to receive training in original classification as provided by the Order and implementing directives prior to you exercising this authority. Your Security Manager will facilitate this training.

(S//REL) The Order also provides that OCAs shall prepare classissification guides to facilitate the proper uniform derivative classification of information. Request that you provide a copy of your guide(s) to this office by December 31, 2013.

The date for declassification must be displayed numerically using the following format (20150930)

Classified By: OCA Name and Position Title
Reason: 1.4(c)
Downgrade to: CONFIDENTIAL on 20141231
Declassify On: 20150930

Banner Line (overall classification marking)

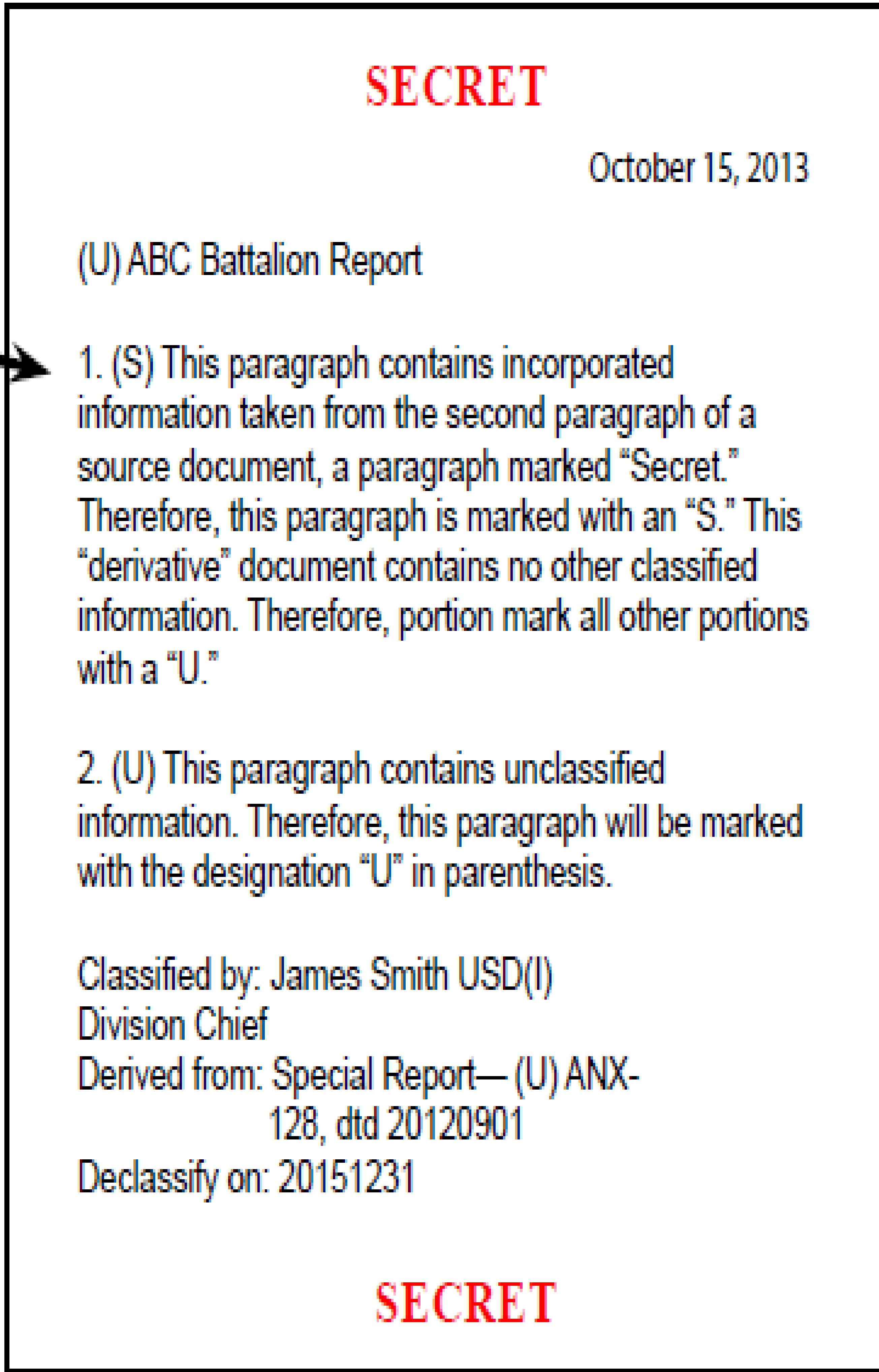
SECRET//REL TO USA, GBR

Classification Authority Block

Classification

Separator

Dissemination Control



SECRET

October 15, 2013

(U) ABC Battalion Report

1. (S) This paragraph contains incorporated information taken from the second paragraph of a source document, a paragraph marked "Secret." Therefore, this paragraph is marked with an "S." This "derivative" document contains no other classified information. Therefore, portion mark all other portions with a "U."

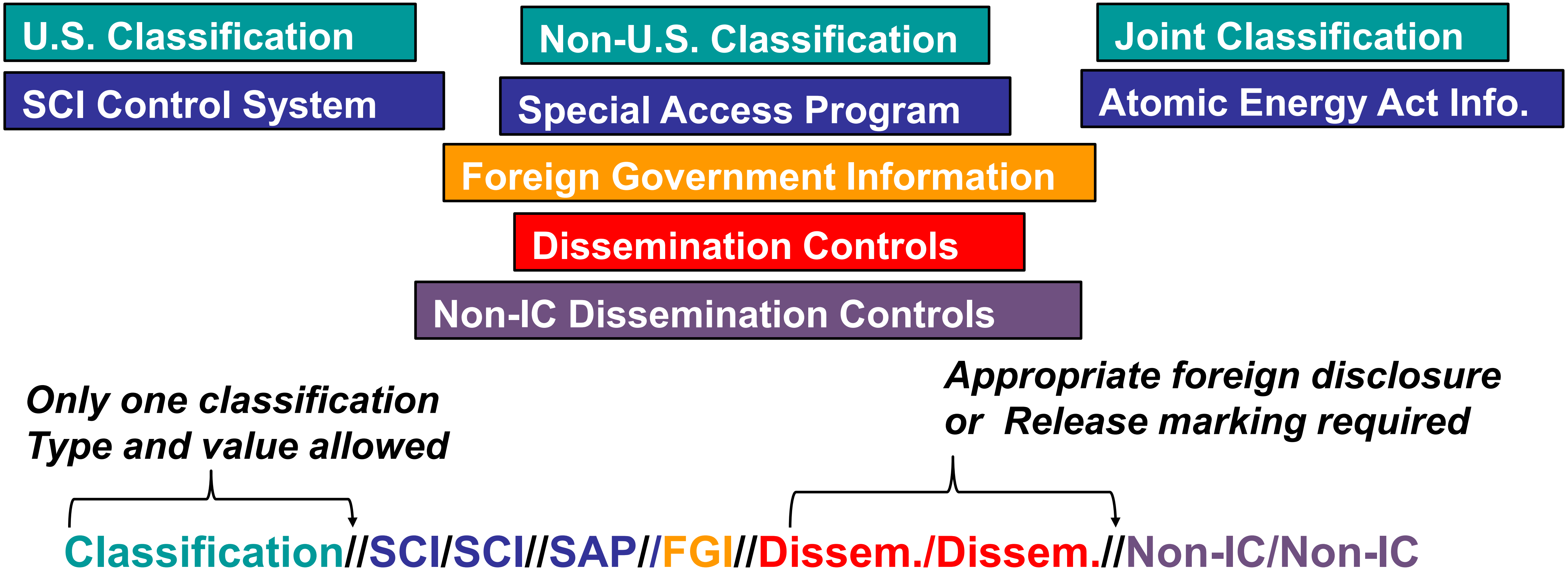
2. (U) This paragraph contains unclassified information. Therefore, this paragraph will be marked with the designation "U" in parenthesis.

Classified by: James Smith USD(I)
Division Chief
Derived from: Special Report— (U) ANX-
128, dtd 20120901
Declassify on: 20151231

SECRET

IC MARKING SYSTEM STRUCTURE

Marking Structure and Formatting



U.S. Classification

Non-U.S. Classification

Joint Classification

SCI Control System

Special Access Program

Atomic Energy Act Info.

Foreign Government Information

Dissemination Controls

Non-IC Dissemination Controls

Only one classification Type and value allowed

Appropriate foreign disclosure or Release marking required

Classification//SCI/SCI//SAP//FGI//Dissem./Dissem.//Non-IC/Non-IC

<u>Separators</u>

// Double forward slash is used to separate marking categories

/ Single forward slash is used to separate multiple values within a marking category

- Hyphen is used to link a marking to a sub-marking (e.g., SI-G or RD-SIGMA

“ “ Space is used to separate multiple sub-marking and multiple trigraph or tetragraph codes in the FGI Marking (e.g., //SI-ABD-G XYZW YYYY//or//FGI GBR JPN//

, Comma is used to separate multiple trigraph or tetragraph codes in the REL TO Marking

THIS STUDY ACTIVITY IS APPROVED TO ACCESS….

- **This activity is approved to access information up to ____________**

INFORMATION TO CAPTURE

- Overall Classification – Found in banner marking; consistent with the the highest and most restrictive level of information contained with in the document
- Portion Markings - e.g. (U) , (S), (TS), (U/ITAR)
- Classification Authority Box – Usually found in a box in the bottom corner of the document cover page/title page. Should contain the person who classified the information, the reason for the classification or the derivative source, date of derivative source, declassification date or instruction
- Other Source Information – Title of Document (not if title itself is classified), Author, Agency, Contact information, Classification Level, special instructions, original creation data, declassification data (when provided).

DURATION OF CLASSIFICATION

- **The duration specified on derivative documents must respect the duration specified by the OCA.**
- **The most restrictive declassification instruction (i.e., the one that specifies the longest duration of classification) must be carried forward.**
- **If not declassification data or obsolete or invalid declassification instructions are specified, derivative classifiers should apply a calculated 25-year duration from the date of the source document.**
- **Examples of Classification Duration**
  - A date or event 10 years from origination.
  - A date or event up to 25 years.
  - 25X1 through 25X9, with a date or event.
  - 50X1–HUM or 50X2–WMD, or Information Security Oversight Office (ISOO)-approved designator reflecting the Interagency Security Classification Appeals Panel (ISCAP) approval for classification beyond 50 years.

MARKING DERIVATIVE DOCUMENTS FROM MULTIPLE SOURCES

- Similar marking procedures as for derivatively classified documents from single sources but the source box contains additional information
- Also must include a list of the referenced documents
- May want to capture as footnote/endnote tied to each reference

Classified By: Jane Doe, President

Derived From: Multiple Sources

Declassify on: 21150406

Source 1

Classified By: John, ABC

Derived From: Multiple Sources

Declassify on: 21080922

Source 2

Classified By: Joe, DEF

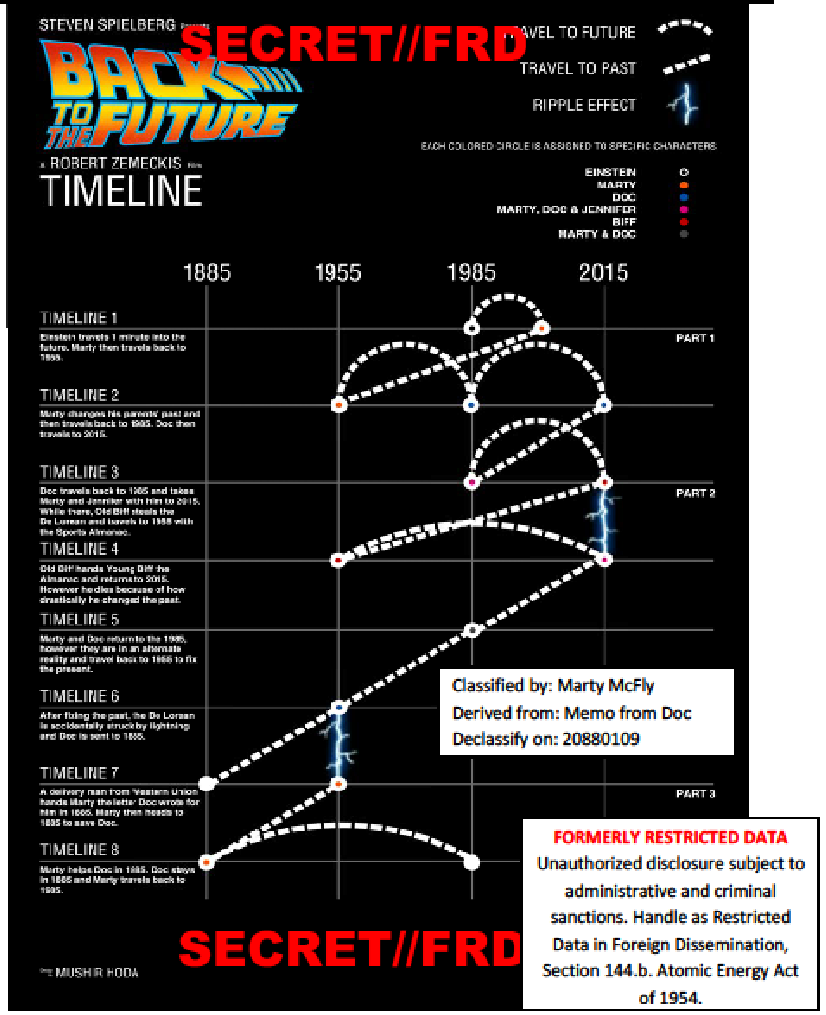
Derived From: Multiple Sources

Declassify on: 21150406

MARKING CLASSIFIED IMAGES, CHARTS, AND GRAPHICS

Sample Security Properly Marked Graphic
OSEC Classified Marking Training

(S/FRD) Back to the Future Timeline



SECRET//FRD

TIMELINE 1

Einstein travels 1 minute into the future. Marty then travels back to 1955.

TIMELINE 2

Marty changes his parents' past and then travels back to 1985. Doc then travels to 2015.

TIMELINE 3

Doc travels back to 1985 and takes Marty and Jennifer with him to 2015. While there, Old Biff steals the De Lorean and travels to 1955 with the Sports Almanac.

TIMELINE 4

Old Biff hands Young Biff the Almanac and returns to 2015. However he dies because of how drastically he changed the past.

TIMELINE 5

Marty and Doc return to the 1985, however they are in an alternate reality and travel back to 1955 to fix the present.

TIMELINE 6

After fixing the past, the De Lorean is accidentally struck by lightning and Doc is sent to 1885.

TIMELINE 7

A delivery man from Western Union hands Marty the letter Doc wrote for him in 1885. Marty then heads to 1885 to save Doc.

TIMELINE 8

Marty helps Doc in 1885. Doc stays in 1885 and Marty travels back to 1985.

Classified by: Marty McFly
Derived from: Memo from Doc
Declassify on: 20880109

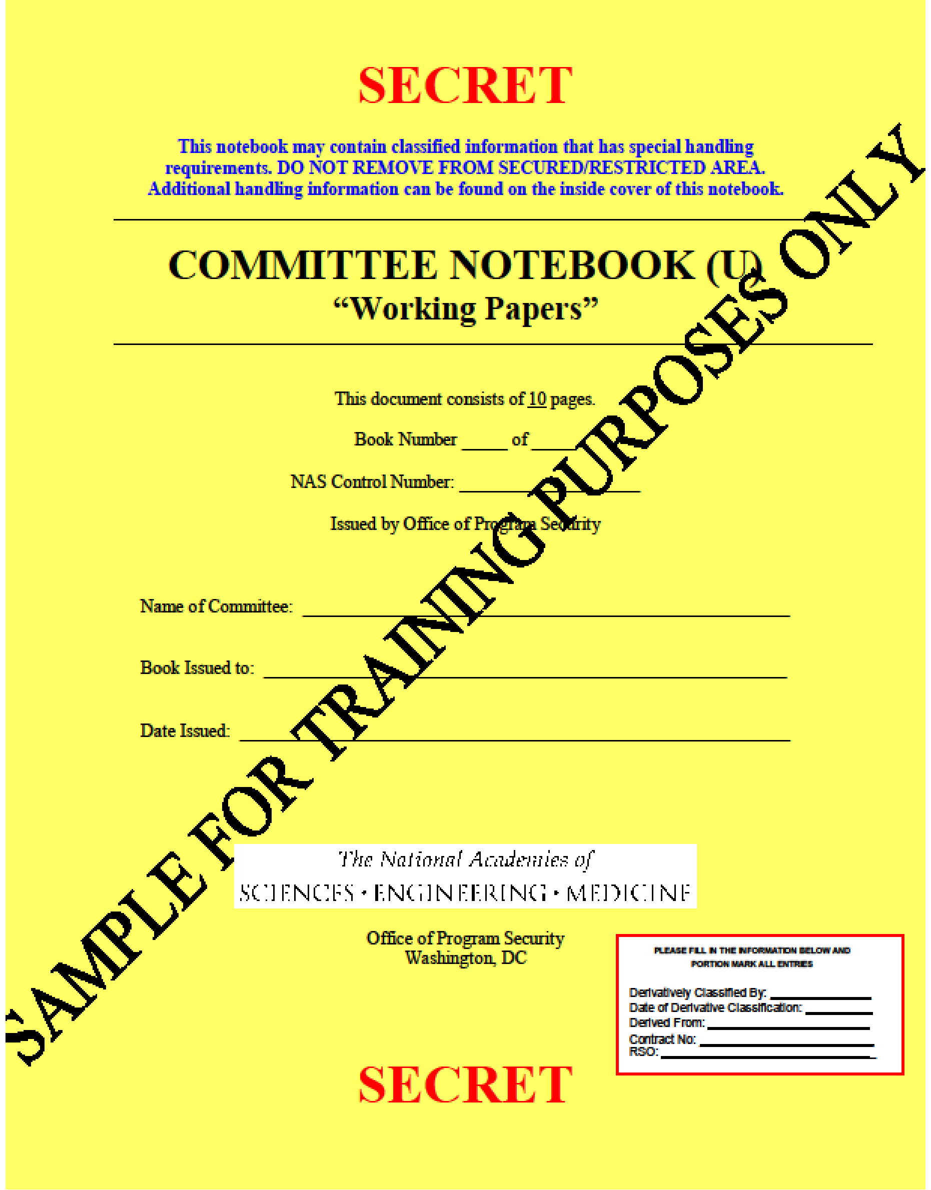
SECRET//FRD

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

FOR TRAINING PURPOSES ONLY

CLASSIFIED NOTEBOOKS AND MARKING INSTRUCTIONS

- Classified Notebooks are issued by OSEC and remain with in the secure area.
- Each notebook may contain classified and controlled unclassified information up to the highest level labeled on the notebook.
- Each cleared individual issued a notebook is required to derivatively mark the contents.



SECRET

This notebook may contain classified information that has special handling requirements. DO NOT REMOVE FROM SECURED/RESTRICTED AREA. Additional handling information can be found on the inside cover of this notebook.

COMMITTEE NOTEBOOK (U)
"Working Papers"

This document consists of 10 pages.

Book Number ____ of ____

NAS Control Number: ____________

Issued by Office of Program Security

Name of Committee: ______________________

Book Issued to: ______________________

Date Issued: ______________________

The National Academies of
SCIENCES • ENGINEERING • MEDICINE

Office of Program Security
Washington, DC

PLEASE FILL IN THE INFORMATION BELOW AND PORTION MARK ALL ENTRIES

Derivatively Classified By: ____________
Date of Derivative Classification: ________
Derived From: ____________________
Contract No: ____________________
RSO: ________________________

SECRET

DECLASSIFICATION

- Declassification must be confirmed by OCA before any release or change in safeguarding
- Classification terms may be extend under certain circumstances, it is important to confirm declassification rather than just assuming.
- Classified information in the public domain does not mean the information is automatically declassified
- Other restrictive markings may also need to be considered. e.g. other FOIA categories may required dissemination limitations, or handlings requirements

LIMITATIONS ON CLASSIFICATION OF INFORMATION

Information is prohibited from being classified

- **to conceal violations of law,**
- **to conceal inefficiency or administrative error,**
- **to prevent embarrassment to a person, organization, or agency,**
- **to restrain competition, or**
- **to prevent or delay the release of information that does not require protection in the interests of national security.**
  - basic scientific research and its results cannot be classified unless that information is clearly related to national security.

SANCTIONS MAY BE IMPOSED FOR...

SECURITY VIOLATIONS & INFRACTIONS

UNAUTHORIZED DISCLOSURES

TYPES OF SANCTIONS

- **Administrative – Institutional**
  - Revocation of Facility Clearance
- **Administrative – Personal**
  - Revocation of security clearance
  - Suspension without pay
  - Termination of employment
- **Criminal**
  - Incarceration
  - Fines

SECURITY INFRACTIONS

Compliance with Security Requirements is an ongoing part of your responsibilities as a cleared individual.

Any security incidents should be reported immediately to the Director of the Office of Program Security or his designee.

Security infractions which breach either The National Academies and/or government regulations relating to the safeguarding of classified information fall into two categories:

- **Minor Infraction –**
  - A minor infraction is any incident resulting from willful disregard, negligence, or unintentional failure to comply with security regulations or requirements and which does not result in compromise or suspected compromise of classified information.
- **Major Infraction –**
  - A major infraction is the willful disregard of the security regulations, or the failure through negligence to comply with any security regulations or requirements which does result in compromise or suspected compromise of classified information. Serious major infractions may rise to the level of statutory security violations and give rise to criminal and financial consequences.

INCIDENT REPORTING & THE GRADUATED SCALE OF DISCIPLINE

- **OSEC is required to submit a written account of all “serious” incidents to the Cognizant Security Authority (CSA) upon notifying the NRC Executive Officer and the President of NAS.**
- **A copy shall be maintained in the employee’s (or consultant’s) permanent security file.**
- **The National Academies addresses these infractions on a Graduated Scale.**

For minor infractions:

- 1st security violation - individual will be counseled by his/her manager and reminded of appropriate security procedures by Director of the Office of Program Security.
- 2nd security violation - individual may be reassigned from any duties requiring access to classified information.
- 3rd security violation - disciplinary action will be considered depending upon the nature and seriousness of the incident and previous compliance. This may affect continuing employment/affiliation with the institution.

For major infractions:

- 1st security violation - individual may be given a written warning which may include probation from accessing classified information and will be rebriefed by the Director, Office of Program Security.
- 2nd security violation - individual will be given written counseling and may be removed from access to classified information. This may affect continuing employment/affiliation with the institution.

.

CLASSIFICATION CHALLENGES

- **When should you challenge a classification?**
  - When you have substantial cause to believe the classification of the information is improper or unnecessary.

- **How should you challenge a classification?**
  - **Step One – Informal Challenge**

    1.a. Contact the your security program - The Office of Program Security

    1.b. Then, if necessary contact the Original Classification Authority (OCA) for clarification

  If an informal challenge does not resolve the issue proceed to

  - **Step Two – Formal Challenge**

    Contact the classifying agency in writing (agency must acknowledge in 60 days, respond with in 120 days or provide estimated response time)

  - **Step Three – Interagency Security Classification Appeals Panel (ISCAP) Appeal**

    Can appeal to ISCAP if challenge ends in denial at agency level ,or

    Agency violates response timeline requirements

CLASSIFICATION CHALLENGES

- **What happens while waiting for a determination?**

  Information must be handled and safeguarded according to the appropriate classification level until the issue is resolved.

- **Is classified information in the public domain considered unclassified?**

  NO! Classified information in the public domain is still treated as classified.

OFFICE OF PROGRAM SECURITY (OSEC) STAFF

If you have any questions or require additional information, please contact a member of the Office of Program Security.

Main Line:	**202-334-2106**
Main Email:	**osec@nas.edu**
Main Fax:	**202-334-2820**

Enita Williams
Director/ Facility Security Officer (FSO)

Kamilya Kamilova
Manager

Ross MacIsaac
Information System Security Manager

Mercedes Fauntleroy
Security Administrator

Appollonia "Appol" Miller
Security Compliance Assistant

ACKNOWLEDGEMENT FORM

Please *print* and *sign* the acknowledgement confirming you have read and agree to comply with the information contained in this briefing.

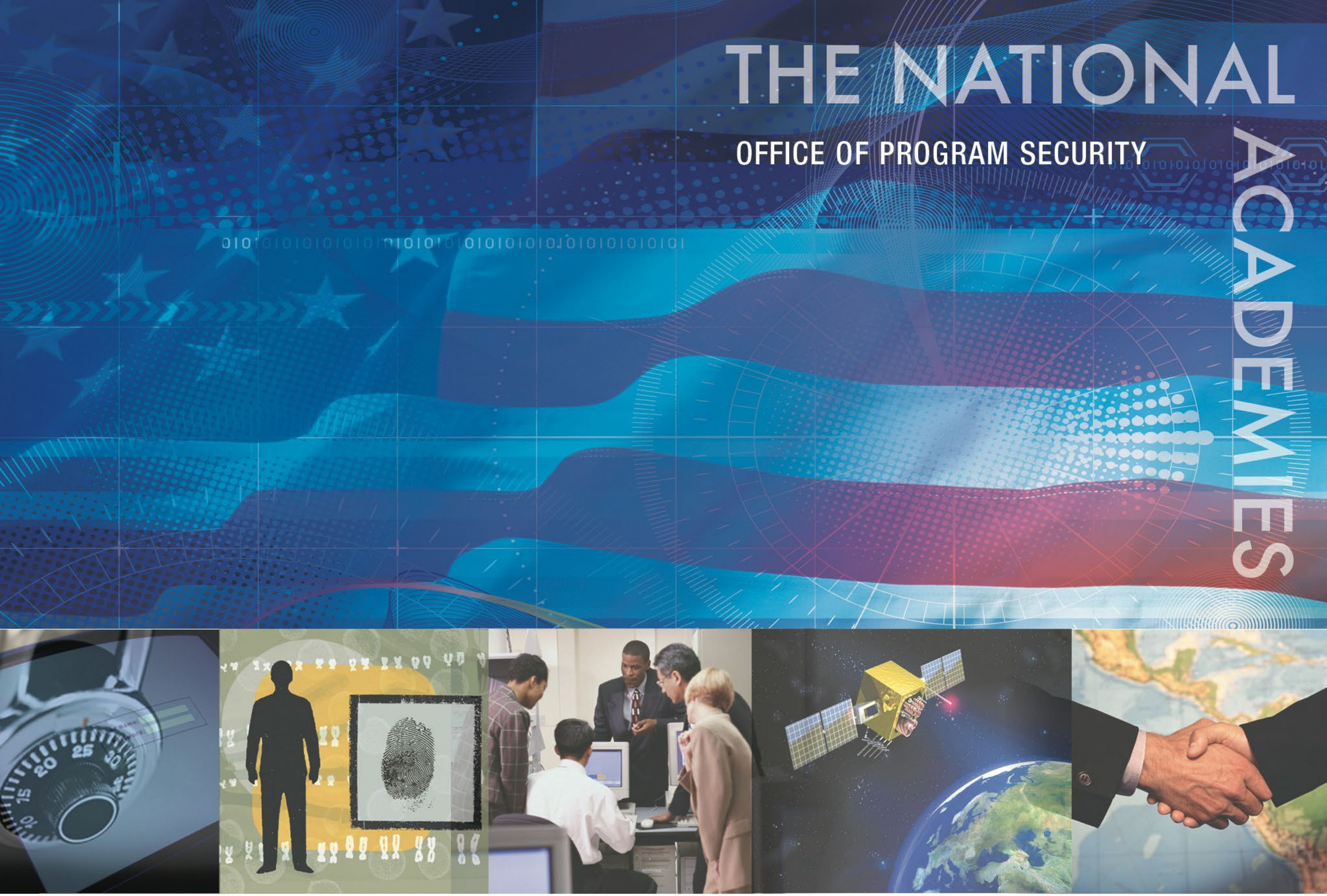
Return **the form to the Office of Program Security**

via email at osec@nas.edu

or fax at 202-334-2820.

** If you encounter any difficulty accessing the document,*
please contact OSEC at ***osec@nas.edu***
for an electronic copy of the form.

Derivative Classification Training
Acknowledgement Form



THE NATIONAL ACADEMIES

OFFICE OF PROGRAM SECURITY

OSEC OFFICE OF PROGRAM SECURITY

The National Academies of
SCIENCES • ENGINEERING • MEDICINE