# Classification Management Tutorial

# TABLE OF CONTENT

# Introduction

The purpose of this Classification Management tutorial is to provide detailed supplemental guidance to Original Classification Authorities (OCAs) for the development of United States (US) Army security classification guides (SCGs) or guidance.

Army Regulation (AR) 380-5, *Department of the Army Information Security Program*, implements the policies set forth in Executive Order 12958, as amended on 25 March 2003, *Classified National Security Information*, and Department of Defense (DoD) 5200.1-R, *Information Security Program*. It establishes the policies for security classification, downgrading, declassification, and safeguarding of information requiring protection in the interest of national security. Incorporated into AR 380-5 is DoD 5200.1-H, *Handbook for Writing Security Classification Guidance*, November 1999, which states that "timely issuance of comprehensive guidance regarding security classification of information concerning any system, plan, program, or project; the unauthorized disclosure of which reasonably could be expected to cause damage to the national security and that precise classification guidance is prerequisite to effective and efficient information security and assures that security resources are expended to protect only that which truly warrants protection in the interests of national security".

This tutorial serves to complement and further define the updated guidance to the above official issuances. It will assist security managers and OCAs in orchestrating the drafting of tailored, user friendly SCGs through the use of a standard methodology and a series of tools. This methodology and accompanying tools will facilitate the achievement of sound, objective security classification decisions and ensure consistency in the quality of SCGs throughout the US Army. At the end of the tutorial, you will be able to do the following:

- Understand the roles and responsibilities of OCAs and their relationship to SCGs
- Apply the ten-step process in developing SCGs
- Employ the standardized classification management tools to assist in determining correct security classification levels
- Develop tailored, user friendly SCGs

## Army Research and Technology Protection Center

# Security Classification Management Tutorial

**Background**

Department of Defense (DoD) 5200.1-R, *Information Security Program* and Army Regulation (AR) 380-5, *Department of the Army Information Security Program* provide for the issuance of a security classification guide (SCG) for each system, plan, program, or project involving classified information. Executive Order (E.O.) 12958, as amended (25 March 2003), *Classified National Security Information* (henceforth referred to as E.O. 12958), addresses the need for SCGs in terms of proper classification of information and uniform derivative classification of information. Specific classification guidance is necessary for effective information security and is instrumental in the allocation of resources for protecting only those items that affect national security. An SCG is the written record of original classification decisions or a series of decisions regarding a system, plan, program, or project.

Specific and detailed guidance is required when identifying information that must be classified. This ensures that information is not over classified or under classified, but classified at the appropriate level. Over classification is costly, inefficient and can cause slow downs to development/operation. Under classification can cause compromise, inadvertent disclosures and confusion. In addition to proper identification of items to be classified, it is equally important to identify the length of time that the information should remain classified.

The decision to classify information is based upon the determination and ability to describe damage to national security if the unauthorized disclosure of the information occurs. Persons having specifically been authorized to make this determination and having received training in this area are the only individuals who may make this decision. These individuals are designated as having Original Classification Authority (OCA) in accordance with the E.O.12958, DoD 5200.1-R and AR 380-5.

Security classification guidance should be issued as early as possible in the life cycle development of a system, plan, program, or project to ensure initial protection and to avoid compromise. An understanding of classification, declassification/downgrading, marking, and the intent of the security classification guide itself is vital to the proper drafting of an SCG.

Every attempt should be made to publish the SCG in an unclassified form. To avoid classifying the SCG, consider the use of classified supplements. This is especially useful when dealing with Special Access Required (SAR) aspects of a program. Care

should also be taken to ensure that the descriptions of classified systems, subsystems and components in the guide do not inadvertently disclose classified or technical controlled unclassified information. Lastly, SCGs should be portion marked, marked with the identity of the classifier, and provide declassification/downgrade instructions.

**Classification Management Working Group (CMWG)**

The process for the development of SCGs is mentally challenging, tedious and labor intensive. It cannot be done in a vacuum by a few individuals. It is recommended that a CMWG be established to develop the guide. The group should meet as often as necessary and work towards established milestones. When establishing the CMWG, consider functional specialists, who should be included in the process. At a minimum, participants must include representation from the following functional areas: security, counterintelligence, Program/Product Manager, operators, engineers, and logistics. There may be others who are affected by the program, system or subsystem; and they should be considered for inclusion in the group.

In preparation for an SCG development event, members of the CMWG must conduct background reviews of applicable issuances, such as AR 380-5 and SCGs from equivalent programs within the U.S. Government.

Some key points to remember in developing an SCG are that guidance must be clear and specific (e.g., stating exact circumstances for which the level of classification should be applied), and the guide must be written with the user's perspective in mind.

**Documenting the Process**

While developing the SCG, it is strongly recommended that a record of the process be documented. The record should be a compendium to the SCG that captures the rationale for the security classification decisions. This compendium will provide clarity and reduce the number of challenges to the SCG.

**Exercise Questions:**

1. What DoD/US Army issuances stipulate the requirement for security classification guides?

a. DoDD 5200.39 and AR 360-1
b. DoD 5200.1-R and AR 380-5
c. DoDD 5000.1 and AR 380-10
d. DoDD 12359 and 350-1
e. None of the above

2. What Executive Order (E.O.) addresses the need for security classification guides in terms of proper classification, uniform derivative classification of information and original classification authority?

a. E.O. 12333
b. E.O. 12958
c. E.O. 12498

3. Classification guidance should be issued _____ in the life cycle development of a system, plan, program or project to ensure initial protection and to avoid compromise.

4. All security classification guides should be classified.

TRUE or FALSE

5. Security classification guides should be developed solely by the Security Manager.

TRUE or FALSE

6. It is recommended that a Classification Management Working Group be established to address the development of the security classification guide.

TRUE or FALSE

7. Some key points to remember in the security classification guide development process:

Guidance must be _____ and _____ and the guide must be written with the _____ perspective in mind.

8. The record of the development process of a security classification guide is called a(n):

a. Concept of operations
b. Operations order
c. Compendium
d. None of the above

9. The compendium captures _____ for security classification _____.

10. The compendium could provide _____ and reduce classification _____ to the security classification guide.

**Exercise Answers:**

1. b (p.1)
2. b (p.1)
3. as early as possible (p.1)
4. False (p.1)
5. False (p.2)
6. True (p.2)
7. clear, specific, user (p.2)
8. c (p.2)
9. rationale, decisions (p.2)
10. clarity, challenges (p.2)

## Security Classification Guide (SCG) Format

There are two parts to an SCG, *General Instructions* and *Elements Table*. Several paragraphs comprise the *General Instructions* or "front section" of the SCG. Usually, this section contains the following paragraphs:

***1. Purpose***
State the name of the program, project, etc. and provide instructions and guidance for determining information at the classified and unclassified levels.

***2. Authority***
Provide the issuing authority by identifying the applicable Army regulation that governs or controls the issuance of SCGs, specifically AR 380-5, *Department of the Army Information Security Program*, dated 29 September 2000. Identify the project information involved and the controlling office. Cite any other SCG or security classification guidance document that deals with the information. State that the SCG provides authority to cite as classification, declassification or downgrading authority only in this particular endeavor. If there are any changes to security classification by applying this SCG, they are to be made immediately. Finally, although E.O. 12958 states that each delegation of OCA will identify the official by name or position title, the Army process calls for the provision of the position title of the OCA, who has been granted the authority for a specific level of security classification of the information in the first instance.

***3. Office of Primary Responsibility (OPR)***
Provide the name, code and mailing address of the issuing office as the issuance authority, so that all inquiries, interpretations and/or recommendations for changes regarding the content of the SCG may be addressed. Include action officer's phone number, fax number and e-mail address, whenever possible.

***4. Classification Challenges***
Provide guidance for classification challenges. State the organization to which all challenges will be submitted. Further indicate that, until a determination is made to the challenge, the information must be protected at the current security classification level.

***5. Reproduction, Extraction and Dissemination***
Provide instructions regarding the authority to reproduce, extract and/or disseminate the SCG, as necessary to those organizations that support the effort (including industry). If there are additional guides associated with the program, those SCGs or security classification guidance documents should be sent to the OPR for dissemination. If a guide is classified, delineate any limitations or conditions.

***6. Public Release***
Clarify that unclassified information reflected in the SCG does not automatically indicate that the information is approved for public release. Provide the organizational address where requests for public release of program information should be submitted.

***7. Foreign Disclosure***
Cite AR 380-10, *Foreign Disclosure and Contacts with Foreign Representatives*, 22 June 2005, as the governing issuance for foreign disclosure. Provide instructions on the procedures for handling foreign disclosure issues within an organization.

***8. Foreign Sales***
Cite AR 12-8, *Operations and Procedures*, 21 December 1990, as the governing issuance for security assistance programs. Provide information regarding the highest security classification level of information and/or materiel that should be disclosed and transferred in conjunction with any end item sale of the system through foreign military sales channels.

***9. Definitions***
Provide a list of applicable terms of reference for clarity and understanding by the user. Include a table of acronyms and or abbreviations that will be used throughout the SCG. Explain each one.

**Exercise Questions:**

1. How many parts are there in an SCG?

2. What Army regulation governs or controls the issuance of SCGs?

3. Information is being leveraged from another program. It is not necessary to cite the applicable SCG from that leveraged program.

   TRUE or FALSE

4. A classification challenge has been made to the appropriate organization concerning the security classification of specific information. Until the determination is made to the challenge, the information must be protected at the _____ security classification level.

**Exercise Answers:**

1. 2 (p.6)
2. AR 380-5 (p.6)
3. False (p.6)
4. current (p.6)

## SCG Table Preparation

When building the *Elements Table* of an SCG, four (4) columns are recommended:

| Element | Classification | Declassify/Downgrade | Remarks |
|---|---|---|---|

When developing an SCG, it is recommended that the Remarks column be used for clarification. Experience has clearly demonstrated that notes become lengthy, confusing and cumbersome for the user. The user frequently fails to refer to them since they are not part of the table, resulting in inconsistencies in security classification. Furthermore, notes are not prioritized leaving the user to decide which specific note has predominance, creating additional inconsistencies in security classification levels. The criteria that are applied to the selection of the security classification level of the information should be explained in the Remarks section (such as the loss of information that would compromise a future capability; see page 23).

There are ten basic steps in the preparation of an SCG *Elements Table*. The key to drafting an effective SCG is to focus on the table. Seldom does an individual (such as an engineer, test and evaluation personnel, operator, or maintenance person), who requires security classification guidance for a particular situation, read the "front section". This is generally referenced by the security staff. The ten-step process is as follows:

1. Build the Elements column with key information provided by program experts and equivalent SCGs, if available, and/or specialized documents, such as a work breakdown structure.
2. Validate Elements column and add clarity, if necessary, in the Remarks column.
3. Determine eligibility of Elements to be classified (Figure 1, pg. 13) and mark Elements included in the guide that do not warrant security classification as "Unclassified".
4. Review those Elements eligible for security classification against the Level of Classification Determination Tool (Figure 2, pg. 23)
5. Record results of the security classification level determination and clarify in Remarks section, if necessary.
6. Use the Declassification/Downgrade Tool for each Element to determine the length of time that the Element should be classified. Attempt to apply specificity in time or by using an event (Figure 3, pg. 39).
7. Record results and clarify, if necessary, in the Remarks column.
8. Those Elements that are not classified at the CONFIDENTIAL(C), SECRET(S), or TOP SECRET (TS) level are to be marked UNCLASSIFIED (U) in the Classification column.
9. Review each Element with a minimum marking of U and determine potential for FOR OFFICIAL USE ONLY (FOUO) handling (Figure 1, pg. 13).
10. Record results and document in the Remarks column.

## Step 1 – Develop the Element Column

This step is a true brainstorming effort. Members of the CMWG should consider for inclusion as possible elements those items they consider being of interest to the program and users. As such, a program name should be included even if it is unclassified. Again, the goal is to provide specific and clear guidance for those items (general or technical) that may be referenced by users.

For example, the Elements column for an acquisition program SCG should include all information associated with the program, such as: Administrative Information, Requirements, Hardware/Software, Capabilities/Performance, Vulnerabilities/ Limitations, Testing/Evaluation, Training, and Maintenance, or an operational project, such as Tactics, Techniques, and Procedures. It should be noted that this methodology eliminates the "Critical Elements" section of the SCG, which is redundant to other portions of this guide, runs counter to the need-to-know principle, and, if compromised, provides an adversary with leads to the critical aspects of any program. Within each of these headings (e.g., HARDWARE), clarifying details should be included, such as "Fact of", "General details of", and "Technical details of". It is strongly recommended that any discussion/decision making process be incorporated into the compendium.

When developing items for inclusion in the Elements column, consideration should be given to the concept of *classification by compilation*. This is important when considering the implementation of the security classification guidance. If a user is considering more than one unclassified piece of information and compiles them, the sum total of the information may be eligible for classification. For example, suppose deployment dates are classified CONFIDENTIAL. However, if an adversary is watching a base to obtain information and notices increased supply activities, several florist deliveries and large numbers of military members coming to the base at the same time, one may conclude that a deployment is imminent. Individually, each piece of information is treated as unclassified; however, when reviewed in its totality, the end product or conclusion may be classified since it could reveal deployment dates. With this scenario in mind, the CMWG should ensure that guidance reflects the "effect" of disclosure, so the user can identify the "cause" – compilation when it occurs. An example of an Elements column is as follows:

| **2.0 REQUIREMENTS** |
|---|
| 2.0.1 General information regarding requirements for the *program name* |
| 2.0.2 Specific technical requirements associated with a specific system, subsystem or component |
| 2.0.3 Identification of key performance threshold/objective parameters associated with the *program name* a specific system, subsystem or |

| |
|---|
| component |
| **3.0 HARDWARE/SOFTWARE** |
| **3.1 Technology Integration** |
| 3.1.1 General description of technologies being considered for use in the *program name* |
| 3.1.2 Specific technical details of technologies being considered for use in a specific system, subsystem, or component |

## Step 2 – Validating the Elements

During the Elements validation process, ask the questions who, what, why, where, when, and how. This process will confirm the requirement for each element in the table. Look for examples and discuss in terms of tangible data that provide the specificity required by the user. If necessary, add clarifying comments in the Remarks column, and amplifying details to the compendium.

## Step 3 -Determine Eligibility of Elements for Classification

The CMWG should use the Eligibility Determination Tool (Figure 1) to determine if the Element is eligible to be classified. It is important to take each Element through the entire tool to establish that the originator is the owner of the information to be classified for the first time, or to establish that the information is derivative or being leveraged from another program or source. If the information does not belong to the program using it, that fact must be identified in the SCG and reference made to the appropriate OCA or owner. Following these steps may appear unnecessary; however, after using the tool, it will become clear that all of the questions must be answered each and every time to establish if the information is owned by the current program. The thoroughness in the implementation of this process will help when using the next tool in the series. Any discussion items should be recorded in the compendium for future reference.

# Eligibility Determination Tool (Figure 1)

Classification management is predicated on protection/management of that critical and sensitive items/information. Results of the output of the criticality/sensitivity tool should lead you here. This tool should be completed before proceeding to the Classification Level Tool.

**Eligibility**

A. Is the information already classified in another US Army program or by another Military Department? (Note:-Request G-2 support to ascertain)

☐ No
☐ Yes (go to that Security Classification Guide or Military Department for derivative classification)
(See page 16 for amplification)

B. Is the information eligible for classification? (Information may be classified **only if** questions 1, 2 and at least one part of 3 is ***yes***)

1. Is the information being submitted to an original classification authority (OCA) for inclusion in a security classification guide (SCG)?
   ☐ No
   ☐ Yes
   (See page 16 for amplification)
2. Is the information official (owned by, produced for or under the control of the US Government)?
   ☐ No
   ☐ Yes
   (See page 16 for amplification)
3. Within Classification Management Regulations (E.O. 12958, as amended, DoD 5200.1-R, AR 380-5, etc.), does the information fall within one or more of the categories listed below and could it be expected to result in damage to national security including defense against transnational terrorism? (check all that apply)

   a. military plans, weapons systems, operations
      ☐ No
      ☐ Yes

   b. foreign government information – Refer to Program Manager (PM), Program Security Manager (PSM)/Contract Security Manager (CSM)
      ☐ No

☐ Yes

c. intelligence activities, intelligence sources or methods, or cryptology – (Note: Refer to G-2 to ascertain if these activities, sources, or methods are involved)
☐ No
☐ Yes

d. foreign relations or foreign activities of the US including confidential sources – Note: Refer to PM and if necessary G-2 to ascertain)
☐ No
☐ Yes

e. Information within one of the following categories relative to national security including defense against transnational terrorism

1. scientific
☐ No
☐ Yes

2. technological
☐ No
☐ Yes

3. economic
☐ No
☐ Yes

- resources–Refer to PSM/CSM for amplifying details, e.g., numbers of persons, MOS of persons, trained, and readiness.
☐ No
☐ Yes
- budget – Refer to PSM/CSM for amplifying details
☐ No
☐ Yes

- sensitive contractual relationships or contractual relationships with foreign governments, including wholly owned subsidiaries, (should have “yes for item 3.b and item 3.d) – Refer to PSM/CSM to ascertain
  ☐ No
  ☐ Yes Refer to PSM/CSM

f. U.S. government programs for safeguarding nuclear materials or facilities – Note: Refer to PSM/CSM to ascertain)
  ☐ No
  ☐ Yes

g. Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to national security including defense against transnational terrorism.
  ☐ No explain
  ☐ Yes

h. Weapons of mass destruction
  ☐ No
  ☐ Yes

**Information items deemed eligible for classification should be migrated to the Level of Classification Determination Tool

**Extrapolation of Items in Eligibility Determination Tool.**

***Is the information already classified by another Original Classification Authority?***
If the information has been previously classified and is being leveraged from another program, then an SCG should exist and the security classification becomes derivative. This is consistent with the "original" in OCA. If the OCA signing the SCG is not the classification authority for the items in either of these categories, then the OCA of the SCG being developed cannot "originally" classify them.

CMWGs should immediately enter in the Classification column for information determined to be derivative the phrase "See Remarks" and in the Remarks column the entry "See XXX SCG, See Program Security Manager, "See Operational Requirements Documents", or "See Capabilities Development Document (CDD)". The XXX SCG and specific documents are direct references to the origin of the derivative information. The "See Program Security Manager" phrase is often used when exercising the need-to-know principle relative to the specific source for the derivation. Examples of such sources include classified, Sensitive Compartmented Information or Special Access Program SCGs.

***Is the information being submitted to an OCA for inclusion in an SCG?***
The answer to this question appears to be simple and straightforward since we are now in the third step of the process of developing an SCG to be submitted for OCA signature. However, the CMWG should consider the following: Does the OCA have cognizance over the information, program, plan, project, or system being proposed for classification? This is similar to the first question regarding derivative information, but also considers factors such as linkage to the program. There have been cases where an SCG was signed by an OCA, who had no affiliation with the program except for geographic proximity. This could mean that all disclosure issues revert to an OCA that may have no insight into the program – not an ideal situation. Does the OCA have proper authority in writing, and is the OCA able to articulate the damage to national security if the information being classified is compromised or subject to an unauthorized disclosure or being challenged regarding the security classification level determination? The list of Army OCAs is limited. CMWGs should always check with HQDA, G-2 (DAMI-CDS) if they are uncertain if the proposed signatory of the SCG is an approved OCA.

***Is the information official (owned by, produced for or by, or under the control of the U.S. Government (USG))?***
It must be established that the information is owned by, produced by or for, or is under the control of the USG. When a U.S. contractor voluntarily introduces "company proprietary" information into a USG program, the U.S. contractor is effectively placing that data under the control of the USG. In this case, that information is subject to the provisions of the program SCG. This point is very important since CMWGs are often confronted with the claim that proprietary data means that type of information cannot be classified, and that claim is incorrect.

**Examples:**

1. Jack Spade, the Security Manager for the COSMIC Program, is conducting a combined security classification orientation and training session for the newly-established Classification Management Working Group. In explaining the eligibility of elements to be classified under a security classification guide (SCG), Mr. Spade emphasized two key points:

a. First, identify all basic elements that will constitute the system and program, regardless of the origins of the information, technologies, components, subsystems, or systems.

b. Second, once all of the basic elements of the system and program have been identified, then the group should review whether any of the elements have already been classified in the first instance by another original classification authority. By doing so, the group will automatically eliminate those elements from original classification under the COSMIC SCG.

2. MAJOR Jay Olsen, US Army Training and Doctrine Command (TRADOC) point of contact for Army concepts and doctrine (to include tactics, techniques and procedures (TTPs)) elicits the assistance of the command Security Manager to develop security classification guidance involving counter-improvised explosive device (C-IED) TTPs. In reviewing the requirements outlined by MAJ Olsen, the Security Manager recommended convening a working group to determine whether background references were available to assist the group in identifying elements for the requested guidance, such as concepts and doctrine regarding convoy operations currently being taught at any TRADOC schools. The collection of such documents would assist in identifying the applicable elements for this C-IED guidance and then tailoring the elements for such a security classification guide.

**Exercise Questions:**

1. Executive Order 12958, as amended, states that each delegation of original classification authority shall identify the official by name or position title. From an Army perspective, the optimum method for identification is by:

a. Name of the Official

b. Position Title of the Official

c. Both Name and Position Title of the Official

2. In developing an attack helicopter system for the Army and in keeping with Department of Defense acquisition policy that advocates compressing the length of time required to field a weapon system, the Program Manager instructed the prime contractor to leverage readily available technologies, components, subsystems, and/or systems to achieve the primary goal in defense acquisition. Should all leveraged technologies, components, subsystems, and/or systems be included as elements in the attack helicopter security classification guide?

a. Yes

b. No

3. If official information is owned by, produced for or by, or under the control of an original classification authority (OCA) and the compromise of it will damage national security, does it automatically constitute eligibility to classify originally under a security classification guide of that OCA?

a. Yes

b. No

4. In negotiating a program security instruction for an international cooperative development program, representatives from Country X opined that the US security classification guide (USG) should be used as the base guidance for the arrangement and their information would just be added to and addressed in the document. Since all information and materials provided to the US by Country X will be appropriately marked in terms of security classification and handling instructions, the US side opined that those elements should not be included in the US SCG. Is the US position prudent in terms of the eligibility of elements in the guide?

a. Yes

b. No

5. While it is acknowledged that the Classification Management Working Group is the preferred and optimum venue for the development of security classification guides (SCGs), in an emergency, a Security Manager can independently draft an effective guide by copying an equivalent or a series of similar SCGs.

a Yes

b No

6. In developing the sections of the security classification guide (SCG), there has been a penchant for specifying a “Critical Elements” section. The current methodology eliminates this section. What factor(s) contribute to the rationale for eliminating this section from the SCG?

a. Redundancy in terms of other parts of the guide.

b. Lead an adversary to target the most important information regarding the system if the document is compromised.

c. Need-to-know principle.

d. All of the above.

7. Can proprietary, patent or copyright data be eligible elements of a security classification guide?

a. Yes

b. No

8. Under the applicable classification standards listed in Executive Order 12958, as amended, the following eligible “Elements” conditions apply:

a. Information is being classified by an original classification authority.

b. Information is owned by, produced by or for, or is under the control of the United States Government.

c. Information falls within military plans, weapons systems, or operations; intelligence activities; scientific, technological, or economic matters; or vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security.

□ TRUE or FALSE

9. Compilation of information is not an eligible element in a security classification guide, particularly the combining of data from two or more systems.

□ TRUE or FALSE

10. Are commercial off-the-shelf products that are acquired for a system eligible elements for inclusion into a security classification guide?

a. Yes

b. No

**Exercise Answers:**

| | | |
|---|---|---|
| 1. | b | (p. 6) |
| 2. | a | (p. 13) |
| 3. | a | (p. 13) |
| 4. | b | (p. 13) |
| 5. | b | (pp. 2, 11) |
| 6. | d | (p. 11) |
| 7. | a | (pp. 13, 17) |
| 8. | TRUE | (p. 13-15) |
| 9. | FALSE | (p. 11) |
| 10. | a | (p. 13) |

## Step 4 - Level of Classification

The Level of Classification Tool was developed to assist OCAs and Security Managers in making consistent classification decisions. Guidance that has been provided in directives and regulations is broad and not clearly defined, so that the interpretation of the guidelines for the determination of security classification is purely subjective. This tool facilitates the necessary dialogue within the CMWG and increases objectivity when determining the appropriate classification level for each element. Additionally, the application of the tool provides the OCA with detailed rationale for each security classification decision.

The CMWG should take each Element through the entire Level of Classification Determination Tool, beginning with CONFIDENTIAL and ending with UNCLASSIFIED. It is designed to work through each level even after the criteria for a previous level was met. What meets the CONFIDENTIAL criteria may also meet the SECRET or TOP SECRET criteria. The highest level of security classification is always selected.

The Army Research and Technology Protection Center (ARTPC) developed criteria to discriminate between and among the definitions of the three levels of security classification that have been established by E.O. 12958. In addition, the criteria will assist the users of the SCGs in arriving at the proper level of security classification for each element in the guide. Use of these criteria will contribute to the standardization of SCGs throughout the U.S. Army.

Information that does not meet the criteria for security classification either individually or by compilation is deemed to be unclassified. However, information deemed to be unclassified does not mean that it is automatically releasable to the public. Before unclassified information can be officially deemed “Public Release”, a competent authority, specifically the Public Affairs Officer, must review and determine that the information is releasable to the public. The provisions of AR 360-1, *The Army Public Affairs Program*, apply. Additionally, information may be exempt from public release under certain statutes, regulations or policies (such as the Arms Export Control Act, International Traffic in Arms Regulation, Freedom of Information Act, Privacy Act, or Export Administration Act). It is important for the CMWG to remember that “Public Release” publications will normally be assigned the “Distribution Statement A” marking in accordance with AR 380-5.

## Level of Classification Determination Tool
## (Figure 2)

Using the results of the Eligibility Determination Tool, this next tool assists in determining the level of security classification assigned to each element as part of the development of the SCG. According to E.O. 12958, as amended, security classification is related to ”damage to national security” which means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information. There are three levels of classification defined in terms of level of damage -- CONFIDENTIAL, SECRET and TOP SECRET.

** Compilation of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that: 1) meets the standards for classification; and 2) is not otherwise revealed in the individual items of information. The aggregate information will be classified at the appropriate level to prevent compromise until an analysis of the aggregate can be accomplished and validated by the OCA.

1. **CONFIDENTIAL**: compromise or inadvertent release of the information would result in “damage” to national security.

When applying the tool to each eligible element, ask the CMWG if any of the criteria listed below applies.

- loss of *low level* intelligence collection capability or revelation that the US has or is capable of obtaining specific *low level* foreign information or material result in damage to national security.
- loss of information that could threaten the international position of the U.S
- loss of information that could *threaten* the country’s ability to wage war
- loss of information that would reveal details of how we plan to achieve a national security objective or intention
- loss of information that would compromise a current or a future capability

For amplification of the terms used in the criteria, see pages 27 - 30.
If the answer is yes to at least one statement above, consider for **CONFIDENTIAL** classification.
If the answer is yes to more than one statement, consider the possibility of classifying all of the information **SECRET** by the combined effect of the applicability of more than one criterion selected.
If the answer is not yes to any of the above statements, go to **SECRET**.

2. **SECRET**: compromise or inadvertent release of the information would result in "serious damage" to national security.

When applying the tool to each eligible element, ask the CMWG if any of the criteria listed below applies.

- significant impairment to the flow of *sensitive* information to national policy makers and cause serious damage to national security
- loss of *sensitive* intelligence collection capabilities or revelation that the US has or is capable of obtaining *sensitive* foreign information or material
- loss of research, development and engineering, scientific or technical information that would compromise a state of the art capability or negate the operational effectiveness of the system
- loss of operational, intelligence or battlefield information lead to a *tactical* disadvantage
- loss of information that would *weaken* the international position of the US
- loss of information that would *weaken* the country's ability to wage war
- loss of information that would limit the effectiveness of forces
- loss of information that would render the US vulnerable to a terrorist attack
- denial, degradation, disruption, deception, or destruction of mission *essential* system(s)
- major modifications to an acquisition program or operational system to maintain the *tactical* advantage of the system during its projected operational life time

If the answer is yes to at least one statement above, consider for **SECRET** classification.
If the answer is yes to more than one statement, consider the possibility of classifying all of the information **TOP SECRET** by the combined effect of the applicability of more than one criterion selected.
If the answer is not yes to any of the above statements, go to **TOP SECRET**.

3. **TOP SECRET**: compromise or inadvertent release of the information would result in *"exceptionally grave damage"* to national security.

When applying the tool to each eligible element, ask the CMWG if any of the criteria listed below applies.

- significant impairment to the flow of *critical* information to national policy makers cause exceptionally grave damage to national security
- loss of *unique* and *fragile* intelligence collection capabilities or revelation that the US has, or is capable of obtaining *critical* foreign information or material
- loss of research, development and engineering; scientific, technical, operational, intelligence or battlefield information that would lead to a *strategic* disadvantage
- loss of information that would *significantly weaken* the international position of the US
- loss of information that would *significantly weaken* the country's ability to wage war
- loss of information would limit the effectiveness of major forces
- loss of information would render the US senior leadership vulnerable to a terrorist attack
- denial, degradation, disruption, deception, or destruction of mission *critical* system(s)
- major modifications to an acquisition program or operational system to maintain the *strategic* advantage of the system during its projected operational lifetime

If the answer is yes to at least one statement, consider for **TOP SECRET** classification. If the answer is not yes to any of the above statements, go to **UNCLASSIFIED**.

**Unclassified information** is all information that is not classified. It is divided into two categories, public domain and controlled unclassified information (CUI). Public domain is unclassified information that has been identified according to the provision of AR 360-1. The definition of CUI is as follows:

> **Controlled Unclassified Information (CUI)**: other types of information that require application of controls and protective measures, for a variety of reasons, not to include those that qualify for formal classification.
>
> - Sensitive Information: information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interests or the conduct of Federal programs or the privacy that individuals that are entitled under 5 USC. Section 552a but that has not been specifically authorized under criteria established by an E.O. or an act of Congress to be kept secret in the interest of national defense of foreign policy. Subcategories:

- Privacy Act: all information covered by the Privacy Act including medical, pay, and personnel information. Information may be classified or unclassified.
- Financially Sensitive: Financially and contractually sensitive information. Information may be classified or unclassified.
- Proprietary: Information provided by a source or sources under the condition that it not be released to other sources.
- Administrative/Other: DoD information associated with housekeeping activities, information marked For Official Use Only, and unclassified information that does not fall into any of the other info categories.

*Consider using special handling caveats or instruction including company proprietary*

FOR OFFICIAL USE ONLY (FOUO): applies to unclassified information that is exempt from mandatory release to the public under Freedom of Information Act (FOIA) and may be used for protecting a variety of information.

FOIA exemptions:

- X1 Information that is currently and properly classified.
- X2 Information that pertains solely to the internal rules and practices of the agency. This exemption has two profiles, “high” and “low”. The “high” profile permits withholding of a document, which, if released, would allow circumvention of an agency rule, policy, or statute thereby impeding the agency in the conduct of its mission. The “low” profile permits withholding, if there is no public interest in the document, and it would be an administrative burden to process the request.
- X3 Information specifically exempted by a statute establishing particular criteria for withholding. The language of the statute must clearly state that the information will not be disclosed.
- X4 Information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis (could cause competitive harm to the company, impair the government’s ability to obtain like information in the future, or protect the government’s interest in compliance with program effectiveness).
- X5 Intra-agency memoranda which are deliberative in nature; this exemption is appropriate for internal documents which are part of the decision-making process and contains subjective evaluations, opinions, and recommendations. (working papers).
- X6 Information which if released could reasonably be expected to constitute a clear unwarranted invasion of the personal privacy of individuals.
- X7 Records or information compiled for law enforcement purposes.
- X8 Certain records of agencies responsible for supervision of financial institutions.
- X9 Geological and geophysical information concerning wells.

Information cannot be classified and FOUO at the same time. However,

classified information can be declassified and designated FOUO if it meets one of the FOIA criteria.

Note: FOUO can be disseminated within DoD components, and between officials of Army components, and Army contractors, consultants, and grantees as necessary to conduct official business.

Company Proprietary: U.S. Government is obligated to protect information marked with the company name and "proprietary" in accordance with the Federal Acquisition Regulation (FAR).

Some of the terminology in the Level of Classification Determination Tool raises questions of interpretation. The following definitions are intended to elaborate on those terms, and have been extracted from appropriate DoD references. In some instances, they have been modified or tailored to meet the requirements of this process.

**Classified Performance Capabilities or Limitations:** Information that if disclosed would 1) damage national security through facilitating adversary denial, degradation, disruption, deception, or destruction of mission essential or critical system(s), or 2) would require major modifications to an acquisition program or operational system to maintain the technological advantage of the system during its projected operational life time.

**Compromise a Future Capability:** Anything not in the inventory now and is planned to be developed, not a current capability. Applies to Research, Development and Acquisition efforts.

**Critical Information:** To be determined (TBD) by the supported organization. Different organizations may deem information differently as to its criticality. Determination and defense of information as critical is decided by the supported organization.

**Effectiveness of Forces:** TBD by supported organization. Usually refers to military forces from squad to division level. .Different organizations may deem information differently as to its impact on the effectiveness of forces. For example, information that may impact the effectiveness of a Special Forces unit compared to a tank battalion is potentially considerable. Determination and defense of information is decided by the supported organization.

**Effectiveness of Major Forces:** TBD by supported organization. Usually refers to Theater level, Unified Combatant Command, or a combination of Military Departments. Different organizations may deem information differently as to its impact on the effectiveness of major forces. Determination and defense of information is decided by the supported organization.

**Enhanced System Capability:** An improvement over existing performance or capabilities found on similar systems.

**Low Level Intelligence Collection Capability:** Focused on low level counterintelligence or human intelligence sources, e.g., bartender, “beat cop”; or low level detection capability, e.g., unattended ground sensors.

**Mission Critical:** A mission essential item whose disruption or destruction *immediately* degrades the ability of the force to command, control, or effectively conduct combat operations. For example, disruption or destruction of the mechanism used to fuse a system-of-systems (e.g., C4ISR) would result in the *immediate* inability for the separate system to act in concert as a system-of-systems.

**Mission Essential:** Those items *required* to support approved emergency and/or war plans, and where those items are used to:

a. destroy the enemy or the enemy's capacity to continue war;
b. provide battlefield protection of personnel;
c. communicate under war conditions;
d. detect, locate, or maintain surveillance over the enemy;
e. provide combat transportation and support of men and materiel; and
f. support training functions.

For example, loss of a tank does not eliminate a force’s anti-armor capability since AH-64 Apache helicopter and Javelin man-portable missile capability still exist.

**National Military Objectives:** Protect the United States against external attacks and aggression; prevent conflict and surprise attacks; and prevail against adversaries. These are the ends of the strategy and help to assure allies and friends, dissuade adversaries and deter aggression and coercion while ensuring the Armed Forces remain ready to defeat adversaries should deterrence and dissuasion fail. They serve as benchmarks to assess levels of risk and help to define the types and amounts of military capabilities required.

**National Objectives (for DoD):** The aims derived from national goals and interests, toward which a national policy or strategy is directed and efforts and resources of the nation are applied.

**National Security Strategy (for DoD):** The art and science of developing, applying, and coordinating the instruments of national power (diplomatic, economic, military, and informational) to achieve objectives that contribute to national security. Also called national strategy or grand strategy.

**Reveal a National Security Objective:** Fact of statement that would reveal an undisclosed objective or intention that is covert in nature. Details of how we plan to achieve national security objectives (primarily planning oriented).

**Senior Leadership:** President of the U.S. (POTUS); Cabinet Members, Pentagon Senior Leadership, etc.

**Sensitive Information:** TBD by the supported organization. Different organizations may deem information differently as to its sensitivity. Determination and defense of information as sensitive is decided by the supported organization.

**Sensitive Intelligence Collection Capability:** TBD by the user or developer of that capability.

**Significant Impairment:** Any characteristic or concept, design or component that offers a technical disadvantage of enough magnitude to be potentially disruptive in an operational or advanced system.

**State-of-the-Art**: The highest level of development, as of a device, technique, or scientific field, achieved at a particular time. For a system or technology that has no known baseline to determine its relative level of development, the very nature of it being the first of a kind, makes it state of the art.

**Strategic Advantage:** Operational superiority provided via military instruments that enables one nation or group of nations effectively to control the course of a military or political situation beyond a battle or engagement.

**Strategic Disadvantage:** Inverse of strategic advantage (see above definition).

**Tactical Advantage:** Operational superiority provided via unit and system performance and capabilities during battles and engagements planned and executed to accomplish military objectives assigned to tactical units or task forces.

**Tactical Disadvantage:** Inverse of tactical advantage (see above definition).

**Threaten the Country's Ability to Wage War:** Identification of details of war plans that would reveal overall objectives or intentions. .

**Weaken the Country's Ability to Wage War:** Identification of specific details of war plans in a theater of operation including use of tactical capabilities and mission essential items.

**Significantly Weaken the Country's Ability to Wage War:** Identification of specific dependencies and objectives in a theater of operation or sub area of a Unified Combatant Command to include strategic capabilities and mission critical items.

**Threaten the International Position of the U.S.:** Damage U.S. credibility with a foreign government.

**Weaken the International Position of the U.S.:** Negative impact to the international position of the U.S. and its ability to negotiate with foreign governments.

**Significantly Weaken the International Position of the U.S.:** Inability of the U.S. to successfully negotiate with a foreign government for a significant period of time.

**Unique and Fragile Intelligence Collection Capability:** To be determined by the user or developer of that capability.

---

**Examples:**

1. In reviewing an acquisition system SCG, the original classification authority (OCA) notices that the element related to the identification of the potential subcontractors involved in the development of the system is public release information. The OCA concurs that the identification of potential subcontractors does not rise to the level for security classification. However, the OCA does not consider that information to be unclassified, public release data. The OCA calls in specific members of the CMWG, specifically the Security Manager, Senior Engineer and Public Affairs Officer, to discuss the issue. The OCA asks these specialists whether there is a way to prevent this unclassified information from being categorized as public release data. The OCA's rationale centered on the fact that certain subcontractors have a narrow and specialized niche in the defense industry. The group of specialists concluded that the OCA's desires could be accomplished by assigning the FOR OFFICIAL USE ONLY handling caveat
to this element.

2. The CMWG convenes after a Critical Program Information (CPI) assessment to ensure that the identified CPI is properly addressed in the current system SCG. One of the CPI was assessed as representing unique, beyond state-of-the-art technology that is being employed to satisfy one of the key performance parameters for the system. The prime contractor has declared this technology as proprietary data. Based on the above circumstances, the members of the CMWG discussed whether proprietary data is eligible to be classified by the US Army. After extensive discussion, the group concluded that since the technology was an eligible element of the system, its eligibility to be considered for security classification was valid and an inherent part of the SCG, which in turn was an integral component of the contract between the US Army and the prime contractor. In applying the classification management methodology and tools, the IPT determined that the CPI should be classified at the SECRET security classification level. The following rationale applied:

- In assessing the CONFIDENTIAL security classification level, the CMWG determined that the following criteria applied:

- Loss of information that would compromise a future capability.

- In assessing the SECRET security classification level, the CMWG determined that the following criteria applied:

  - Loss of research, development and engineering, scientific or technical information that would compromise a state of the art capability or negate the operational effectiveness of the system.
  - Loss of information that would limit the effectiveness of forces.
  - Denial, degradation, disruption, deception, or destruction of mission *essential* system(s)
  - Major modifications to an acquisition program or operational system to maintain the *tactical* advantage of the system during its projected operational life time.

Since the system involved was not considered a strategic weapons program, the TOP SECRET security classification level was not considered warranted.

3. A CMWG has been convened to develop security classification guidance regarding special operations tactics, techniques and procedures (TTPs). In discussing the eligible elements for inclusion in the guidance document, the team realized that it had to address TTPs employed against targets of tactical and strategic interests as separate and distinct entities. Accordingly, the CMWG determined that TTPs used against targets of tactical and strategic interests were eligible to be classified under the guidance being developed. However, the team decided to address these TTPs in two separate sections of the guidance document. In applying the classification management methodology and tools, the CMWG determined that the TTPs employed against targets of tactical interest should be classified at the SECRET security classification level. The following rationale applied:

- In assessing the CONFIDENTIAL security classification level, the CMWG determined that the following criteria applied:

  - Loss of information that would compromise a future capability

- In assessing the SECRET security classification level, the CMWG determined that the following criteria applied:

  - Loss of operational, intelligence or battlefield information leads to a *tactical* disadvantage.
  - Loss of information that would limit the effectiveness of forces.

However, in determining the security classification level for unique TTPs employed against targets of strategic interest, the criteria at the TOP SECRET security classification level were met. The following rationale applied:

- In assessing the CONFIDENTIAL security classification level, the CMWG determined that the following criteria applied:

  - Loss of information that could threaten the international position of the U.S
  - Loss of information that would compromise a future capability

- In assessing the SECRET security classification level, the CMWG determined that the following criteria applied:

  - Loss of *sensitive* intelligence collection capabilities or revelation that the US has or is capable of obtaining *sensitive* foreign information or material.
  - Loss of operational, intelligence or battlefield information leads to a *tactical* disadvantage.
  - Loss of information that would *weaken* the international position of the US.
  - Loss of information that would limit the effectiveness of forces.

- In assessing the TOP SECRET security classification level, the CMWG determined that the following criteria applied:

  - Significant impairment to the flow of *critical* information to national policy makers.
  - Loss of *unique* and *fragile* intelligence collection capabilities or revelation that the US has, or is capable of obtaining *critical* foreign information or material.
  - Loss of operational, intelligence or battlefield information that would lead to a *strategic* disadvantage.
  - Loss of information that would *significantly weaken* the international position of the US.
  - Loss of information would limit the effectiveness of major forces.

---

**Step 5 – Record Results of Classification Determination**

For a single classification level, delineate the primary criteria that applied to the level of classification in the Remarks column. For a range, e.g., U-S, or U, C, S, etc., it is imperative that criteria for the differing levels are included in the remarks column. For example, “C if xxx”, “S when yyy.” The goal of the process is to develop as clear and specific guidance as possible. As such, using a classification range requires the remarks column to differentiate when an item meets the various levels.

Remember that Not Releasable to Foreign Nationals (NOFORN) is used to identify *intelligence* which an originator has determined falls under the criteria of Director of Central Intelligence Directive (DCID) 6/7 *Intelligence Which May Not Be Disclosed or Released* and may not be provided in any form to foreign governments, international organizations, coalition partners, foreign nationals or immigrant aliens without originator approval. Document all substantive discussions in the compendium.

---

**Example:**

1. A Classification Management Working Group is utilizing the criteria for the three security classification levels to determine the proper security classification of vulnerabilities to the guidance components of a smart munition system. In analyzing the CONFIDENTIAL criteria list, the group agreed that the loss of this information would in fact result in the "compromise of a future capability." Consequently, the group moved up to the next higher security classification level and reviewed the criteria list. The consensus was that the following criteria were deemed appropriate:

a. Loss of information would limit the effectiveness of forces.

b. Loss of information would lead to the denial, degradation, disruption, deception, or destruction of a mission essential system.

c. Loss of information would result in major modifications to an acquisition program or operational system to maintain the *tactical* advantage of the system during its projected operational life time.

Since the equipment was a tactical and not strategic weapons system, the group concluded that the vulnerability of the guidance component element of the security classification guide should be classified at the SECRET level.

2. MAJOR Jay Olsen, US Army Training and Doctrine Command (TRADOC) point of contact for Army concepts and doctrine (to include tactics, techniques and procedures (TTPs)) elicits the assistance of the command Security Manager to develop security classification guidance involving counter-improvised explosive device (C-IED) TTPs. In assessing the extent of the task, the Security Manager immediately realized that a working group of subject matter experts (SMEs) would be required to determine the proper security classification levels of the information involved. The initial analysis by the SMEs concluded that the majority of the raw data that will be reviewed in developing the Army's TPPs would be after-action or lessons-learned reports, which ranged in security classification from CONFIDENTIAL to SECRET. Some of the reports were unclassified, but protected with the FOR OFFICIAL USE ONLY handling caveat. Although some of the reports were classified, the group, using the Army Research and Technology Protection Center Classification Management Classification tool,

determined that TPP information did not meet any of the criteria listed for each security classification level, but decided that the FOR OFFICIAL USE ONLY handling caveat would apply. The group provided the following rationale for its recommendation:

a. Derivative classification from the classified reports did not apply since the TTPs were general in nature. In addition, no specific details from any of the classified reports would be incorporated in the TTPs.

b. The general nature of the TTPs permitted commanders to exercise their initiative and tailor the TTPs to the specific threat situation and tactical mission. Therefore, the TTPs would not constitute the proverbial “one size fits all situations” approach.

---

**Exercise Questions**:

1. Under the provisions of Executive Order 12958, as amended, an original classification authority determines that an element in his/her SCG is unclassified and therefore automatically releasable to the public.

□ TRUE or FALSE

2. Aggregate or compiled information should be classified at an appropriate level until an analysis of that data can be accomplished and validated by the OCA. This action is conducted to prevent compromise or inadvertent disclosure of that information.

□ TRUE or FALSE

3. When a Classification Management Working Group exercises the option of using an equivalent security classification guide (SCG) to identify elements for its SCG, the security classification levels associated with each equivalent element will also be automatically inherited.

□ TRUE or FALSE

4. Not Releasable to Foreign Nationals or NOFORN is a security classification that is exclusive to the Intelligence Community.

□ TRUE or FALSE

5. An Army original classification authority (OCA) at an Army test range determines that, absent a security classification guide for a specific Marine Corps weapon system that is undergoing battlefield evaluation at the Army range, the results of the test will be classified SECRET. The rationale for classification in the first instance is that the loss of information would *weaken* the country's ability to wage war. In this case, the Army OCA interpreted this criteria correctly.

□ TRUE or FALSE

6. In determining the proper security classification of combined foreign and United States classified information in support of a division-level exercise, officials from both parties convened a meeting to discuss this issue. In a specific instance, Country X SECRET information was combined with United States CONFIDENTIAL information. The following question arose: What is the proper security classification of the resultant information? Both parties agreed that the combined information should be classified as

“U.S./Country X SECRET” with ownership residing jointly. The final security classification

determination was correct and did not violate the provisions of Executive Order 12958, as amended.

□ TRUE or FALSE

7. Despite having the authority to applying security classification to proprietary data, the United States Government is nevertheless obligated to protect information marked with the company name and “proprietary” in accordance with the Federal Acquisition Regulation (FAR).

□ TRUE or FALSE

8. According to Executive Order 12958, as amended, the fourth and final classification standard states that “the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.” How does the executive order define the three security classification levels in terms of “damage” to national security:

a. CONFIDENTIAL: _____

b. SECRET: _____

c. TOP SECRET: _____

9. In conducting scientific research for an Army Technology Objective, the Technology Manager originally classifies a unique technique as SECRET. After making this determination, what is the next step in the Classification Management process?

10. FOR OFFICIAL USE ONLY (FOUO) is a handling caveat that applies to unclassified information that is exempt from mandatory release to the public under the Privacy Act and may be used for protecting a variety of information.

□ TRUE or FALSE

**Exercise Answers:**

1. FALSE (p. 22)

2. TRUE (p. 23)

3. FALSE (p. 13)

4. FALSE (p. 32)

5. FALSE (p. 13)

6. TRUE (p. 13)

7. TRUE (p. 26)

8. a. Damage (p. 23)
   b. Serious damage (p. 24)
   c. Exceptionally grave damage (p. 25)

9. Declassification/downgrading (p. 10)

10. FALSE (pp. 26, 27)

## Step 6 – Declassification/Downgrading

Maintaining security classification beyond its usefulness is costly and burdensome. At the time information is classified, the OCA should address downgrading (if applicable) and declassification. Downgrading and declassification are usually associated with a predetermined point in time or a specific event, such as the initial fielding or deployment of a system, expected life of the system, or date of completion of an exercise.

The CMWG should take each item that is classified through the Declassification/ Downgrading Tool with the goal of linking downgrading (if applicable) and declassification to a specific time or event. Choose a date within 25 years from the date of the classification to declassify the information, or it will automatically be declassified 25 years from the date of classification. When choosing a date, the CMWG should try to identify an event after which classification is no longer appropriate, such as a missile launch event. While the data gathered at the site may remain classified after the completion of the event, the date of the actual launch may not require continued protection by security classification. The CMWG should document all pertinent discussions/rationale in the compendium.

*Special consideration: Keep in mind the 25 year automatic declassification rule when dealing with programs such as research and development, acquisition, operational planning, or exercises.*

## Declassification/Downgrade Tool

**(Figure 3)**

*Information will be declassified when it no longer requires protection. Declassification is to remove security classification protection from the information under E.O. 12958 and AR 380-5. Information will be regraded when its sensitivity changes. Regrading is changing the classification level either higher of lower.*

**Can you determine during the SCG development process when to declassify or regrade?**

☐ Yes:

- Sensitivity lessens (list date or event for downgrade, such as initial fielding of a system — downgrade DOES NOT replace or equate to declassification)
- Classification is no longer needed (list declassification date, such as XX April 200X)
  - Automatic declassification at 25 years

☐ No: Requests for exemption from the 25-year automatic declassification rule must be reported to DAMI-CD, as a "Notice of the Intent to Exempt Information from Automatic Declassification," and will

- Describe the specific information to be exempted
- Explain why the information must remain classified

Except for the identity of a confidential human source or a human intelligence source, provide a specific date or event upon which the information will be declassified.

**Example:**

1. An organization initially issues a security classification guide on the AH-007 Attack Helicopter aircraft on 4 July 1997. The guide states that the fact that the AH-007 aircraft has a maximum airspeed of 350 miles per hour will be classified at the SECRET level for a period of 15 years. A document dated 16 October 2004 is classified because it reveals the maximum airspeed of the AH-007 helicopter. The document should be marked for declassification on 4 July 2012, 15 years after the specific information was first recorded in the guide, not on 16 October 2019, 15 years after the derivatively classified document was created.

2. An organization security classification guide issued on 11 December 1996 states that the maximum effective range of any smart munitions will be classified at the SECRET level for a period of five years. The organization first records the specific maximum effective range of the new M-666 munitions on 14 August 1998. The document should be marked for declassification on 14 August 2003, five years after the specific information is first recorded, and not on 11 December 2001, five years after the date of the guide's generic instruction. Subsequent documents containing this information would be marked for declassification five years from the date of the original document dated 14 August 1998.

---

## Step 7 – Record Declassification/Downgrade Results

The results should be listed in the Declassification column. Any event that facilitates the declassification or downgrading of information should be considered and noted in this column, such as the declassification of certain information after a test. The only exemption to the automatic 25-year declassification is Exemption #1, revealing of the identity of a confidential source or revealing information about the application of an intelligence source or method. Requests for exemptions may be submitted according to E.O. 12958. All necessary information should be recorded in the Remarks column. Amplifying information should be recorded in the compendium.

## Step 8 – Filling Out the Classification Column

Those Elements not classified as "C", "S" or "TS" are to be marked "U" in the Classification column. Elements that are unclassified should remain in the table. This facilitates user needs. Remember, stating that an element is unclassified is security classification guidance.

## Step 9 – Determining FOUO Eligibility

The CMWG should review each Element that is marked U for the potential assignment of the FOR OFFICIAL USE ONLY or FOUO caveat.

Use the Level of Classification Determination Tool (Figure 1) to review each applicable Element and determine whether the information is exempt from public release under the Freedom of Information Act (FOIA). Document all pertinent discussions in the compendium.

**Step 10 – Record FOUO Results and Determine Distribution**

Record the results of the assignment of the FOUO caveat to any element in the Remarks column. For example, use wording such as "Mark and handle as FOUO and FOIA exemption 4 applies." Always link the use of FOUO to a FOIA exemption category. Information previously released to the public under the Distribution Statement A marking should not be marked FOUO. Document any amplifying information in the compendium.

Upon determining that FOUO caveat markings apply, the CMWG should review those U/FOUO Elements for the assignment of specific Distribution Statements. DoD Directives 5230.24, *Distribution Statements on Technical Documents*, and 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure*, provide criteria for assignment of Distribution Statements associated with technical data. DoD Directive 5230.25 provides policy and procedures for the withholding of unclassified technical data from the public at large when the following criteria are met:

1. the information is in the possession of or under the control[1] of the DoD,
2. the information has military or space application,[2]
3. the information may not be exported lawfully without an approval, authorization or license under US export control laws, and
4. the information discloses critical technology.

DoD Directive 5230.25 defines critical technology as data that reveals production know-how that would contribute significantly to a country's military potential and possibly prove detrimental to the security of the United States. Such data may be comprised in part or in whole of:

- Arrays of design and manufacturing know-how
- Keystone manufacturing, inspection, and test equipment
- Keystone materials
- Goods accompanied by sophisticated operation, application or maintenance know-how

[1] Created or received by elements of the Department and information developed and produced for the Department under contractual arrangements or other agreements

[2] Blueprints, drawings, plan, instruction, computer software and documentation, or other technical information that can be used or adapted for use to design, engineer, produce, manufacture, operate, repair, overhaul or reproduce military or space equipment or technology.

---

**Example:**

1. An Exercise Group of U.S. Army Forces Command (FORSCOM) is commencing the development of a scenario for a combined exercise with defense forces from Country X. Since exercise specialists from Country X are participating fully in the development of the scenario and script, U.S. FORSCOM officials decided to use notional information for the exercise and classified that data according to the organization's SCG for exercises, to include all intelligence threat data. After applying security classification determinations to the exercise scenario and script information, the exercise group reviewed the downgrading and declassification instructions outlined in the SCG. Accordingly, all classified exercise information would be declassified at the completion of the exercise and then assigned the FOR OFFICIAL USE ONLY handling caveat. Both exercise participants concurred that the specific scenario and script information should not be made available to the public at large.

---

Figure 4 provides a consolidated list of the Distribution Statements and warning statements that are available for use when marking technical information, export-control data, information on software or hardware in development, or information requiring protection from premature dissemination or subject to special dissemination limitations.

## Distribution Statements
## Figure 4

DoD Directive 5230.24 requires statements to be placed on both classified and unclassified technical documents. When deciding which Distribution Statement to apply, consider the extent of the audience to whom the information should be disseminated to ensure that the enforced need-to-know principle is implemented.

Distribution Statement A: Approved for Public Release; distribution is unlimited

- Unclassified technical documents
- Cleared for public release
- Competent authority (owner of data)
- Technical documents resulting from contracted fundamental research (exception: high likelihood disclosure of performance characteristics, mfg technologies that are unique and critical to defense and agreement on this has been documented in the contract or grant—see eligibility tool for sensitive/classified issues)
- Technical documents with this statement may be made available or sold to the public and foreign nationals, companies, and governments including adversary governments, and may be exported.
- May not be used on technical documents that formerly were classified unless the documents are cleared for public release in accordance with DoD Directive 5230.9 *Clearance of DoD Information for Public Release, April 2, 1982*.
- Shall not be used on classified technical documents or documents containing export-controlled technical data

Distribution Statement B: Distribution authorized to US Government Agencies only (fill in reason) (date of determination). Other requests for this document shall be referred to (insert controlling DoD office). This would include Agencies such Department of Transportation, Department of Commerce, Department of Energy, Department of Treasury, and Department of Homeland Security.

- Unclassified and classified technical documents
- Reasons include:

Foreign Government Information: To protect and limit distribution in accordance with the desires of the foreign government that furnished the technical information. Information of this type normally is classified at the CONFIDENTIAL level or higher in accordance with DoD 5200.1-R.

Proprietary Information: To protect information not owned by the US Government and protected by a contractor's "limited rights" statement, or received with the understanding that it not be routinely transmitted outside the US Government.

Critical Technology: To protect information and technical data that advance current technology or describe new technology in an area of significant or potentially significant military application or that relate to a specific military deficiency of a potential adversary. Information of this type may be classified or unclassified; when unclassified, it is export-controlled and subject to the provisions of DoD Directive 5230.25

Test and Evaluation: To protect results of test and evaluation of commercial products or military hardware when such disclosure may cause unfair advantage or disadvantage to the manufacturer of the product.

Contractor Performance Evaluation: To protect information in management reviews, records of contract performance evaluation, or other advisory documents evaluating programs of contractors.

Premature Dissemination: To protect patentable information on systems or processes in the developmental or concept stage from premature dissemination.

Administrative or Operational Use: To protect technical or operational data or information from automatic dissemination under the International Exchange Program or by other means. This protection covers publications required solely for official use or strictly for administrative or operational purposes. This statement may be applied to manuals, pamphlets, technical orders, technical reports, and other publications containing valuable technical or operational data.

Software Documentation: Releasable only in accordance with DoD Instruction 7930.2, *ADP Software Exchange and Release, 31 December 1979.*

Specific Authority: To protect information not specifically included in the above reasons and discussions, but which requires protection in accordance with valid documented authority such as Executive Orders, classification guidelines, DoD or DoD Component regulatory documents.

When filling in the reason, cite *"Specific Authority (identification of valid documented authority)."*

Distribution Statement C: Distribution authorized to US Government Agencies and their contractors (fill in reason) (date of determination). Other requests for this document shall be referred to (insert controlling DoD office).

- Unclassified and classified technical documents
- Reasons include:

  Foreign Government Information: To protect and limit distribution in accordance with the desires of the foreign government that furnished the technical information. Information of this type normally is classified at the CONFIDENTIAL level or higher in accordance with DoD 5200.1-R.

  Critical Technology: To protect information and technical data that advance current technology or describe new technology in an area of significant or potentially significant military application or that relate to a specific military deficiency of a potential adversary. Information of this type may be classified or unclassified; when unclassified, it is export-controlled and subject to the provisions of DoD Directive 5230.25

  Software Documentation: Releasable only in accordance with DoD Instruction 7930.2.

  Administrative or Operational Use: To protect technical or operational data or information from automatic dissemination under the International Exchange Program or by other means. This protection covers publications required solely for official use or strictly for administrative or operational purposes. This statement may be applied to manuals, pamphlets, technical orders, technical reports, and other publications containing valuable technical or operational data.

  Specific Authority: To protect information not specifically included in the above reasons and discussions, but which requires protection in accordance with valid documented authority such as Executive Orders, classification guidelines, DoD or DoD Component regulatory documents. When filling in the reason, cite *"Specific Authority (identification of valid documented authority)."*

Distribution Statement D: Distribution authorized to DoD Department of Defense and U.S. DoD contractors only (fill in reason) (date of determination). Other requests shall be referred to (insert controlling DoD office).

- Unclassified and classified technical documents
- Reasons include:

Foreign Government Information: To protect and limit distribution in accordance with the desires of the foreign government that furnished the technical information. Information of this type normally is classified at the CONFIDENTIAL level or higher in accordance with DoD 5200.1-R.

Administrative or Operational Use: To protect technical or operational data or information from automatic dissemination under the International Exchange Program or by other means. This protection covers publications required solely for official use or strictly for administrative or operational purposes. This statement may be applied to manuals, pamphlets, technical orders, technical reports, and other publications containing valuable technical or operational data.

Software Documentation: Releasable only in accordance with DoD Instruction 7930.2.

Critical Technology: To protect information and technical data that advance current technology or describe new technology in an area of significant or potentially significant military application or that relate to a specific military deficiency of a potential adversary. Information of this type may be classified or unclassified; when unclassified, it is export-controlled and subject to the provisions of DoD Directive 5230.25

Specific Authority: To protect information not specifically included in the above reasons and discussions, but which requires protection in accordance with valid documented authority such as executive Orders, classification guidelines, DoD or DoD Component regulatory documents. When filling in the reason, cite *"Specific Authority (identification of valid documented authority)."*

Distribution Statement E: Distribution authorized to DoD Components only (fill in reason) (date of determination). Other requests shall be referred to (insert controlling DoD office).

- Unclassified and classified technical documents
- Reasons include:

Direct Military Support: The document contains export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize an important technological or operational military advantage of the United States. Designation of such data is made by competent authority in accordance with DoD Directive 5230.25.

Foreign Government Information: To protect and limit distribution in accordance with the desires of the foreign government that furnished the technical information. Information of this type normally is classified at the CONFIDENTIAL level or higher in accordance with DoD 5200.1-R.

Proprietary Information: To protect information not owned by the U.S. Government and protected by a contractor's "limited rights" statement, or received with the understanding that it not be routinely transmitted outside the U.S. Government.

Premature Dissemination: To protect patent able information on systems or processes in the developmental or concept stage from premature dissemination.

Test and Evaluation: To protect results of test and evaluation of commercial products or military hardware when such disclosure may cause unfair advantage or disadvantage to the manufacturer of the product.

Software Documentation: Releasable only in accordance with DoD Instruction 7930.2.

Contractor Performance Evaluation: To protect information in management reviews, records of contract performance evaluation, or other advisory documents evaluating programs of contractors.

Critical Technology: To protect information and technical data that advance current technology or describe new technology in an area of significant or potentially significant military application or that relate to a specific military deficiency of a potential adversary. Information of this type may be classified or unclassified; when unclassified, it is export-controlled and subject to the provisions of DoD Directive 5230.25.

Administrative or Operational Use: To protect technical or operational data or information from automatic dissemination under the International Exchange Program or by other means. This protection covers publications required solely for official use or strictly for administrative or operational purposes. This statement may be applied to manuals, pamphlets, technical orders, technical reports, and other publications containing valuable technical or operational data.

Distribution Statement F: Further dissemination only as directed by (inserting controlling DoD office) (date of determination) or higher DoD authority.

- Normally used for classified technical documents

- May be used on unclassified technical documents when specific authority exists (e.g., designated as direct military support as in statement E.).

Distribution Statement X: Distribution authorized to US Government Agencies and private individuals or enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25 "Withholding of Unclassified Technical Data From Public Disclosure", Nov 6, 1984, (date of determination). Controlling DoD Office is (insert).

- Unclassified documents when Distribution Statements B, C, D, E, or F does not apply, but the document does contain technical data as explained in DoD Directive 5230.25.
- Shall not be used on classified technical documents; however may be assigned to technical documents that formerly were classified.

Export Control Warning: "WARNING -This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, USC., Sec 2751, et. seq.) or the Export Administration Act of 1979, as amended, (Title 50 USC., App.2401 et. seq). Violations of these laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25."

- All technical documents containing export-controlled technical data
- Technically infeasible to use the entire statement, an abbreviated marking may be used, and a copy of the full statement added to the "Notice To Accompany Release of Export-Controlled Data" required by DoD Directive 5230.25.
- Must also bear the following marking: "**DESTRUCTION NOTICE –** For classified documents, follow the procedures in DoD 5220.22-M, Industrial Security Manual, Section 11-19 or DoD 5200.1-R, Information Security Program Regulation, Chapter IX. For unclassified, limited documents, destroy by any method that will prevent disclosure of contents or reconstruction of the document"

In determining whether data represents technical controlled unclassified information under the provisions of DoD Directive 5230.25, CMWG representatives (particularly scientists and engineers) should be familiar with the US Munitions Lists of the International Traffic in Arms Regulation (Department of State) and the Commerce Control List of the Export Administration Regulation. These documents are available at the following websites:

http://www.pmdtc.org/ITAR/2005/22cfr121_Part_121 and
http://www.access.gpo.gov/bis/ear/pdf/774, respectively.

## Updating the SCG

AR 380-5 requires that SCGs be reviewed every five years or prior to any defense acquisition program milestone review. Figure 5 is a Classification Review Tool that will assist in this review. It is recommended that the CMWG convene to conduct the review. In addition, consideration should be given to downgrading classified information whenever possible, especially when the lower classification level will provide adequate protection. *Remember that downgrade does not replace declassification*.

Sample formats of SCGs (acquisition program and research project) are at appendices A and B, respectively.

## Classification Review Tool
## Figure 5

In accordance with AR 380-5, SCGs or security classification guidance should be reviewed every five (5) years, prior to the milestone review of a defense acquisition program or when there are significant changes to a program.

1. Have there been any changes in criticality/sensitivity to the existing elements in the Security Classification Guide (SCG)?

☐ No Go to #4 and keep existing classification
☐ Yes Go to #2

2. Has the information changed to reflect lower/decreased sensitivity?

☐ No Go to #3
☐ Yes Go to Level of Classification Determination Tool

3. Has the information changed to reflect increased sensitivity?

☐ No Go to #4
☐ Yes Go to Level of Classification Determination Tool

4. Is there new (not previously captured/identified) sensitivity/critical program information?

☐ No Stop
☐ Yes Go to Eligibility Tool

**Exercise Questions:**

1. According to E.O. 12958, as amended, information that is classified is automatically downgraded to the next lower security classification level at 10-year intervals (as applicable) and declassified at 25 years, unless an exemption is approved.

□ TRUE or FALSE

2. In submitting a request for exemption from the automatic 25-year declassification rule, the requestor must describe the specific classified information to be exempted and provide rationale for the continued security classification of the information beyond 25 years.

□ TRUE or FALSE

3. An Original Classification Authority initially publishes a security classification guide regarding the OH-88 Reconnaissance Helicopter on 9 September 1999. The guide indicates that the manufacturing technique employed to achieve a "silent" rotor blade is SECRET. The period of classification of this information is 20 years. A technical specifications document for the aircraft includes the classified data on this rotor blade. The document is dated 1 January 2003. As a result, the document should be declassified on:

A. 31 December 2022

B. 1 January 2023

C. 9 September 2019

D. 8 September 2019

E. None of the above

4. An organization issued a security classification guide on 15 May 2002 stating that all countermeasures to detection of ground surveillance radars will be classified at the SECRET security classification level for a period of ten years. The US Army Training and Doctrine Command first records tactics, techniques and procedures that effectively provide countermeasures to detection for the AN/GSR-77 radar is in a training manual. The date of issuance of the manual is 17 August 2007. The declassification instructions for this manual should be:

A. 17 August 2017

B. 15 May 2012

C. 16 August 2017

D. 14 May 2012

E. None of the above

5. In determining that an element of a security classification guide is unclassified but not releasable to the public, the Classification Management Working Group should at a minimum select a DISTRIBUTION STATEMENT that would apply to the information according to Department of Defense Directive (DoDD) 5230.24, *Distribution Statements on Technical Documents,* and/or DoDD 5230.25*, Withholding of Unclassified Technical Data from Public Disclosure.*

□ TRUE or FALSE

6. According to the definition cited in Department of Defense Directive 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure*, the unclassified technical data involved essentially constitutes export-controlled information.

□ TRUE or FALSE

7. When addressing declassification considerations after a security classification level has been determined for a specific element of a security classification guide, the Classification Management Working Group should factor the following:

- Sensitivity decreases
- Security classification is no longer required
- Automatic declassification at 25 years
- Automatic downgrading at 10 years, as appropriate

□ TRUE or FALSE

8. In applying the "FOR OFFICIAL USE ONLY" handling caveat for unclassified information that is determined to be withheld from the public, the applicable "Exemption" categories to the Freedom of Information Act should be designated to inform the user of the security classification guide regarding the rationale for the withholding of the information from the public.

□ TRUE or FALSE

9. The Exercise Working Group of a combatant command is developing a security classification guide with the assistance of the Classification Management Working Group. The collective subject matter experts determined, through the employment of the classification tool, that the exercise scenario would be classified at the SECRET security classification level. Additionally, the guide would also dictate that the scenario would be downgraded to the CONFIDENTIAL security classification level at the

termination of the exercise. Declassification of the scenario would occur five years after the completion of the exercise, but the “FOR OFFICIAL USE ONLY” handling caveat would apply. The declassification and downgrading of classified information described above is in compliance with the principles of Executive Order 12958, as amended, as well as its implementing issuances within the Department of Defense.

□ TRUE or FALSE

10. Some of the categories that are used to justify the exemption of classified information from the 25-year automatic declassification provision include the following:

A. Identity of a confidential human source, or a human intelligence source.

B. Information that would assist in the development or use of weapons of mass destruction.

C. Information that would embarrass the U.S. Government.

D. Actual U.S. military war plans.

□ TRUE or FALSE

**Exercise Answers:**

1. FALSE (p. 39)
2. TRUE (p. 39)
3. c (p. 40)
4. a (p. 40)
5. TRUE (p. 41, 43-47)
6. TRUE (p. 41)
7. FALSE (p. 40)
8. TRUE (pp. 40-41)
9. TRUE (p. 38)
10. FALSE (p. 40)

# Appendix A

## Sample Acquisition Program Security Classification Guide Format

| ELEMENT | CLASS | DECLAS | REMARKS |
|---|---|---|---|
| **1.0 ADMINISTRATIVE** | | | |
| ***1.1 General Details*** | | | |
| 1.1.1Program Name | | | |
| 1.1.2 Description of *program* | | | |
| ***1.2 Contractor Relationships*** | | | |
| 1.2.1 Association of specific vendors with *program name* | | | |
| **1.3 Program Resources** | | | |
| 1.3.1 Funding level | | | |
| 1.3.2 Overall budget by year, category, and system, (e.g., POM submission) | | | |
| 1.3.3 Manpower, overall by year, category, skill, and system | | | |
| 1.3.4 Identification of particular installation, facility, or range associated with *program name* | | | |

| | | | |
|---|---|---|---|
| 1.3.5 Information about *program name* related facilities that reveal production details (e.g., capacity, volume, etc.) | | | |
| **1.4 Program Security** | | | |
| 14.1 Identification of program protection risk management processes | | | |
| 1.4.2 Results of program protection risk management analysis | | | |
| 1.4.3 Details of specific protection measures associated with the *program name* | | | |
| **2.0 REQUIREMENTS** | | | |
| 2.0.1 General information regarding requirements for the *program name* | | | |
| 2.0.2 Specific technical requirements associated with a specific system, subsystem or component | | | |
| 2.0.3 Identification of key performance threshold/objective parameters associated with the *program name* a specific system, subsystem or component | | | |
| **3.0 HARDWARE/SOFTWARE** | | | |
| **3.1 Technology Integration** | | | |
| 3.1.1 General description of technologies being considered for use in the *program name* | | | |
| 3.1.2 Specific technical details of technologies being considered for use in a specific system, subsystem, or component | | | |

| | | | |
|---|---|---|---|
| **3.2 Design Details** | | | |
| 3.2.1 Design specifications of individual system, subsystem or component | | | |
| 3.2.2 General details of individual system, subsystem or component design | | | |
| 3.2.3 Specific technical details regarding individual system, subsystem or component design | | | |
| **3.3 Modeling & Simulation** | | | |
| 3.3.1 Fact that modeling & simulation is used for design and validation of the a specific system, subsystems or components | | | |
| 3.3.2 Operational parameters for specific modeling & simulation at the force, system, subsystem, or component level (e.g., force lay-down) | | | |
| 3.3.3 Details of specific items in the modeling & simulation data base | | | |
| 3.3.4 Results of modeling & simulation | | | |
| **3.4 Commercial off the shelf (COTS)/Government off the shelf (GOTS)** | | | |
| 3.4.1 Fact that COTS/GOTS are used on *program* systems | | | |
| 3.4.2 Identification of COTS/GOTS used on a particular system, subsystem, component | | | |
| 3.4.3 Fact of modification to COTS/GOTS | | | |
| 3.4.4 Technical details about modification of COTS/GOTS | | | |
| **3.5 Manufacturing/Fabrication** | | | |
| 3.5.1 Fact that unique/non-traditional manufacturing processes are used to develop systems, subsystems and components | | | |

| | | | |
|---|---|---|---|
| 3.5.2 Identification of specific unique/non-traditional manufacturing processes used to develop systems, subsystems and components | | | |
| 3.5.3 Technical details of unique/non-traditional manufacturing processes used to develop systems, subsystems and components | | | |
| ***3.6 Integration*** | | | |
| 3.6.1 Fact that unique/non-traditional integration processes are used to develop systems, subsystems and components | | | |
| 3.6.2 Identification of unique/non-traditional integration techniques with a specific system, subsystem or component | | | |
| 3.6.3 Technical details of unique/non-traditional integration techniques relative to a specific system, subsystem or component | | | |
| ***3.7 External/Internal Views*** | | | |
| 3.7.1 External views of systems, subsystem or components | | | |
| 3.7.2 Internal views of systems, subsystem or components | | | |
| **4.0 CAPABILITIES/PERFORMANCE** | | | |
| 4.0.1 General information regarding the capabilities of the *program* specific systems, subsystems or components | | | |
| 4.0.2 Specific details regarding the performance of the *program* specific systems, subsystems or components | | | |

| | | | |
|---|---|---|---|
| **5.0 VULNERABILITIES/LIMITATIONS** | | | |
| 5.0.1 General information regarding vulnerabilities/limitations of the *program* specific systems, subsystems or components | | | |
| 5.0.2 Details of specific operational limitations of the *program* a specific systems, subsystems or components | | | |
| 5.0.3 Identification of system susceptibilities in the presence of a validated threat relative to a specific system, subsystem or component | | | |
| 5.0.4 Identification of specific candidate countermeasures to mitigate system security risks | | | |
| 5.0.5 Technical details of specific countermeasures employed (e.g., ECM, signature management, anti tamper, etc.) | | | |
| 5.0.6 Effectiveness of specific countermeasures | | | |
| **6.0 TESTING/ EVALUATION** | | | |
| 6.0.1 Details of test associated with the *program* a specific system, subsystem, or component | | | |
| 6.0.2 Identification of specific dates for program associated tests | | | |
| 6.0.3 Identification of specific test locations associated with the *program* system of system, specific system, subsystem or component | | | |
| 6.0.4 Identification of specific or specialized test instrumentation or equipment associated with the *program* specific systems, subsystems or components | | | |
| 6.0.5 Measures of Effectiveness (MOEs)/Measures of Performance (MOPs) associated with a specific system, subsystem or | | | |

| | | | |
|---|---|---|---|
| component test | | | |
| 6.0.6 Predicted Test Data | | | |
| 6.0.7 Raw test data | | | |
| 6.0.8 Reduced test data | | | |
| **7.0 TRAINING** | | | |
| 7.0.1 Identification and/or location of training specific to *program* a specific system, subsystem or component | | | |
| 7.0.2 Training that reveals specific system information (e.g., design, development, capabilities, vulnerabilities, etc.) | | | |
| **8.0 MAINTENANCE** | | | |
| 8.0.1 Identification and/or location of specialized maintenance organizations associated with *program* a specific system, subsystem or component | | | |
| 8.0.2 Association of maintenance equipment or tools that may reveal specific system information | | | |
| 8.0.3 Maintenance that reveals specific system information (e.g., design, development, capabilities, vulnerabilities, etc.) | | | |
| 8.04. Field level Maintenance | | | |
| 8.0.5. Intermediate level Maintenance | | | |
| 8.0.6. Depot level Maintenance | | | |

## Appendix B

## Sample Research (ATO) Project Security Classification Guide Format

| ELEMENT | CLASS | DECLASS | REMARKS |
|---|---|---|---|
| **1.0 ADMINISTRATIVE** | | | |
| ***1.1 General Details*** | | | |
| 1.1.1Program Name | | | |
| 1.1.2 Description of *program* | | | |
| 1.1.3. The fact that Army is interested in and pursuing programs on | | | |
| 1.1.4. The fact that Army is studying program, including mention of generic mission applications. | | | |
| 1.1.5. The fact that Army is studying program for a specific application or mission. | | | |

| | | | |
|---|---|---|---|
| 1.1.6. Information that predicts or demonstrates the feasibility of program technology. | | | |
| 1.1.7. Status of the program technology without reference to success or failure. | | | |
| ***1.2 Contractor Relationships*** | | | |
| 1.2.1 Association of specific vendors with *program name* | | | |
| **1.3 Program Resources** | | | |
| 1.3.1 Funding level | | | |
| 1.3.2 Overall budget by year, category, and system, (e.g., POM submission) | | | |
| 1.3.3. Detailed breakdown of RDT&E, procurement, or operational costs of program | | | |
| 1.3.4 Manpower, overall by year, category, skill, and system | | | |
| 1.3.5 Identification of particular installation, facility, or range associated with *program name* | | | |
| 1.3.6 Information about *program name* related facilities that reveal technology details (e.g., breakthrough, techniques, applications, etc.) | | | |
| **1.4 Program Security** | | | |
| 1.4.1 Details of specific protection measures associated with the *program name.* | | | |
| **2.0 REQUIREMENTS** | | | |
| 2.0.1 General information regarding requirements for the *program name* | | | |

| | | | |
|---|---|---|---|
| 2.0.2 Specific technical requirements associated with the research program. | | | |
| 2.0.3 Identification of key performance threshold/objective parameters associated with the *program name*. | | | |
| **3.0 CAPABILITIES/PERFORMANCE** | | | |
| 3.0.1 General information regarding the capabilities of the *program* | | | |
| 3.0.2 Specific details regarding the performance of the *program* | | | |
| 3.0.3. Program objectives revealing performance goals of program. | | | |
| 3.0.4. Generic research efforts on materials and devices in a laboratory environment without revealing program technology. | | | |
| **4.0 HARDWARE/SOFTWARE** | | | |
| **4.1 Technology Integration** | | | |
| 4.1.1. General description of technologies being considered for use in the *program name.* | | | |
| 4.1.2. Specific technical details of technologies being considered for use in the program. | | | |
| **4.2 Design Details** | | | |
| 4.2.1 Design specifications of individual technologies within the program. | | | |
| *4.2.2 General details of technology design* | | | |
| 4.2.2.1. Design specifications of the ATO. | | | |

| | | | |
|---|---|---|---|
| *4.2.3 Specific technical details regarding technology design .* | | | |
| 4.2.3.1. Specific technical details of the ATO | | | |
| 4.2.4. Research efforts that indicate significant scientific breakthrough or unique concepts that represent major advance in the state-of-the-art in the program designs, devices, or techniques the program. | | | |
| **4.3 Modeling & Simulation** | | | |
| 4.3.1 Fact that modeling & simulation is used for design and validation of the program. | | | |
| 4.3.2 Operational parameters for specific modeling & simulation. | | | |
| 4.3.3 Details of specific items in the modeling & simulation data base | | | |
| 4.3.4 Results of modeling & simulation | | | |
| 4.3.5. Program objectives revealing performance goals of program demonstrators. | | | |
| 4.3.6. Dates of initial operational capability (IOC) or feasibility demonstrations; RDT&E milestone schedules from which such dates could be inferred. | | | |
| 4.3.7. R&D schedules from which one cannot infer an IOC date or key dates for major technology advances. | | | |
| 4.3.8. Developmental data revealing a significant advance in the state-of-the-art applicable to program. | | | |
| 4.3.9. Designs and/or hardware of test facilities and/or test specimens which if revealed would compromise information classified elsewhere in this document, or permit the conduct of experiments demonstrating program the objectives. | | | |
| **4.4 Commercial off the shelf (COTS)/Government off the shelf (GOTS)** | | | |

| | | | |
|---|---|---|---|
| 4.4.1 Fact that COTS/GOTS are used on *program.* | | | |
| 4.4.2 Identification of COTS/GOTS used on a particular aspect of the research in the program. | | | |
| 4.4.3 Fact of modification to COTS/GOTS | | | |
| 4.4.4 Technical details about modification of COTS/GOTS | | | |
| **4.5 Manufacturing/Fabrication** | | | |
| 4.5.1 Fact that specific unique/non-traditional manufacturing processes are used to develop the program technology. | | | |
| 4.5.2 Identification of specific unique/non-traditional manufacturing processes used to develop the program technology. | | | |
| 4.5.3 Technical details of specific unique/non-traditional manufacturing processes used to develop the program technology. | | | |
| 4.5.4. Research efforts that indicate significant scientific breakthrough or unique concepts that represent major advance in the state-of-the-art in the program materials, processing and fabrication techniques within the program. | | | |
| **4.6 Integration** | | | |
| 4.6.1 Fact that specific unique/non-traditional integration processes are used to develop the program technology | | | |
| 4.6.2 Identification of specific unique/non-traditional integration techniques within the program technology | | | |
| 4.6.3 Technical details of unique/non-traditional integration techniques relative to program technology. | | | |

| | | | |
|---|---|---|---|
| **4.7 External/Internal Views** | | | |
| 4.7.1 External views of component hardware. | | | |
| 4.7.2 Internal views of component hardware. | | | |
| **5.0 VULNERABILITIES/LIMITATIONS** | | | |
| 5.0.1 General operational limitations of the *program.* | | | |
| 5.0.2 Details of specific operational limitations of the *program* . | | | |
| 5.0.3. Identification of system susceptibilities in the presence of a validated threat relative to specific technologies within the program. | | | |
| 5.0.4 *Specific candidate countermeasures employed*. | | | |
| 5.0.5.1. Identification of specific countermeasure | | | |
| 5.0.5.2. Performance/effectiveness of specific countermeasures employed. | | | |
| 5.0.5.3. Technical details of specific countermeasures employed (e.g., ECM, signature management, anti tamper, etc.) | | | |
| 5.0.4. Technical details of specific countermeasures employed (e.g., ECM, signature management, anti tamper, etc.) | | | |
| 5.0.5. Research programs that reveal system vulnerability or susceptibility. | | | |
| **6.0 TESTING/ EVALUATION** | | | |
| 6.0.1 *Identification of specific test and evaluation information* | | | |
| 6.0.1.1 Dates | | | |
| 6.0.1.2. Location | | | |
| 6.0.1.3. Purpose | | | |
| 6.0.1.4. Combination of one or more of the above | | | |

| | | | |
|---|---|---|---|
| listed data elements. | | | |
| 6.0.1.5. Specific test, specialized test instrumentation or equipment. | | | |
| 6.0.2. Unanalyzed test data. | | | |
| 6.0.3. Analyzed test data | | | |
| **7.0 TRAINING** | | | |
| 7.0.1 Identification and/or location of training specific to *program* | | | |
| 7.0.2 Training that reveals specific system information (e.g., design, development, capabilities, vulnerabilities, etc.) | | | |
| **8.0 MAINTENANCE** | | | |
| 8.0.1 Identification and/or location of specialized maintenance organizations associated with *program* | | | |
| 8.0.2 Association of maintenance equipment or tools that may reveal specific system information | | | |
| 8.0.3 Maintenance that reveals specific system information (e.g., design, development, capabilities, vulnerabilities, etc.) | | | |
| 8.0.4. Field level Maintenance | | | |
| 8.0.5. Intermediate level Maintenance | | | |
| 8.0.6. Depot level Maintenance | | | |