
# DERIVATIVE CLASSIFICATION TRAINING

# JOB AID

CDSE Center for Development of Security Excellence

# Introduction

The purpose of this job aid is to provide reference information for the responsibilities and procedures associated with derivative classification.

This job aid also provides an overview of the approved security classification documents that assist in analyzing and evaluating information for identification of elements that require classification.

# Contents

Click the individual links to view each topic. You may also use the forward and backward arrows to navigate through each topic in order.


**Derivative Classification**

**Training Requirements**

**Principles of Derivative Classification**

**Prohibitions and Limitations**

**Classification Levels**

**Classification Duration**

**Classification Markings**

**Sources of Classification Guidance**

**Classification Challenges**

**Sanctions**

**Acronyms and Abbreviations**

# Derivative Classification

While working with classified information, individuals sometimes generate or create new documents and materials based on information derived from another classified document or a security classification guide, which is defined as derivative classification. Individuals who paraphrase and restate or summarize classified information, or who apply classification markings derived from source material or as directed by a security classification guide, need not possess original classification authority but will be acting as a Derivative Classifier.

The newly created documents created by the Derivative Classifier must be classified based upon the classification level of the information from which the new document was developed.

## Derivative Classifiers

The individuals responsible for applying derivative classification to documents are called derivative classifiers. Derivative classifiers can be either government or contractor employees.

Derivative classifiers are responsible for maintaining the protection and integrity of classified information. These individuals must possess expertise regarding the subject matter of the classified information, as well as classification management and marking techniques.

## Original Classification Authority (OCA)

An OCA is an individual occupying a position designated in writing that is charged with making the initial determination that information requires protection against unauthorized disclosure in the interest of national security.

When applying derivative classification to documents generated from classified information, derivative classifiers should observe and respect the classification determination of the OCA.

# Training Requirements

To accurately apply derivative classification, individuals must only use authorized sources. Prior to applying derivative classification markings, personnel must be trained in proper application of derivative classification principles.

Derivative classifiers who do not receive training annually shall not be authorized or allowed to derivatively classify information until they have completed training.

## Training Components

Training in the proper application of the derivative classification principles of Executive Order (E.O.) 13526 must be accomplished and must emphasize the avoidance of over-classification.

At a minimum, training should cover the principles of derivative classification, classification levels, duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, security classification guides, and information sharing.

**NOTE:** For both training requirements and components, refer to the eLearning course IF103.16 Derivative Classification available through STEPP.

# Principles of Derivative Classification

## The principles of derivative classification are:

- Use only authorized sources for classification guidance. The use of only memory or "general rules" about the classification of broad classes of information is prohibited.
- Observe and respect the classification determinations made by the OCA.
- Identify yourself by name and position, or by personal identifier, in a manner that is immediately apparent for each derivatively classified document you created.
- Apply standard markings to the derivatively classified material.
- Take appropriate and reasonable challenge steps to resolve doubts or apparent conflicts about the classification, level of classification, and duration of classification of information.
- Use caution when paraphrasing or restating information.

## Authorized Sources

Individuals should only use authorized sources of classification guidance, which includes:

- Security Classification Guides (SCG)
- Properly marked source documents

# Prohibitions and Limitations

There are several prohibitions and limitations derivative classifiers must be cognizant of when applying derivative classification.

In no case shall information be classified, continue to be maintained as classified, or fail to be declassified in order to:

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

# Classification Levels

As defined by E.O. 13526, information is classified at one of three levels: Top Secret, Secret, or Confidential.

## Top Secret (TS)

Top Secret classification shall be applied to information whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security that the OCA is able to identify or describe.

## Secret (S)

Secret classification shall be applied to information whose unauthorized disclosure could reasonably be expected to cause serious damage to the national security that the OCA is able to identify or describe.

## Confidential (C)

Confidential classification shall be applied to information whose unauthorized disclosure could reasonably be expected to cause damage to the national security that the OCA is able to identify or describe.

## Classification Level Review

Classified documents should be reviewed periodically to determine if the level of classification should be maintained, upgraded (will require OCA review and decision), downgraded, or declassified.

# Classification Duration

The duration specified on derivative documents must respect the duration specified by the OCA.

The declassification instruction from the source document will be carried forward to the newly created document.

If the source document or applicable security classification guide provides no declassification instruction from the OCA, or obsolete or invalid declassification instructions are specified, derivative classifiers should apply a calculated 25-year duration from the date of the creation of the derivative document.

## Examples of Classification Duration

Examples of classification duration include:

- A date or event 10 years from original classification.
- 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.

## Multiple Sources

When using multiple sources from either the SCG or source document, the date or event for declassification, which corresponds to the longest period of classification, shall be carried forward for derivative classification.

When material is derivatively classified based on "multiple sources" (i.e., more than one security classification guide, classified source document, or combination thereof), the derivative classifier shall compile a list of the sources used. This list shall be included in or attached to the document.

# Classification Markings

The derivative classifier should apply the following guidelines for classification markings:

- Classification markings shall be indicated in a manner that is immediately apparent.
- Each portion of a derivatively classified document shall be marked immediately preceding the portion to which it applies.
- Information must be marked as one of the three classification levels defined in E.O. 13526 (Top Secret, Secret, or Confidential).
- The "Classified By" line must include the name and position, or personal identifier, of the derivative classifier in a manner that is immediately apparent for each classification action.
- Identify the agency and office of origin, if not otherwise evident.
- All classified documents should include date of origin.
- Declassification instructions must be included on the document.

**NOTE:** Classified addenda or unclassified versions of documents should be used whenever practicable to facilitate greater information sharing.

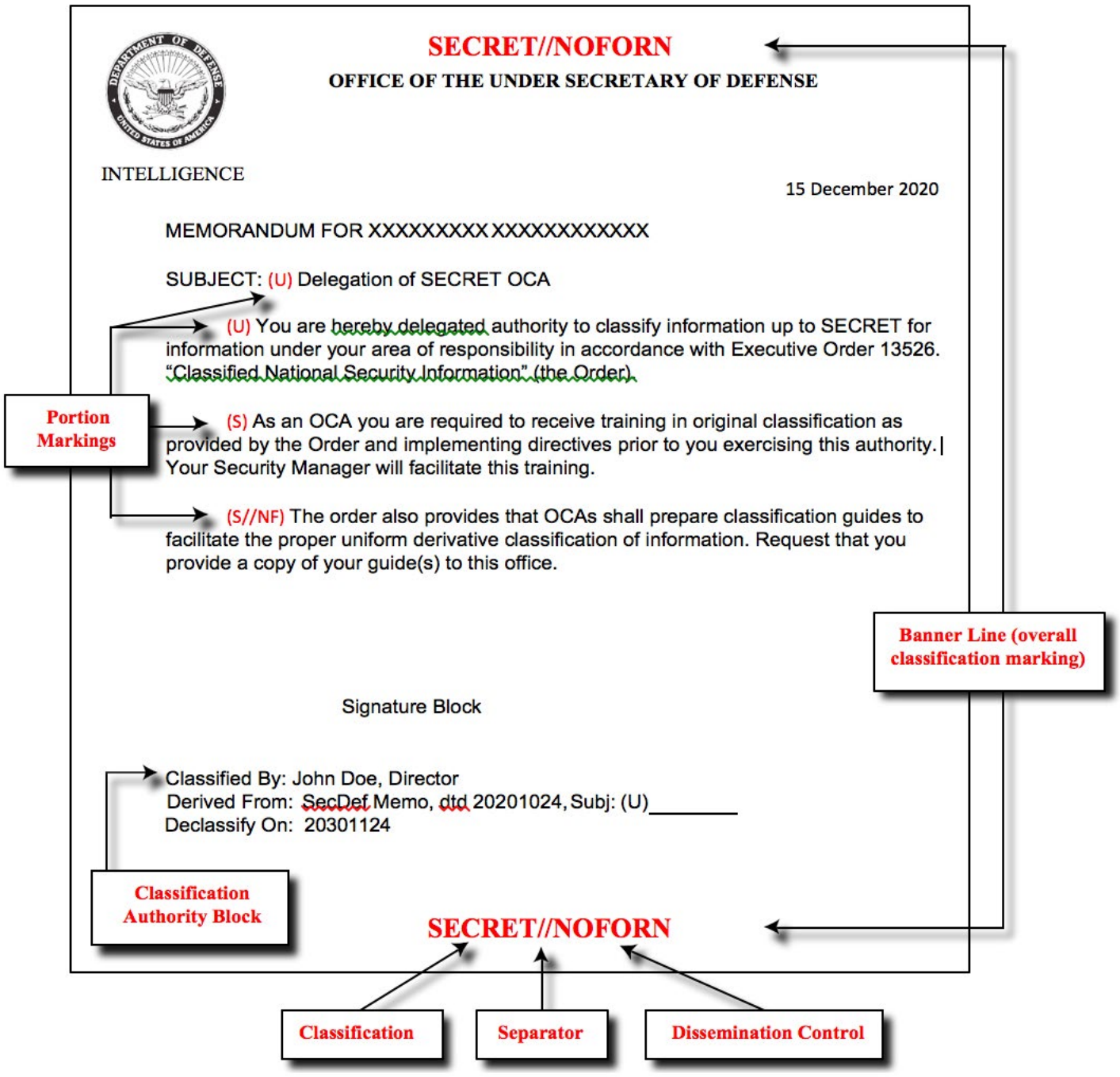
## Declassification Instructions

The date of declassification and duration between reviews is defined in the declassification instructions.

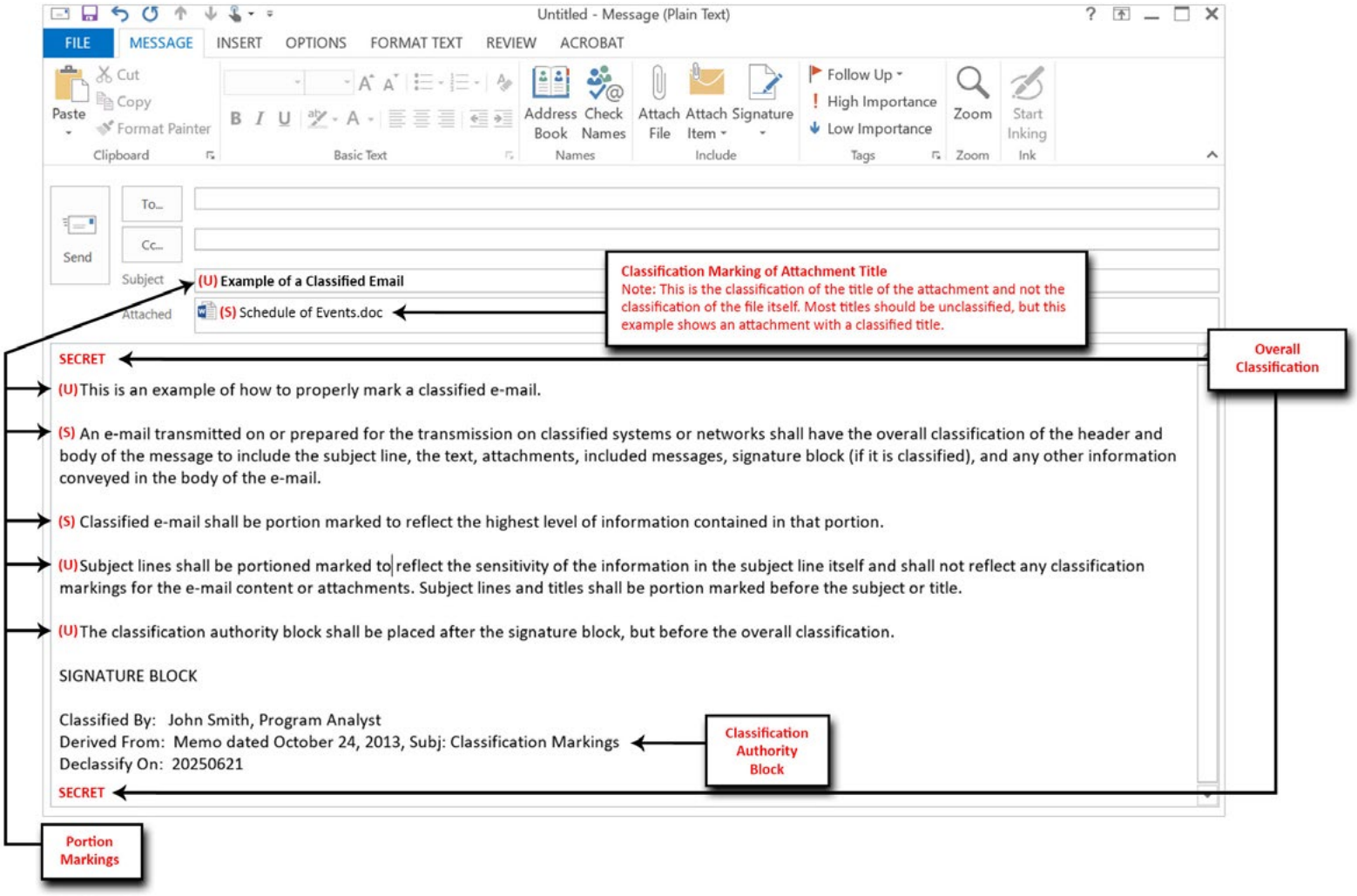
The following guidelines are applicable to declassification instructions:

- When declassification dates are displayed numerically, the following format shall be used: YYYYMMDD.
- The date of creation of the source documents must also be included with declassification instructions.

# Marking Example



# Marking Example



# Sources of Classification Guidance

A Security Classification Guide (SCG) is a record of original classification decisions and a collection of precise, comprehensive guidance about a specific program, system, operation, or weapon system identifying what elements of information are classified. For each element of information, the SCG includes its classification level, the reason(s) for that classification, and information about when that classification will be downgraded or declassified.

For this reason, SCGs are the primary source guidance for derivative classification.

## Source Documents

A second authorized source for derivative classification is 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. If there is an apparent marking conflict between a source document and an SCG regarding a specific item of information, derivative classifiers must follow the instructions in the SCG.

When multiple sources are used, a list of the source materials must be included in or attached to the new document.

## DD Form 254 (for Contractors)

Is NOT a source for derivative classification as stated in the past! The DD Form 254, the Department of Defense Contract Security Classification Specification, is used to identify specific classification guides or source documents that are to be referenced during the performance of a classified contract.

It provides classification guidance to contractors performing on classified contracts by referring the reader to another document, such as an SCG for specific classification guidance. The form identifies the level of information they will need to access, the required level of security clearance for access, and the performance requirements. For example, performance requirements may include safeguarding and special security requirements.

# Classification Challenges

Authorized holders of information, including authorized holders outside the classifying agency, are encouraged and expected to challenge the classification of information they believe is improperly classified.

A challenge to a classification decision occurs when the holder of information has cause to believe the information has been improperly or unnecessarily classified.

Informal questioning of classification is encouraged before resorting to formal challenge. If the authorized holder has reason to believe the classification applied to information is inappropriate, he or she should contact the classifier of the source document or material to address the issue.

## Timeline for Agency Response

Agency responses to classification challenges must adhere to the following:

- The agency must provide an initial written response to the formal challenge within 60 days. If the agency is unable to respond fully, the agency must acknowledge the formal challenge and provide an estimated date of response.
- The 60-day acknowledgement must indicate that if no response is provided within 120 days, the challenger has the right to forward the challenge to the ISCAP.
- If the information subject to the formal challenge has been challenged within the preceding 2 years or is currently under review, the agency must respond with this status and need not process the challenge.

**NOTE:** For additional information regarding classification challenges, refer to the eLearning course Classification Conflicts and Evaluations IF110.16, available through STEPP.

# Sanctions

Heads of the Department of Defense (DoD) Components must establish procedures to ensure that prompt and appropriate management action is taken in case of compromise of classified information, improper classification of information, and incidents that may put classified information at risk of compromise.

Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

## Management Actions

Management actions should focus upon correction or elimination of the conditions that caused or occasioned the incident. Individuals shall be subject to appropriate sanctions if they knowingly, willfully, or negligently:

- Disclose properly classified information to unauthorized persons;
- Classify or continue the classification of information in violation of E.O. 13526 or any implementing directive;
- Create or continue a Special Access Program (SAP) contrary to the requirements of E.O. 13526.
- Contravene any other provision of E.O. 13526 or its implementing directives.

# Acronyms and Abbreviations

| | |
|---|---|
| **CDSE** | Center for Development of Security Excellence |
| **(C)** | Confidential |
| **DoD** | Department of Defense |
| **DCSA** | Defense Counterintelligence and Security Agency |
| **E.O.** | Executive Order |
| **HUM** | Human |
| **ISCAP** | Interagency Security Classification Appeals Panel |
| **ISOO** | Information Security Oversight Office |
| **NF** | No Foreign |
| **OCA** | Original Classification Authority |
| **(S)** | Secret |
| **SCG** | Security Classification Guide |
| **STEPP** | Security Training, Education and Professionalization Portal |
| **(TS)** | Top Secret |
| **(U)** | Unclassified |
| **WMD** | Weapons of Mass Destruction |


CDSE Center for Development of Security Excellence

938 Elkridge Landing Road Linthicum, MD 21090

**www.cdse.edu**