

Glossary

Course: Derivative Classification

Access: The ability and opportunity to gain knowledge of classified information.

Classification: The act or process by which information is determined to be classified information.

Classifier: An individual who makes a classification determination and applies a security classification to information or material. A classifier may be an original classification authority (OCA) or a person who derivatively assigns a security classification based on a properly marked classified source or a classification guide.

Classified National Security Information or “Classified Information”: Information that has been determined, pursuant to Executive Order 13526 or any predecessor order, or pursuant to the Atomic Energy Act of 1954, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Classification Guidance: Is an authorized source of classification guidance. Within DoD there are three authorized sources for classification guidance: a Security Classification Guide (SCG), a properly marked source document, and the DD Form 254, “Department of Defense Contract Security Classification Specification.”

Classification Guide: Also referred to as a Security Classification Guide (SCG). A document issued by an authorized original classifier that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element. A 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 the downgrading/duration of classification.

Cognizant Security Agencies (CSAs): Agencies of the Executive Branch that have been authorized by Executive Order 12829, “National Industrial Security Program,” to establish an industrial security program to safeguard classified information under the jurisdiction of these agencies when disclosed or released to industry. These agencies are: The Department of Defense (DoD), the Department of Energy (DOE), the Director of National Intelligence (DNI), and Nuclear Regulatory Commission (NRC).

Cognizant Security Office (CSO): The organizational entity delegated by the head of a CSA to administer industrial security on behalf of the CSA.

Compilation: The concept also known as aggregation, which involves combining or associating individually, unclassified information which reveals an additional association or relationship that warrants protection as classified information. This concept also applies to elements of information classified at a lower level which become classified at a higher level when combined.

Compromise: An unauthorized disclosure of information.

Confidential: The classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

Contained in: The concept that refers to the process of extracting classified information as it is stated in an authorized source of classification guidance without the need for additional interpretation or analysis, and incorporating this information into a new document.

DD Form 254, Department of Defense Security Classification Specification: This form, including applicable attachments and supplements, provides classification guidance to prime and subcontractors performing on classified contracts. This form, as such, is an authorized classification source used by derivative classifiers. This form also informs contractors of the level of information they will need to access, the required level of security clearance for access, and the performance requirements to include safeguarding, special security requirements, etc.

Damage to the National Security: Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information.

Declassification: The authorized change in the status of information from classified information to unclassified information.

Derivative Classification: The process of determining whether information has already been originally classified and, if it has, ensuring that it continues to be identified as classified by marking or similar means when included in newly created material.

Derivative Classifier: The cleared individual responsible for ensuring that they apply the highest possible level of security classification when derivatively classifying information. These individuals bear the principal responsibility for the accuracy of the derivative classification.

DoDM 5200.01, Volumes 1-4, Department of Defense Information Security Program: The Regulation that implements Executive Order 13526, "Classified National Security Information," and associated OMB directives within the DoD. It applies to all Components of the DoD. It establishes the DoD Information Security Program to promote proper and effective classification, protection, and downgrading of official information requiring protection in the interest of the national security. It also promotes the declassification of information no longer requiring such protection.

DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM): The manual issued in accordance with the National Industrial Security Program (NISIP) that prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information.

Downgrading: A determination that information classified at a specific level shall be classified and safeguarded at a lower level.

Duration of Classification: A determination made by an original classifier, at the time of original classification, on the length of time information will require protection of security classification.

Extract: Taking information directly from an authorized source of classification guidance and stating it verbatim in a new or different document.

Facility Security Officer (FSO): A U.S. citizen employee, appointed by a contractor, who will supervise and direct security measures necessary for implementing the NISPOM and other Federal requirements for classified information.

Generate: Taking information from an authorized source of classification guidance and using it in another form or media.

Government Contracting Activity (GCA): An element of an agency designated by the agency head and delegated broad authority regarding acquisition functions.

Information: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

Information Security: The system of policies, procedures, and requirements established in accordance with Executive Order 13526 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security. The term also applies to policies, procedures, and requirements established to protect unclassified information that may be withheld from release to the public pursuant to Executive order, statute or regulation.

Marking: The principal means to inform holders of classified information about specific protection requirements for that information. Marking and designation of classified information are the specific responsibility of original and derivative classifiers.

Multiple Sources: Two or more source documents, classification guides, or a combination of both.

Need-to-Know (NTK): A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

National Security: The national defense or foreign relations of the United States.

Original Classification: An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

Original Classification Authority (OCA): An individual authorized in writing, either by the President, or by Agency Heads or other officials designated by the President, to originally classify information.

Paraphrase/Restate: Taking information from an authorized source of classification guidance and re-wording it in a new or different document.

Regrade: To raise or lower the classification assigned to an item of information.

Revealed by: The concept applied when derivative classifiers incorporate classified information from an authorized source of classification guidance into a new document, which is not clearly or explicitly stated in the source document.

Safeguarding: Measures and controls that are prescribed to protect classified information.

Secret: The classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to national security that the original classification is able to identify or describe.

Security Classification Guide (SCG): Also referred to as a Classification Guide. A document issued by an OCA that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element. A 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 the downgrading/duration of classification.

Source Document: An authorized source of classification used by a derivative classifier, from which information is extracted, paraphrased, restated, and/or generated in a new form for inclusion in another document.

Top Secret: The classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

Unauthorized disclosure: A communication or physical transfer of classified information to an unauthorized recipient.