Seven Step Plan of Action for Writing Classification Guides

JOB AID Source: DoD Manual 5200.45 Enclosure 2 Section 3

June 26, 2014

LEARN.
PERFORM.
PROTECT.

Center for Development of Security Excellence (CDSE) | 938 Elkridge Landing Rd | Linthicum, MD 21090

Introduction

The purpose of this job aid is to provide examples and scenarios associated with guidance found in DoD Manual 5200.45, "Instructions for Developing Security Classification Guides," April 2, 2013. The job aid describes processes and decisions an Original Classification Authority (OCA) must complete when creating a Security Classification Guide (SCG). DoD Manual 5200.45 refers to the process as a Seven Step Plan of Action.

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.

Step 1: Consider Related Current Guidance 3

Step 2: Determine State-of-the-Art Status 4

Step 3: Identify National Advantage 4

Step 4: Make Initial Classification Determinations 5

Step 5: Identify Specific Items of Information that Require Classification 6

Step 6: Determine to Duration of Classification 7

Step 7: Write the Guide 8

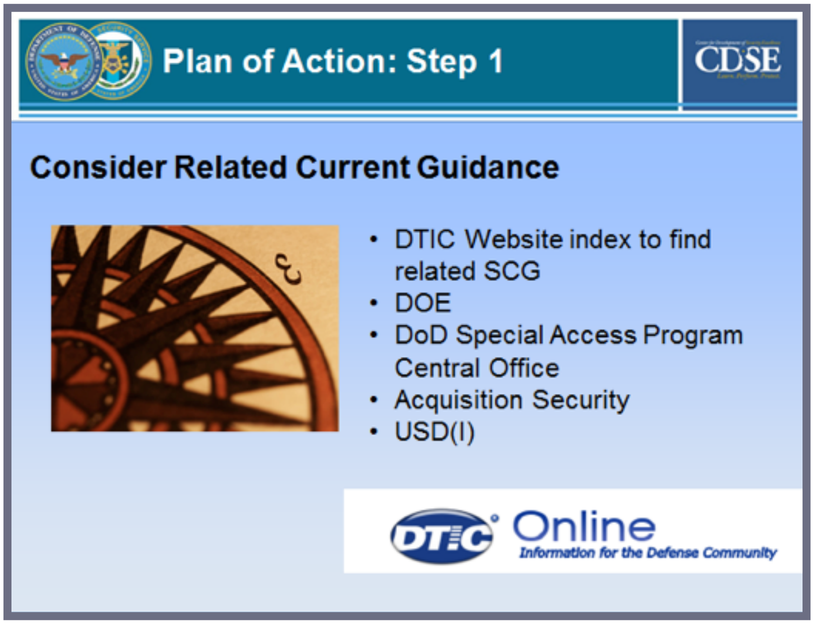
Acronyms and Abbreviations 10

Step 1: Consider Related Current Guidance

1. Determine if any classification guidance, to include umbrella guides, exists that is applicable to items of information concerning the system, plan, program, project, or mission.

   In some fields or subject areas, guides that apply to a broad spectrum of activities are sometimes referred to as umbrella guides. Since uniformity and consistency in exercising classification authority are paramount, the OCA must be aware of potential conflicts between the guide they are developing and any previously approved guides.

2. Next, begin searching for existing SCGs. The Defense Technical Information Center (DTIC) provides an online index of most SCGs issued within DoD.



Plan of Action: Step 1

CDSE

Consider Related Current Guidance

- DTIC Website index to find related SCG
- DOE
- DoD Special Access Program Central Office
- Acquisition Security
- USD(I)

DTIC Online Information for the Defense Community

   During the search for existing guides, the OCA may find other classification guides issued along functional lines by activities outside DoD that could have a bearing on the effort.

   The OCA may also want to consider the advice of those who have knowledge of classification in the subject area or in closely related fields.

   In addition, the local information security manager or information security specialist may be a valuable source of advice and assistance. Make efforts to exhaust all available resources during the construction of the SCG.

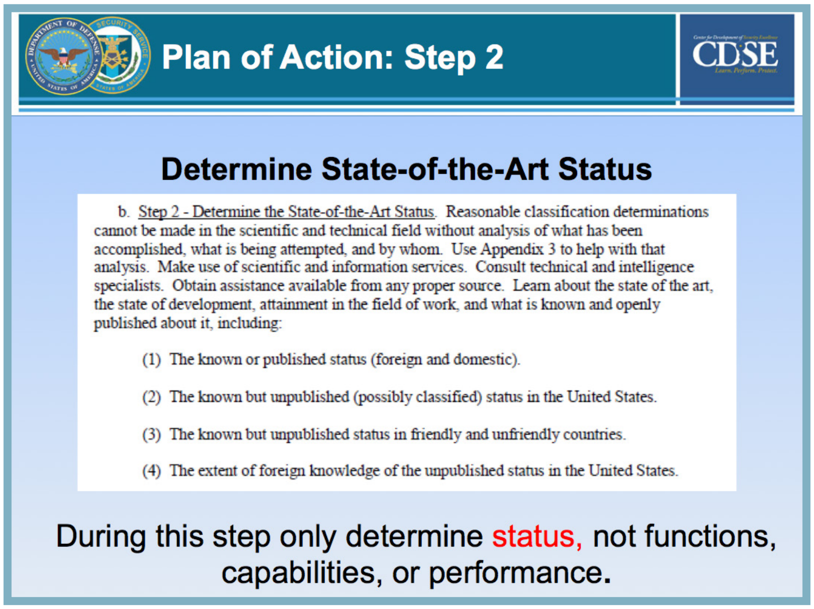
3. Finally, if potentially similar information is identified, the OCA must follow up as needed. This is done to determine information similarities or differences. If similarities are identified, the OCA has to ensure consistent, horizontal classification of the information.

   PLEASE NOTE: when there is a conflict in classification guidance between the guide the OCA is developing and a previously approved guide, there lies a risk of unauthorized disclosure. It is important to understand and resolve those differences and ensure the appropriate guidance is approved by the responsible OCAs.

   In cases where the data is similar but not the same, the OCA must include an explanation of the differences in the data and their classification levels within their guide. This ensures that users can clearly understand those differences and protect the information appropriately.

Step 2: Determine State-of-the-Art Status

An analysis of what has been accomplished, what is being attempted, and who attempted it is required in order to make a reasonable classification determination in the scientific and technical field.



Plan of Action: Step 2

CDSE

Determine State-of-the-Art Status

b. Step 2 - Determine the State-of-the-Art Status. Reasonable classification determinations cannot be made in the scientific and technical field without analysis of what has been accomplished, what is being attempted, and by whom. Use Appendix 3 to help with that analysis. Make use of scientific and information services. Consult technical and intelligence specialists. Obtain assistance available from any proper source. Learn about the state of the art, the state of development, attainment in the field of work, and what is known and openly published about it, including:

(1) The known or published status (foreign and domestic).

(2) The known but unpublished (possibly classified) status in the United States.

(3) The known but unpublished status in friendly and unfriendly countries.

(4) The extent of foreign knowledge of the unpublished status in the United States.

During this step only determine status, not functions, capabilities, or performance.

Other resources to consider are scientific and information services. Consult technical and intelligence specialists for this data.

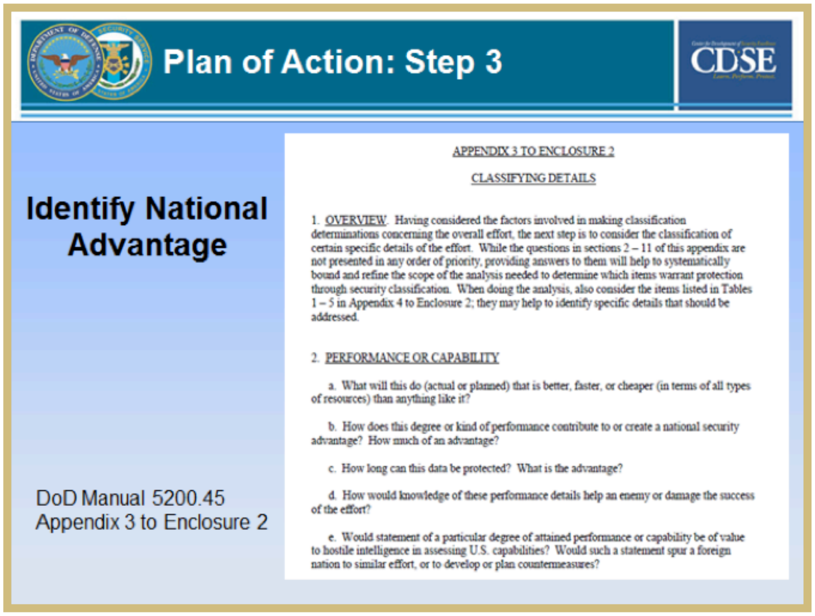
Also, take the time to learn about the state of the art, the state of development, attainment in the field of work, and what is known and openly published about it. Examples are shown to the left.

Step 3: Identify National Advantage

Some aspects of this step duplicate what has been done in Step 2 to determine state of the art status. The eleven categories in Appendix 3 of DoD Manual 5200.45 are also used as tools for identifying national advantage.

In order to successfully navigate through this step, the OCA should review the subject matter in its totality. The OCA needs to determine what the system, plan, program, project, or mission does or seeks to accomplish that will result in a net national advantage. Cover all the benefits including direct, indirect, accruing, or expected to accrue to the United States.

In the final analysis of this step, the decision to classify will be related to one or more of the eleven factors that produce, directly or indirectly, the actual or expected net national advantage.



Plan of Action: Step 3

CDSE

Identify National Advantage

DoD Manual 5200.45
Appendix 3 to Enclosure 2

APPENDIX 3 TO ENCLOSURE 2

CLASSIFYING DETAILS

1. OVERVIEW. Having considered the factors involved in making classification determinations concerning the overall effort, the next step is to consider the classification of certain specific details of the effort. While the questions in sections 2 – 11 of this appendix are not presented in any order of priority, providing answers to them will help to systematically bound and refine the scope of the analysis needed to determine which items warrant protection through security classification. When doing the analysis, also consider the items listed in Tables 1 – 5 in Appendix 4 to Enclosure 2; they may help to identify specific details that should be addressed.

2. PERFORMANCE OR CAPABILITY

a. What will this do (actual or planned) that is better, faster, or cheaper (in terms of all types of resources) than anything like it?

b. How does this degree or kind of performance contribute to or create a national security advantage? How much of an advantage?

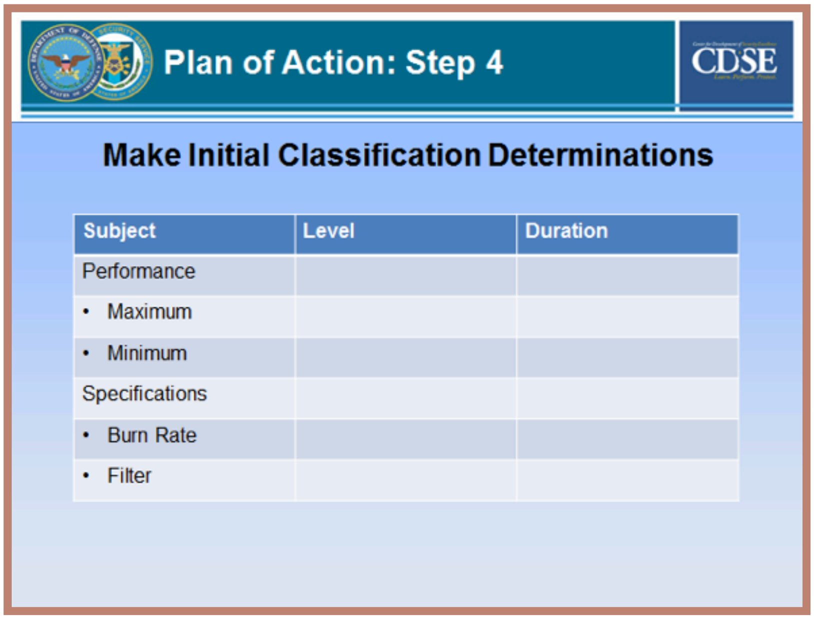
c. How long can this data be protected? What is the advantage?

d. How would knowledge of these performance details help an enemy or damage the success of the effort?

e. Would statement of a particular degree of attained performance or capability be of value to hostile intelligence in assessing U.S. capabilities? Would such a statement spur a foreign nation to similar effort, or to develop or plan countermeasures?

Step 4: Make Initial Classification Determinations

In Step 3, the OCA identified the net national advantage. In Step 4, the OCA identifies what requires classification to protect that advantage.



Plan of Action: Step 4

Make Initial Classification Determinations

Subject	Level	Duration
Performance		
• Maximum		
• Minimum		
Specifications		
• Burn Rate		
• Filter		

Although the focus is primarily on information relating to the overall effort at this stage of the SCG's preparation, consideration must be given to some of the specific information or data that covers performance capabilities. Possible vulnerabilities and weaknesses must also be considered. There are three distinct considerations:

1. First, the OCA should have some knowledge about the system, plan, program, project, or mission that needs protection before trying to identify specific items of information that require classification. How does the OCA compile this knowledge?

   He or she could use an engineering approach or group the information into large categories and then consider each category individually. This could possibly eliminate one or more categories from further consideration.

   He or she could also consider a work breakdown structure or system architecture to help identify the categories. Alternatively, after the large categories are identified, the OCA could repetitively break them into smaller and smaller pieces until specific elements of information are identified.

2. Second, the OCA should be aware that the information that needs protection may change as the system, plan, program, project, or mission progresses through its life-cycle.

   Basically, what needs to be classified in the early stages of the system, plan, program, project, or mission may differ from what requires classification in another life cycle phase. This would include system development, production, operations, or even execution.

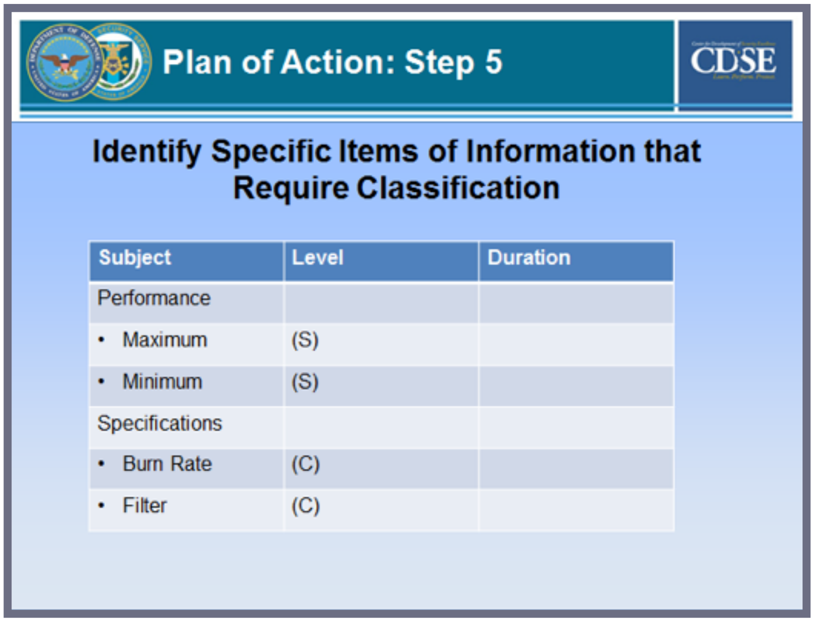
   The key thing to remember is to regularly reevaluate the SCG to determine which information requires, or still requires classification and update as appropriate. Periodically reviewing information to see if it can be downgraded or declassified can help reduce program security costs and can enhance information sharing.

3. Finally, once the OCA has identified the information that needs to be protected, he or she must remember to look at all the related processes (e.g., manufacturing, logistics, budgeting) to ensure the information is protected throughout execution of those processes. Some thoughts would be "Do the budget estimates need to be classified?" or "Does shipment of the end item to certain locations reveal classified data?" These are the types of questions that keep the OCA focused on the process for classification of the information.

Step 5: Identify Specific Items of Information that Require Classification

Step 5 requires four considerations.

1. First, the OCA must understand that the core of a classification guide is identifying the specific items or elements of information that require protection. Regardless of the size or complexity of the subject matter of the guide, or the classification level the guide is issued, there are certain identifiable features of the information that create or contribute to actual or expected national security advantage.



Plan of Action: Step 5

CDSE

Identify Specific Items of Information that Require Classification

Subject	Level	Duration
Performance		
• Maximum	(S)	
• Minimum	(S)	
Specifications		
• Burn Rate	(C)	
• Filter	(C)	

   There is also the possibility of certain items of information that have to be protected to prevent or make it more difficult for hostile forces to develop or apply timely and effective countermeasures.

   The challenge is to identify and state those special features or critical items of information, and decide how and why they are related to the net national advantage.

   The OCA must also ensure the statements and descriptions identifying the items of information to be classified are clear and specific enough to minimize the probability of error by the derivative classifiers who will use the SCG.

2. Second, when writing the SCG, the research, development, and acquisition projects and programs must consider critical program information (CPI). This is accomplished by ensuring proper protection of the elements or components that could cause significant degradation in the mission effectiveness, or could shorten the expected combat-effective life of the system, or even reduce technological advantage if compromised.

3. Third, the level of classification to be applied to each item of information identified in the guide must be specified precisely and clearly. Broad guidance like "Unclassified to Secret" does not provide sufficient instruction to users of the guide unless the exact circumstances under which each level of classification should be applied are defined. A better example is "Unclassified (U) when X is not revealed; Confidential (C) when X is revealed; or Secret (S) when X and Y are revealed."

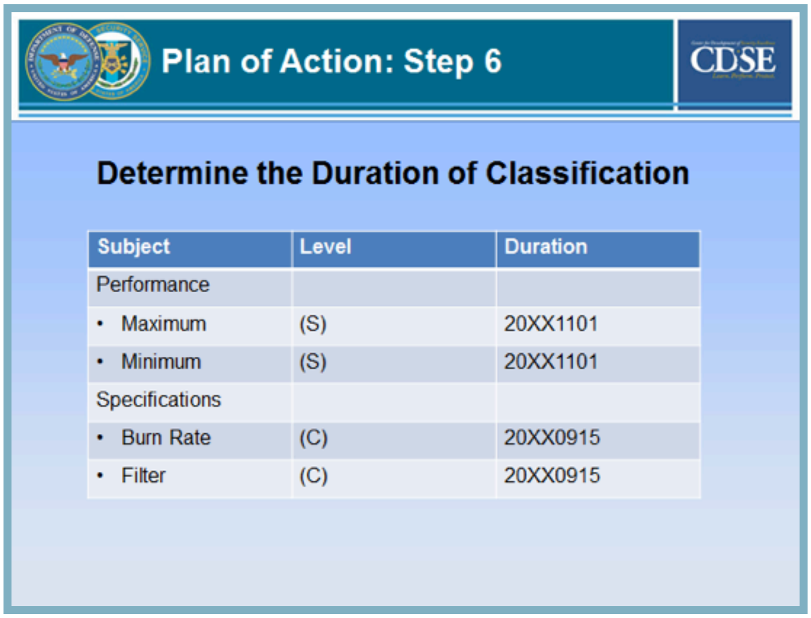
   If the OCA neglects to provide specific guidance, derivative classifiers will make their own interpretations that may or may not be consistent with the intent.

   The lack of guidance could lead to over or under classification of information. This impacts information sharing and can add additional cost to the security program or result in inadequate protection or unauthorized disclosure.

4. The last consideration concerns information that has been officially released to the public. It CANNOT be classified or reclassified, except in very limited cases. Note, however, this does not apply to unauthorized disclosures, such as leaks, because that information remains classified until it is declassified by the OCA.

Step 6: Determine to Duration of Classification

Executive Order 13526 stipulates that no information may remain classified indefinitely. Therefore, the decision on how long to classify is equally important to a determination to classify.



Plan of Action: Step 6

Determine the Duration of Classification

Subject	Level	Duration
Performance		
• Maximum	(S)	20XX1101
• Minimum	(S)	20XX1101
Specifications		
• Burn Rate	(C)	20XX0915
• Filter	(C)	20XX0915

Remember Restricted Data (RD) and Formerly Restricted Data (FRD) are not subject to automatic declassification, so no determination is required. These are factors that may influence the duration decision:

(a) Consideration that some information loses its sensitivity and importance in terms of creating or contributing to the national advantage over time. Therefore, information must constantly be evaluated to determine the need for continued classification.

(b) At certain stages in production or deployment, it may not be practical or possible to protect certain items of information from disclosure. It is also possible that design improvements may have eliminated exploitable vulnerabilities.

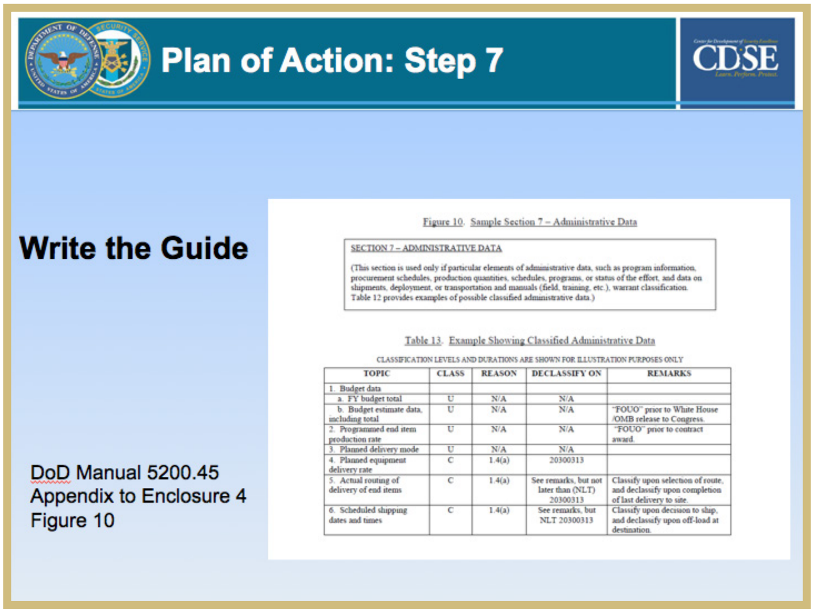
(c) Remember, once a decision is made to officially release information to the public, it CANNOT remain classified.

With these factors in mind, the OCA can proceed with the determination of the appropriate declassification instructions for each item of classified information.

The OCA also should always consider the possibility of providing downgrading instructions in every instance and even provide downgrading at fixed future points in time or upon a specified event occurring when the damage that is expected to be reduced to a lower classification level.

Step 7: Write the Guide

It is vital that the OCA use clear and precise language and statements to describe which items of information require classification.



Plan of Action: Step 7

Write the Guide

Figure 10. Sample Section 7 – Administrative Data

SECTION 7 – ADMINISTRATIVE DATA

(This section is used only if particular elements of administrative data, such as program information, procurement schedules, production quantities, schedules, programs, or status of the effort, and data on shipments, deployment, or transportation and manuals (field, training, etc.), warrant classification. Table 12 provides examples of possible classified administrative data.)

Table 13. Example Showing Classified Administrative Data

CLASSIFICATION LEVELS AND DURATIONS ARE SHOWN FOR ILLUSTRATION PURPOSES ONLY

TOPIC	CLASS	REASON	DECLASSIFY ON	REMARKS
1. Budget data				
a. FY budget total	U	N/A	N/A	
b. Budget estimate data, including total	U	N/A	N/A	"FOUO" prior to White House /OMB release to Congress.
2. Programmed end item production rate	U	N/A	N/A	"FOUO" prior to contract award.
3. Planned delivery mode	U	N/A	N/A	
4. Planned equipment delivery rate	C	1.4(a)	20300313	
5. Actual routing of delivery of end items	C	1.4(a)	See remarks, but not later than (NLT) 20300313	Classify upon selection of route, and declassify upon completion of last delivery to site.
6. Scheduled shipping dates and times	C	1.4(a)	See remarks, but NLT 20300313	Classify upon decision to ship, and declassify upon off-load at destination.

DoD Manual 5200.45
Appendix to Enclosure 4
Figure 10

While there is no mandatory DoD-wide format for SCGs, it is encouraged that the OCA considers using the recommended format described in Enclosure 4 of DoD Manual 5200.45. The format can vary for clarity or to best suit the needs of the system, plan program, project, or mission.

Only in exceptional cases are SCGs issued as documents within the Office of the Secretary of Defense, DoD Component policy, or regulatory structure. Typically, the issuing office coordinates the guide with other subject matter experts and potential users prior to approval by the OCA. This ensures timely updates of the SCG.

Administrative requirements:

(a) Place the most significant words of the SCG title first.

(b) Identify the OCA who personally approved the guide in writing and has program or supervisory responsibility over the information addressed in the guide as well as the office of primary responsibility (OPR) that can be contacted for clarification or additional information.

(c) Specify, clearly and concisely, the reason(s) for classification, the level of classification, and a declassification instruction(s) for each item to be classified. A table format is recommended for identifying this information as well as any downgrading instructions and other needed comments and instructions.

(d) Classify the guide if required by its contents. If the guide does not require classification, it must be marked and protected as FOR OFFICIAL USE ONLY (FOUO). SCGs shall NOT be released to the public.

OCAs must ensure that the SCG precisely states the specific information elements to be protected and uses clear, precise language or statements to describe which items of information require classification.

It is also advisable to include items that are designated as controlled unclassified information (CUI) or that are unclassified to assure derivative classifiers that information is in fact CUI or unclassified and was not inadvertently omitted.

The SCG must identify any additional dissemination control marking or special handling caveats such as RD, FRD, Releasable To (REL TO), or Not Releasable to Foreign Nationals (NOFORN), whichever applies to the elements of information.

The SCG must include amplifying comments whenever appropriate to explain the exact application of classification.

Finally, the OCA must provide any additional guidance required for effective use of the guide.

Acronyms and Abbreviations

C	Confidential
CDSE	Center for Development of Security Excellence
CPI	Critical Program Information
CUI	Controlled Unclassified Information
DoD	Department of Defense
DOE	Department of Energy
DTIC	Defense Technical Information Center
E.O.	Executive Order
FOUO	For Official Use Only
FRD	Formerly Restricted Data
NOFORN	Not Releasable to Foreign Nationals
OCA	Original Classification Authority
OPR	Office of Primary Responsibility
RD	Restricted Data
REL TO	Releasable To
S	Secret
SCG	Security Classification Guide
TS	Top Secret
U	Unclassified
USD(I)	Under Secretary of Defense for Intelligence

Center for Development of Security Excellence

CDSE

Learn. Perform. Protect.

Seven Step Plan of Action for Writing Classification Guides | JOB AID