n this tutorial we will discuss how a document becomes classified and who can do this. Please keep in mind that Small Business Innovation Research/Small Business Technology Transfer (SBIR/STTR) topics are not classified. Therefore, this information will be relevant only to a subset of small businesses whose work may eventually “go dark” or become classified.

There are three sources or categories of document classification referred to as Original classification, Derivative classification, and Contractor developed information. The original classification of any level for a document can only be made by a US Government official designated in writing as having the authority to do so. The National Industrial Security Program Operating Manual (NI-SPOM) states that, “A determination to originally classify information may be made only when (a) an original classification authority is classifying the information; (b) the information falls into one or more of the categories set forth in reference (b); (c) the unauthorized disclosure of the information, either by itself or in context with other information, reasonably could be expected to cause damage to the national security, which includes defense against transnational terrorism, that can be identified or described by the original classifier; and (d) the information is owned by, produced by or for, or is under the control of the U. S. Government.” (Department of Defense [DOD], 2006, p. 4-1-1)  

DERIVATIVE CLASSIFICATION

So where do you as a small business contractor fit into all of this? Since you are not a US government official with original classification authority, you fall into the category referred to as “Derivative Classification”. Derivative Classification is defined as, “the incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information.” (DOD, 2006, p. C-2)

According to the NISPOM, “Contractors who extract or summarize classified information, or who apply classification markings derived from a source document, or are directed by a classification guide or a Contract Security Classification Specification, are making derivative classification decisions.” (DOD, 2006, p. 4-1-1)

When this happens, the contractor employee that copied, extracted or translated the classified information from another document, must mark the new document or copy with the same classification markings as the original document. Also, if the employee has reason to believe the information is classified unnecessarily or improperly, they have the responsibility to challenge the classification.

USING PREVIOUSLY IDENTIFIED CLASSIFIED INFORMATION

There are situations in which you, as a contractor, may originate information that is of a classified nature and you must be prepared to deal with it properly. These situations occur when a contractor submits an unsolicited proposal to the government or generates information not in the performance of a classified contract. When this happens, the NISPOM states, “If the information was previously identified as classified, it shall be classified according to an appropriate Contract Security Classification Specification, classification guide, or source document, and marked as required by this Chapter. If the information was not previously classified, but the contractor believes the information may or should be classified, the contractor should protect the information as though classified at the appropriate level and submit it to the agency that has an interest in the subject matter for a classification determination.” (DOD, 2006, p. 4-1-2)

This situation also requires that you, the contractor, make the accompanying annotation at least once on the document(s) in a conspicuous location:

“CLASSIFICATION DETERMINATION PENDING Protect as though classified (TOP SECRET, SECRET, or CONFIDENTIAL).” (DOD, 2006, p. 4-1-2)

Because of its critical nature, the generation of TOP SECRET material produced by the contractor shall be made when the material is, “(1) completed as a finished document, (2) retained for more than 30 days after creation, regardless of the stage of development, or (3) transmitted outside the facility.” (DOD, 2006, p. 5-2-1)

CLASSIFIED WORKING PAPERS

Over the course of working on a classified government project or program, contractors will go through various stages of document development. As with any project, there will be working papers in the form of notes, drafts, etc. This NISPOM requires that, “Classified working papers generated by the contractor in the preparation of a finished document shall be: (1) dated when created, (2) marked with its overall classification and with the annotation “WORKING PAPERS”, and (3) destroyed when no longer needed. Working papers shall be marked in the same manner prescribed for a finished document at the same classification level when: (1) transmitted outside the facility, or (2) retained for more than 30 days from creation for TOP SECRET, or 180 days from creation for SECRET and CONFIDENTIAL material.” (DOD, 2006, p. 5-2-1)

MARKING REQUIREMENTS

Closely linked to the process of generating classified documents is the subject of marking requirements. Obviously, it is important to ensure that those who possess classified information are very aware of what level of protection is needed for those documents. Classified material must be clearly marked, showing the classification level, which sections are classified, the time period for classification, and any other annotations needed to protect the information.

In general, the rules for marking classified information apply to all forms of information and media. Some forms such as paper documents are easier than others to mark, but all require the following: Identification Markings, Overall Markings, Page Markings, Component Markings, Portion Markings, Subject and Title Markings, and Markings for Derivatively Classified Documents. All of these are discussed in detail in the NISPOM. Any questions regarding classified document generation, authorizations, and document marking procedures should be directed to your Facility Security Officer (FSO) and/or Industrial Security Representative (ISR).