Derivative Classification Training

Job Aid

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.

This job aid provides the required training for derivative classifiers as specified in E.O. 13526 and DoD Policy.

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

Derivative Classification

While working with classified information, individuals sometimes generate or create new documents and materials based upon that classified information. These individuals who reproduce, extract, or summarize classified information, or who apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

The newly created documents must be classified based upon the classification level of the information from which the new document was developed. This is defined as "derivative classification."

Derivative Classifiers

The individuals responsible for applying derivative classification to documents are called derivative classifiers.

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)

When applying derivative classification to documents generated from classified information, derivative classifiers must observe and respect the classification determination of the Original Classification Authority (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 at least once every 2 years, shall not be authorized or allowed to derivatively classify information until they have received training.

NOTE: For additional information, refer to the web-based training (WBT) course IF103.16 Derivative Classification available through STEPP.

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.

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 derivative classification action.
- Apply standard markings to the derivatively classified material.
- Take appropriate and reasonable 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
- Properly marked source documents
- Department of Defense (DD) Form 254 (for Contractors)

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.

NOTE: If there is significant doubt about the appropriate level of classification, the original classification authority (OCA) shall classify the information at the lower level.

Top Secret

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 original classification authority is able to identify or describe.

Secret

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

Confidential

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

Classification Level Review

Classified documentation is reviewed periodically to determine if the level of classification should be maintained, upgraded, downgraded, or declassified.

Classification Duration

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 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 source document.

Examples of Classification Duration

Examples of classification duration include:

- 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.

Multiple Sources

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

When derivatively classifying documents from multiple sources, a list of source material carried forward from the source document must be included in or attached to the new 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.
- 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.

Derivative Classifier Identification

Individuals who derivatively classify must be identified by name and position, or by personal identifier in a manner that is immediately apparent for each classification action.

This information must be included in the "Classified By" line. Also, identify the agency and office of origin, if not otherwise evident.

Declassification Instructions

Classified documentation is reviewed periodically to determine if the information should be declassified. 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 origin of source documents must also be included with declassification instructions.

Marking Example

SECRET//NOFORN

OFFICE OF THE UNDER SECRETARY OF DEFENSE

INTELLIGENCE

date

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 an 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/NF) The Order also provides that OCAs shall prepare classification 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, 2010.

Signature Block

Classified By: John Doe, Director
Derived From: SecDef Memo, dtd 20101024, Subj:(U) _____
Declassify On: 202011024

SECRET//NOFORN

Portion Markings

Banner Line (overall classification marking)

Classification Authority Block

Classification

Separator

Dissemination Control

Marking Example

E-Mail

Mail To:

File Edit View Actions Tools Accounts Window Help

Send Cancel Address Spell Check

Mail Send Options

From: John Smith CC:

To: BC:

Subject: (U) Example of a Classified e-mail

SECRET

(U) This is an example of how to properly mark a classified e-mail.

(S) An e-mail transmitted on or prepared for the transmission on classified systems or networks shall have the overall classification of the header and body of the message to include the subject line, the text, attachments, included messages, signature block (if it is classified), and any other information conveyed in the body of the e-mail

(S) Classified e-mail shall be portion marked to reflect the highest level of information contained in that portion.

(U) Subject lines shall be portioned marked to reflect the sensitivity of the information in the subject line itself and shall not reflect any classification markings for the e-mail content or attachments. Subject lines and titles shall be portion marked before the subject or title.

(U) The classification authority block shall be placed after the signatuyre block, but before the overall classification.

SIGNATURE BLOCK

Classified By: John Smith, Program Analyst
Derived From: Memo dated June 21, 2010, Subj: Classification Markings
Declassify On: 20150621

Classification authority block

SECRET

(S) Schedule of Events.doc

Classification marking of title of attachment

Note: This is the classification of the title of the attachment, and not the classification of the file itself. Most titles should be unclassified, but this example shows an attachment with a classified title.

Portion markings

Overall classification

Sources of Classification Guidance

A Security Classification Guide (SCG) is a collection of precise, comprehensive guidance about a specific program, system, operation, or weapons 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 guide 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.

A list of source material carried forward from the source document must be included in or attached to the new document.

DD Form 254 (for Contractors)

The third authorized source is the DD Form 254, the Department of Defense Contract Security Classification Specification.

The DD Form 254 provides classification guidance to contractors performing on classified contracts. 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.

Commonly, the DD Form 254 refers the reader to another document such as a security classification guide for specific classification guidance.

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 substantial cause to believe that 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 a 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 the challenge to the Interagency Security Classification Appeals Panel (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 the component need not process the challenge.

NOTE: For additional information regarding classification challenges, refer to the WBT course Classification Conflicts and Evaluations available through STEPP, or the instructor-led training (ILT) Information Security Management Course.

Sanctions

Heads of the 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 the order;
- Create or continue a special access program contrary to the requirements of this order; or
- Contravene any other provision of E.O. 13526 or its implementing directives.

Acronyms/Abbreviations

Acronyms/ Abbreviations	Definitions
CDSE	Center for Development of Security Excellence
DoD	Department of Defense
DSS	Defense Security Service
E.O.	Executive Order
ILT	Instructor-Led Training
ISCAP	Interagency Security Classification Appeals Panel
ISOO	Information Security Oversight Office
OCA	Original Classification Authority
SCG	Security Classification Guidance
WBT	Web-Based Training

Derivative Classification Training

Job Aid

Center for Development of Security Excellence

CDSE

Learn. Perform. Protect.

July 2011

Center for Development of Security Excellence