Security Classification Guidance

Lesson: Course Introduction

Course Information

Welcome to the Security Classification Guidance Course.

Purpose: Provide an understanding of security classification and declassification guidance to personnel performing classification and declassification actions

Audience: DoD military, civilian, and contractor personnel with a functional knowledge of the DoD Information Security Program

Course Overview

The safety and security of the United States depends on the ability to adequately protect classified information.

When an Original Classification Authority, or OCA, determines that information must be classified, he or she must also develop security classification guidance to communicate that determination to others.

Developing clear and precise security classification guidance is critical because it ensures that all users of the information treat it consistently and protect it properly.

In this course, you will learn about the process of developing security classification guidance; that is, the policy documents that govern its creation, the different types of guidance, the classification determination itself, and specifically, how to develop each type of guidance, including declassification guides.

Course Objectives

Here are the course objectives. Take a moment to review them.

Course Objectives

- Identify the policy documents that govern the development of security classification guidance
- Identify the types of security classification guidance
- Identify the classification determination process
- Identify the principles of developing security classification guidance
- Identify the process of developing declassification guidance

Course Structure

This course is organized into the lessons listed here.

Lessons

- Course Introduction
- Security Classification Guidance Overview
- Classification Guidance Development Process
- Developing Security Classification Guidance
- Developing Declassification Guidance
- Course Conclusion

Lesson: Security Classification Guidance Overview

Lesson Introduction

It is vital in the protection of our national security to properly develop classification guidance and communicate the decisions.

This guidance can come in different forms, but both of them facilitate comprehensive, relevant, and concise classification guidance by authorized officials. They are issued to communicate classification determinations effectively and efficiently.

In this lesson, you will learn the definition and purpose of security classification guidance, the policy documents that govern its development, and the different types of classification guidance.

Purpose

Security classification guidance is any instruction or source that sets out the classification of a system, plan, program, mission, or project.

It is initially issued by Original Classification Authorities, or OCAs, to document and disseminate classification decisions under their jurisdiction.

The purpose of security classification guidance is to communicate classification decisions, promote uniform derivative classification and consistent application of classification decisions to all users of the relevant information.

This is critical to ensure all users of the information are applying the same level of protection, for the same information, and for the same duration.

Finally, it helps ensure that classified information receives the required level of protection when making derivative classification decisions.

National Policy

The foundation of national policy for classified information is Executive Order 13526, Classified National Security Information.

This Executive Order prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information that relates to defense against transnational terrorism.

The Executive Order directs the Information Security Oversight Office (ISOO) under the direction of the National Archives, to develop implementing guidance.

They issued ISOO, 32 CFR Parts 2001 and 2003, Classified National Security Information; Final

Rule, which sets forth more specific guidance to agencies on the implementation of the Executive Order. It addresses security classification guidance.

Based on this national policy, the Department of Defense (DoD) has issued its own implementing guidance.

Sec. 2001.15: Classification Guides:
- Preparation
- Content
- Dissemination
- Reviews/updates

DoD Policy

The DoD has implemented national policy guidance on classified information in several documents.

DoD Instruction 5200.01, DoD Information Security Program and Protection of Sensitive Compartmented Information, or SCI, establishes the general framework and responsibilities for DoD implementation of national policy on classified national security information.

It authorizes the publication of DoD Manual 5200.01, Volume 1 through 3, DoD Information Security Program, which prescribe the defined procedures for the DoD Information Security Program.

These manuals contain the requirements and minimum standards for developing classification guidance.

Another key DoD resource for developing security classification guidance is DoDM 5200.45, Instructions for Developing Security Classification Guides. This manual provides detailed information on how to develop security classification guidance. All of these DoD resources address the protection of classified information at the Confidential, Secret, and Top Secret levels.

Overview

There are two authorized methods used to communicate classification decisions. They are, in order of preference, a Security Classification Guide, or SCG, and a properly marked source document. This course will address developing both types of guidance. Let's look at each one in more detail.

Derivative Classifier rollover text: A derivative classifier is any cleared DoD and authorized contractor personnel who generates material from sources which are already classified.

OCA rollover text: An original classification authority, OCA, is a senior government

official who is granted the authority to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security.

SCG

The preferred method for communicating an original classification decision is through a security classification guide, or SCG.

An SCG is a collection of precise decisions and comprehensive guidance regarding a specific system, plan, program, mission, or project.

SCGs allow the OCA to identify specific items or elements requiring classification, the exact classification levels assigned, reason for classification, applicable downgrading and declassification instructions, any special handling caveats or dissemination controls, identity and position of the classifier and a point of contact for questions and/or suggestions regarding the SCG.

Properly Marked Source Document

The other preferred method for disseminating classification guidance is through a properly marked source document. A properly marked source document may be either an originally classified document or a derivatively classified document developed from an original source.

Using this method provides guidance in some form including, but not limited to, a memorandum, plan, message document, letter, or an order. Classification guidance could be issued through one or all of these sources.

document rollover text: Any physical medium in or on which information is recorded or stored, to include written or printed matter, audiovisual materials, and electromagnetic storage material

Review Activity 1

What is the purpose of classification guidance?

What is the purpose of security classification guidance?

- □ To ensure sensitive information receives adequate protection
- □ To communicate classification decisions
- □ To inform OCAs and derivative classifiers when they should classify information
- □ To ensure that users of classified information treat it consistently

Answer: To ensure sensitive information receives adequate protection; To communicate classification decisions; To ensure that users of classified information treat it consistently

Review Activity 2

Now try this series of questions.

Question 1 of 4:
Which policy document prescribes a uniform system for classifying, safeguarding, and declassifying national security information?

- ISOO, 32 CFR Parts 2001 and 2003, Classified National Security Information; Final Rule
- DoD Manual 5200.01, Volumes 1-3, DoD Information Security Program
- E.O. 13526, Classified National Security Information
- DoD Instruction 5200.01, DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)

Answer: E.O. 13526, Classified National Security Information

Question 2 of 4:
Which policy document provides a high-level framework for DoD implementation of national policy on classified national security information?

- ISOO, 32 CFR Parts 2001 and 2003, Classified National Security Information, Final Rule
- DoD Manual 5200.01, Volumes 1-3, DoD Information Security Program
- E.O. 13526, Classified National Security Information
- DoD Instruction 5200.01, DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)

Answer: DoD Instruction 5200.01, DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)

Question 3 of 4:
Which policy document provides guidance to all government agencies on classification, downgrading, declassification, and safeguarding of classified national security information?

- ISOO, 32 CFR Parts 2001 and 2003, Classified National Security Information; Final Rule
- DoD Manual 5200.01, Volumes 1-3, DoD Information Security Program
- E.O. 13526, Classified National Security Information
- DoD Instruction 5200.01, DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)

Answer: ISOO, 32 CFR Parts 2001 and 2003, Classified National Security Information; Final Rule

Question 4 of 4:
Which policy document provides detailed information on how to develop security classification guidance?

- ISOO, 32 CFR Parts 2001 and 2003, Classified National Security Information; Final Rule
- DoD Manual 5200.45, Instructions for Developing Security Classification Guidance
- E.O. 13526, Classified National Security Information
- DoD Instruction Manual 5200.01, DoD Information Security Program and Protection of

Sensitive Compartmented Information (SCI)

Answer: DoD Manual 5200.45, Instructions for Developing Security Classification Guidance

Review Activity 3

Which of the following provides classification guidance in the form of a memorandum, plan, message document, letter or order?

- Properly marked source document
- Security Declassification Guide
- Distribution statements
- Security Classification Guide (SCG)

Answer: Properly marked source document

Review Activity 4

Do you know the primary authorized source of classification guidance?

What is the primary source of security classification guidance?

- Security Classification Guide
- An OCA's official notes
- Your memory
- A properly marked source document

Answer: Security Classification Guide

Summary

You have completed the Security Classification Guidance Overview lesson.

Lesson: Classification Guidance Development Process

Introduction

When an Original Classification Authority, or OCA, sets out to determine whether information is classified, there is a specific process he or she needs to follow.

Having such a process ensures that classification decisions are made systematically, efficiently, and effectively.

In this lesson you will learn about the considerations an OCA takes into account before making a classification determination, and the specific process an OCA follows in making that determination. The end result, of course, is communicating the classification decision by documenting the determination in an authorized form of security classification guidance.

Here is the lesson objective. Take a moment to review it.

Lesson Objective:

- Identify the process for developing security classification guidance

Who Issues Security Classification Guidance?

Original security classification guidance is issued by OCAs and carried forward by derivative classifiers.

OCAs create this guidance through issuance of security classification or declassification guides, or a properly marked source document. If the guidance is issued outside of a security classification or declassification guide, it should be incorporated into a guide in a timely manner.

Derivative classifiers take the OCAs' original classification guidance and derivatively classify information. This may be in the form of a properly marked source document.

> **OCA's MORE button:** Because their decisions have such an impact, OCAs are senior government officials only, contractors are prohibited from being an OCA. The government grants the authority to originally classify information only when there is a "demonstrable and continuing need" for such authority. That is, there must be a justifiable requirement to perform original classification, and that need must be expected to last over time.
>
> In addition, in order for an individual to exercise original classification authority, he or she must have the appropriate level of security clearance. The individual must also have sufficient expertise in the relevant subject matter to ensure the validity of his or her classification decisions. There are specific positions in the Department of Defense, or DoD, with original classification authority. This authority may be delegated only in specific circumstances. It is also important to remember that original classification authority is tied to a position and not the individual occupying the position. Once an

individual leaves a position designated as an OCA, that person no longer has original classification authority.

DoD positions with original classification authority:

- Secretary of Defense
- Secretaries of the Military Departments
  - Secretary of the Army
  - Secretary of the Navy
  - Secretary of the Air Force
- Officials specifically delegated original classification authority in writing

OCAs MORE button: Conditions on delegation of original classification authority:

- Delegations of original classification authority are limited to the minimum number required for effective operation of the DoD
- Delegations of original classification authority must be made only to officials with a demonstrable and continuing need to exercise it
- Individuals delegated to exercise original classification authority must receive training as required by DoDM 5200.01, Volume 3, DoD Information Security Program (Enclosure 5: Security Education and Training)

Derivative Classifiers MORE button: Derivative classification is the process of using existing classified information to create new material and marking that newly developed material consistent with the classification markings that apply to the source information. The individuals who perform derivative classification are known as derivative classifiers. In contrast to original classification, there are a great many individuals who derivatively classify information.

Who does it?

- All DoD and authorized contractor personnel who generate or create material from classified sources

Classification of Broad Aspects of an Effort

There are some key considerations an OCA needs to take into account early in the classification determination process.

One is whether there is already existing guidance that relates to the information in question. Another factor is how new and unique the state of the art information or item is. Finally, the OCA should consider whether classifying the item or information would result in a net national advantage for the United States.

If this early analysis indicates that broad aspects of the effort warrant classification, the OCA can move on to consider specific details of the effort and their individual classification. If not, the classification determination ceases. Let's examine each factor in more detail to see how the factors play into the classification determination.

Early considerations in the classification determination process:

- Is there pre-existing security classification guidance?
- What is the state-of-the-art of the information or item?
- Will classification result in a net national advantage?

Pre-Existing Guidance

As early as possible in the classification process, it is necessary to check whether there is any existing classification guidance that applies to the item or information that is the subject of the determination.

Exercising classification authority in a uniform and consistent manner is essential, and researching existing guidance is a key part of that effort.

In some cases, there are existing guides that apply to a broad spectrum of systems, plans, programs, missions, and projects. In other cases, there may be specific guidance covering the same classifiable information. There are a variety of resources available to assist in this process.

Many Security Classification guides, or SCGs, are available from an online accessible database maintained by the Defense Technical Information Center, or DTIC. Some SCGs, however, due to the sensitivity of the information, may be classified.

In addition, there may be relevant SCGs issued along functional lines by activities outside the DoD. For this reason, always check with Component Headquarters in addition to consulting the index before writing an SCG to ensure that applicable guidance does not already exist.

DITC rollover text: Defense Technical Information Center

State-of-the-Art

In scientific and technical fields, classification determinations must take into account the state-of-the-art status of the information under consideration. That is, what has already been accomplished, what is being attempted by the effort under consideration, and by whom?

For example, a brand new technology that no one in the world knows about would be considered state-of-the-art. Classifying this kind of information will prevent enemies from developing countermeasures to combat it. In addition, information can be added to existing ideas and concepts that will make them state-of-the-art.

In order to assess state-of-the-art, it is critical to consult with scientific and technical information experts, as well as intelligence specialists. Department of Defense Manual, or DoDM, 5200.45 lists some factors that relate to state-of-the-art.

State-of-the-Art Factors popup: Factors to consider when assessing state-of-the-art status include the state-of-the-art itself, the state of development, the level

of attainment in the field of work, and what is known and openly published about it. This last consideration has several aspects. Is the information known or published either in the U.S. or abroad? If information is already in the public eye, for example, on the Internet, in books or in movies, it may need to be reexamined to determine if it meets the criteria for classification.

If the information is not published, is it known in the U.S.?

Is it known in friendly and unfriendly countries?

And what is the extent of foreign knowledge of the information's unpublished status in the U.S.?

These considerations relate to whether it is worthwhile and feasible to protect the information.

Examples popup:

State-of-the-art deals primarily with today's weapons systems, but also applies to information that reveals capabilities and vulnerabilities of legacy weapons systems when this would impair a current U.S. weapons system:

- U.S. detection capabilities still in use and remaining vulnerable to detection, denial or deception, and spoofing
- In-depth scientific or engineering analysis or description of a state-of-the-art weapons system
- National and military command, control, and communications systems that are still in use
- Average values, variations and tolerances for sensitivity, timing, or other factors affecting the response of a state-of-the-art weapons system firing mechanism
- Countermeasures recommended for use against a state-of-the-art weapons system
- Recommended operational adjustments and tactics
- Maximum life of a state-of-the-art weapons system
- Operational information concerning the firing mechanisms
- Signatures (acoustic, seismic, infrared, radar, etc.) and procedures and techniques for signature reduction or mitigation
- Theory of operation/function, performance parameters and limitations, countermeasure susceptibility or counter-countermeasures capabilities
- Transmission security designs
- Special deception devices and techniques

Net National Advantage

Another factor that plays into the early stages of classification determination is whether classifying the information or items under consideration will result in a net national advantage for the United States. If so, then that fact supports the decision to classify the information or

items.
In assessing net national advantage, an OCA must reflect on what value, direct or indirect, would accrue or be expected to accrue to the U.S. as a result of classifying the information under consideration. DoDM 5200.45 lists some factors that relate to net national advantage.

Net National Advantage Factors popup: There are many factors that might provide the U.S. with a net national advantage. An OCA needs to carefully consider these and others when assessing whether broad aspects of an effort warrant classification. These factors fall into some basic categories. For example, what interest does the U.S. government have in the effort?

What characteristics of the item or information, if they are not disclosed, would provide value to the U.S.?

What details about the item's production would provide an advantage to the U.S. if they were not revealed?

Factors to consider in assessing net national advantage:

U.S. Government interest:

- Fact of interest by the U.S. Government in the particular effort as a whole or in specific parts that are being considered or emphasized
- Fact of possession of the information by the U.S. Government

Characteristics of the item/information:

- Capabilities of the resulting product in terms of quality, quantity, and location
- Performance, including operational performance, as it relates to capabilities
- Vulnerabilities, weaknesses, countermeasures, and counter-countermeasures
- Uniqueness (i.e., exclusive U.S. knowledge)
- Surprise (related to possession and capability to use)

Production characteristics:

- Lead time, related to state-of-the-art
- Specifications (may be indicative of goals, aims, or achievements)
- Manufacturing technology
- Associations with other data or activities

Specific Item Classification

Once preliminary analysis indicates that broad aspects of the effort under consideration warrant classification, the next step is to consider the classification of certain specific details of the effort.

DoDM 5200.45 contains information about the relevant factors in this phase of the determination.

Broad aspects of the effort warrant classification:

- No pre-existing guidance
- State-of-the-art
- Net national advantage

Original Classification Process

OCAs must follow a process known as the original classification process to determine the classification, level, and duration for each specific item of information that may require classification.

This process is organized into six distinct steps the OCA follows when making an original classification determination. At each step, if the information does not meet the criteria for becoming classified, the process must terminate, and the OCA cannot classify the information.

For an in-depth knowledge of the original classification process, refer to the Original Classification eLearning course offered by the Center for Development of Security Excellence or CDSE.

The CDSE OCA Desk Reference Guide is also available for step-by-step guidance through the process.

Original Classification Authority Lesson:
To ensure they make effective classification decisions, OCAs must follow a standard process. CDSE packaged the standard process into six digestible steps. The six-step process takes different elements info account at different stages of the process. In this lesson you will learn how OCAs reach their classification decisions.

Six-Step Process for Original Classification

Step 6 – Guidance
Step 5 – Duration
Step 4 – Classification Level
Step 3 – Impact
Step 2 – Eligibility
Step 1 – Government Information

CDSE rollover: Center for Development of Security Excellence

Step 1 – Government Information

Since the OCA must be the only one to classify the information, the OCA must first determine whether the information is official. This means the information must be owned by, produced by or for, or under the control of the U.S. Government. If the government does not have any ownership interest in or control of the information, it cannot be classified, regardless of how

sensitive it might be.

OCA rollover: Original Classification Authority

Owned by rollover: "Owned by" is information that belongs to the U.S. Government.

Produced by rollover: "Produced by" is government-developed information. "Produced for" is when the government enters into an agreement through purchase, lease, contract, or receipt of the information as a gift. It covers situations in which the government uses a contractor.

Under the control rollover: "Under the control" is the authority of the originating agency to regulate access to the information. The contractor, inventor, etc., agrees to have the U.S. Government place it under their control so that the information is eligible for protection through classification. The contractor still retains ownership but has entrusted the information to the U.S. Government.

Step 2 – Eligibility

Next, the OCA must determine whether the information is eligible to be classified. This determination actually involves four parts.

First, the OCA has to analyze whether the information is eligible for classification.

Second, the OCA needs to assess whether there are any prohibitions or limitations on classifying it.

Third, the OCA must determine if the information has already been classified by another OCA.

Finally, the OCA must determine if classification already exists. Executive Order 13526 identifies eight categories of information that are eligible for classification.

These categories are fairly broad and general in scope.

Exists rollover: Determine that classification guidance is not already available in the form of SCGs, plans, or other memorandums

Limitations rollover: Limitations on classification apply to the following types of information:

- Basic scientific research information not clearly related to

national security
- Information that has been declassified and released to the public may be reclassified only under specific conditions
- Information not previously disclosed to the public may be classified or reclassified only in certain cases

Prohibitions rollover: Information may not be classified, continue to be maintained as classified, or fail to be declassified in order to:
- Conceal violations of law, inefficiency, or administrative error
- Prevent embarrassment to a person, organization, or agency
- Restrain competition
- Prevent or delay the release of information that does not require protection in the interest of national security

MORE popup:

These are the eight categories of information eligible for classification:
1. Military plans, weapons systems, or operations
2. Foreign government information (FGI)
3. Intelligence activities (including covert action), intelligence sources or methods, or cryptology
4. Foreign relations or foreign activities of the United States, including confidential sources
5. Scientific, technological, or economic matters relating to national security
6. U.S. Government programs for safeguarding nuclear materials or facilities
7. Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to national security
8. The development, production, or use of weapons of mass destruction

Step 3: Impact

In Step 3, the OCA has to assess the impact to national security if unauthorized disclosure occurs. The first part of this assessment is to evaluate the potential for damage to national security if unauthorized disclosure of the information occurs. The OCA also needs to examine whether there is a reasonable possibility of protecting the information from unauthorized disclosure. Finally, the OCA must also consider other costs of classifying the information, including operational and technological factors, and how it would impact resources.

Once an OCA determines that the need to protect the information justifies the effort and cost of protecting it, he or she can decide to classify the information.

Step 4: Classification Level

Once the OCA has decided to classify the information, the next step is to determine the appropriate level of classification. This involves determining how sensitive the information is,

and what the potential damage to national security is if the information were not protected. Based on the sensitivity of the information, and the potential harm to national security, the OCA will proceed to assign a classification level to the information. The United States uses three classification levels: Top Secret, Secret and Confidential. Each level is defined in relation to the potential for damage to the national security.

The OCA must look at the damage criteria and decide the appropriate level of classification.

Confidential rollover: Confidential information is information or material of which unauthorized disclosure could reasonably be expected to cause **damage** to the national security that the Original Classification Authority is able to identify or describe.

Secret rollover: Secret information is information or material of which unauthorized disclosure could reasonably be expected to cause **serious damage** to the national security that the Original Classification Authority is able to identify or describe.

Top Secret rollover: Top Secret information is information or material of which unauthorized disclosure could reasonably be expected to cause **exceptionally grave damage** to the national security that the Original Classification Authority is able to identify or describe.

Step 5: Duration

After determining the level of classification, the OCA must decide how long the information will remain classified, and at what level. This involves two considerations. The first is downgrading. The OCA must review the information and its classification level to assess whether it can be lowered, or downgraded, in the future.

The second is declassification. This is a determination made by the OCA of how long the classification of the information will remain in effect.

An important fact to remember is that no information may remain classified indefinitely.

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

Downgrading rollover: A determination that information classified at one level will have its classification reduced to a lower level on a specific date or event

Step 6: Guidance

The final step in the original classification decision process is to designate the information as classified and communicate that decision to individuals who use the information.

There are two authorized methods for communicating classification decisions. The primary method for OCAs is a security classification guide, or SCG. This is the preferred method issued for classification guidance. However, at times a properly marked source document may be used to disseminate classification guidance. This may occur in emergency situations or when limited classification determinations are required, not warranting a formal SCG.

If the classification guidance is issued outside of a security classification or declassification guide, it should be incorporated into a guide in a timely fashion.

Writing Security Classification Guidance

Once an OCA has determined exactly what specific items warrant security classification, he or she must proceed with documenting that classification decision.

When an original classifier issues the guidance, the security classification guidance should contain precise language describing which items require classification, so that the guidance is easy for users to follow consistently. In addition, it is important for guidance to include items that are unclassified to assure users that these items are indeed unclassified and were not inadvertently omitted from the guidance.

The next lesson in this course will go into greater detail about how to write each type of guidance.

Review Activity 1

Who may issue original security classification guidance?

- All cleared DoD officials
- Only DoD officials with original classification authority
- Derivative and original classifiers
- Contractors and DoD officials with original classification authority

Answer: Only DoD officials with original classification authority

Review Activity 2

Which of the following factors relate to state-of-the-art?

- □ Is the information known in other countries?
- □ Will the U.S accrue direct or indirect value by classifying the information?
- □ Is protecting the information feasible?

- □ What has already been accomplished in the field?
- □ What is the opinion of technical experts in the field?
- □ Has the information been published?

Answer: Is the information known in other countries?; What has already been accomplished in the field?; What is the opinion of technical experts in the field?; Has the information been published?

Review Activity 3

Which statement best describes net national advantage?

- o Information under control of the U.S. Government that would cause serious damage to national security if released
- o Unpublished information known only by individuals in the U.S.
- o Information for which the benefits of classification outweigh the costs
- o Information that is or will be valuable to the U.S., either directly or indirectly

Answer: Information that is or will be valuable to the U.S., either directly or indirectly

Review Activity 4

How well do you know the original classification process?

What are the costs of classifying the information?
Step 3 – Impact

Is there a date when the classification level of information may be downgraded?
Step 5 – Duration

What is the best way to disseminate the classification decision?
Step 6 – Guidance

Is the information official?
Step 1 – Government Information

Are there any prohibitions on classification?
Step 2 – Eligibility

How sensitive is the information?
Step 4 – Designate Classification Level

Summary

You have completed the Classification Guidance Development Process lesson.

Lesson: Developing Classification Guidance

Introduction

When an Original Classification Authority, or OCA, makes a determination that information warrants security classification, or when a Derivative Classifier carries that classification determination forward, he or she must develop guidance to communicate the classification to others. The developed guidance must be clear and concise and follow a consistent format. This ensures that users of the information treat it consistently and protect it properly.

In this lesson, you will learn about how to develop the different types of classification guidance. You will learn about the elements each must contain and the publishing requirements for each. Here are the lesson objectives.

Lesson Objectives:
- Identify the required content for each type of classification guidance
- Identify the requirements for publishing each type of classification guidance

Overview

Security classification guides, or SCGs, are a written record of an original classification decision. They are issued by an OCA to provide comprehensive guidance regarding specific systems, plans, programs, missions, or projects.

To maximize usability for the greatest number of individuals, the guides should be unclassified. Even so, they generally qualify as Controlled Unclassified Information, or CUI, and must be protected as such. For some programs, however, they may need to be classified and must be handled and safeguarded accordingly.

Required Content

The Information Security Oversight Office, or ISOO, published 32 CFR, Parts 2001 and 2003, Classified National Security Information; Final Rule. This policy document includes specific requirements on the content of security classification guides. SCGs must identify the subject matter, the OCA and the agency point of contact, and the date of approval or last review.

The heart of a classification guide is the identification and delineation of the specific items or elements of information warranting protection, the classification levels, reasons for classification, and the duration of classification. The guide must prescribe applicable warning and handling notices, dissemination controls and declassification instructions, and must be marked with a distribution statement.

OCA rollover: Original Classification Authority
POC rollover: Point of Contact

DoD Instruction 5230.24 popup: A distribution statement indicates the extent of availability for distribution, release, and disclosure without additional approvals and authorizations from the Controlling DoD Office (CDO).

Distribution statements include four critical pieces of information:

- Authorized audience
- Reason for restriction
- Identity of the CDO
- Date of publication

The DoD Instruction 5230.24, Distribution Statements on Technical Documents provides guidance on the requirements and use of distribution statements.

Cover Page

The SCG should include a cover page with the following information; the name of the system, plan, program, mission, or project; the date; the office issuing the guide; the OCA approving the guide; a statement of supersession, if necessary, and a distribution statement.

Recommended Format

DoDM 5200.45, Instructions for Developing Security Classification Guides, is the primary source of "how-to" information about developing classification guidance. This manual recommends that SCGs contain these sections. Guides should include only the sections actually needed based on the subject matter of the guide.

- Section 1: General Instructions
- Section 2: Overall Effort
- Section 3: Performance and Capabilities
- Section 4: Specifications
- Section 5: Critical Elements
- Section 6: Vulnerabilities and Weaknesses
- Section 7: Administrative Data
- Section 8: Hardware

Section 1: General Instructions

The General Instructions section covers the instructions and administrative guidance for the system, plan, program, mission, or project. The section describes the guide's purpose, the issuing authority, and the office of primary responsibility.

The General Instructions section also contains instructions for challenging the classification guidance; reproducing, extracting, and disseminating the guidance; requesting release of its information to the public; and disclosing the information to foreign officials. If foreign disclosure

is prohibited, note it is in this section.

Finally, any definitions needing clarification should be included in the General Instructions.

View Recommended Language pop up:

Section 1: General Information Recommended Language
Section 1 includes:

- Purpose
- Authority
- Office of Primary Responsibility (OPR)
- Classification Challenges
- Reproduction, Extraction, and Dissemination
- Public Release
- Foreign Disclosure
- Definitions

Purpose rollover: "To provide instructions and guidance on the classification of information involved in [name of the system, plan, program, mission, or project] using an unclassified identification of the effort."

Authority rollover: "This guide is issued under authority of [state any applicable departmental or agency regulations authorizing or controlling the issuance of guides, such as DoDM 5200.01]. Classification of information involved in [identify the effort] is governed by, and is in accordance with, [cite any applicable classification guidance or guides under which this guide is issued]. This guide constitutes authority, and may be cited as the basis for classification, regrading, or declassification of information and material involved in [identify the effort]. Changes in classification required by application of this guide shall be made immediately. Information identified in this guide for protection as classified information is classified by [complete title or position of classifying authority]."

Office of Primary Responsibility rollover: "This guide is issued by, and all inquiries concerning content and interpretation, as well as any recommendations for changes, should be addressed to: [Name, code, mailing address of issuing office.]"

Note: An administrative or security office in the issuing activity may be used. Inclusion of the action officer's name, phone or fax number, and e-mail is recommended.

Classification Challenges rollover:

"If at any time, any of the security classification guidance contained herein is challenged, the items of information involved shall continue to be protected at the level prescribed by this guide until such time as a final decision is made on the challenge by appropriate authority. Classification challenges should be addressed to the OPR."

Reproduction, Extraction, and Dissemination rollover:

"Authorized recipients of this guide may reproduce, extract, and disseminate the contents of this guide, as necessary, for application by specified groups involved in [identification of the effort], including industrial activities. Copies of separate guides issued to operating activities in application of this guide shall be sent to the OPR."

Note: If it is necessary to classify the guide, this paragraph may need to be modified to express any required limitations.

Public Release rollover:

"The fact that this guide shows certain details of information to be unclassified, including controlled unclassified information, does not allow automatic public release of this information. DoD information requested by the media or members of the public or proposed for release to the public by DoD civilians or military personnel or their contractors shall be processed in accordance with DoD Manual 5200.01, DoD Instruction 5230.09, DoD Instruction 5230.29, and DoDM 5400.07, as applicable. Proposed public disclosures of unclassified information regarding [identification of effort] shall be processed through [identify office to which requests for public disclosure are to be sent and provide contact information."

Note: Where the specific office cannot be identified, state that requests should be processed through "appropriate channels for approval."

Foreign Disclosure rollover:

"Any disclosure to foreign officials of information classified by this guide shall be in accordance with the procedures set forth in [identify applicable issuances implementing DoD foreign disclosure policy, e.g., DoD Directive 5230.11]. If a country with which the DoD has

entered into a reciprocal procurement memorandum of understanding or offset arrangement, expresses an interest in this effort, a foreign disclosure review should be conducted prior to issuance of a solicitation."

Note: If it is known that foreign participation cannot be permitted because of the sensitivity of the effort, this fact should be stated. Add other guidance as appropriate.

Definitions rollover: "Include in this paragraph the definitions of any items for which there may be various meanings to ensure common understanding of the details of information that are covered by the guide."

Section 2: Overall Effort

The Overall Effort section describes the classification effort itself. The section identifies the item being classified, states the reason for classification, and describes what is being protected by classifying the information – for example, it might be actual hardware, or it might be paperwork that is being protected.

Section 2: Overall Effort
Provides information on the classification effort itself for the system, plan, program, mission, or project.

Section 2 includes:

- Identification
- Goal, Mission, Purpose
- End Item

Identification rollover: Include in this paragraph:

- Any necessary statements explaining the classifications, if any, to be assigned to various statements identifying the effort
- Statements consistent with other program documentation

Goal, Mission Purpose rollover: Include in this paragraph:

- Any necessary statements identifying information concerning the purpose of the effort that can be released as unclassified and that must be classified
- Only unclassified statements that do not reveal classified information

End Item rollover: Include in this paragraph:

- Statements of the classification to be assigned to the end products of the effort, whether paperwork or hardware
- Statements that distinguish between classification required to protect the knowledge of the existence of a completed end item and classification required because of what the end item contains or reveals
    - In some instances, classified information pertaining to the performance, manufacture, or composition of incorporated parts or materials is not ascertainable from mere use of or access to the end item. In others, the classifiable information is that which concerns the total performance, capabilities, vulnerabilities, or weaknesses of the end item itself, rather than any of the parts or materials.

Section 3: Performance and Capabilities

The Performance and Capabilities section is the key section of the classification guide. The section takes the item that is classified and breaks down what specifically is classified in terms of the item's performance and capabilities. For example, if the item being classified is a radar, performance and capability characteristics may include the radar's range and operational altitude and information about the radar's receiver. The performance and capability characteristics are listed and sequentially numbered along with their classification, declassification date, and any remarks.

TOPIC	CLASS	DECLASSIFY ON	REMARKS
1. Range			
a. Actual	"S"	20140615	
b. Planned	"U"		
2. Altitude Operational	"C"	20150130	
Maximum	"C"	20150130	The statement "in excess of 50,000 feet" is "U"
3. Receiver sensitivity, selectivity, and frequency coverage	"S"	20200415	If standard commercial receivers are used, their characteristics are "U" but their application to this effort shall be "S"

Section 3 rollover: "This section includes characteristics of performance and capability of an end item, or an end item's components, parts, or materials, the performance or capabilities of which require classification. In this section also provide, in sequentially numbered items, statements that express details of performance and capabilities planned and actual. Include both those elements that warrant classification and

those that are unclassified. These statements normally would not set forth the numeric values that indicate degree of performance or capability, planned or attained, but merely should identify the specific elements of performance or capability that are covered. When it is necessary to state certain limiting figures above or below which classification is required, the statement itself may warrant classification. For clarity, continuity, or ease of reference it may be desirable to include performance classification data in the sections dealing with the end item or the components or parts to which the performance data apply. Use a "Remarks" column for explanations, limitations, special conditions, associations, etc., as shown."

Section 4: Specifications

The Specifications section details the physical components that make up the classified item. The item that is classified is broken down to what specifically is classified in terms of the item's materials and parts; method of construction, manufacture, or assembly; and specific dimensions – including size, form, shape, and weight.

Each specification is listed and sequentially numbered along with its classification, declassification date, and any remarks. Note that both classified and unclassified elements are included in the guidance.

Section 4: Specifications
Provides information on the physical components and assembly of the system, plan, program, mission, or project.

TOPIC	CLASS	DECLASSIFY ON	REMARKS
1. Burn Rate	"C"	20160917	
2. Power requirements	"S"	20160917	Only when associated with advanced model ##, otherwise "U"
3. Chemical composition	"U"		

View Recommended Language popup:

Use the following paragraph, or a similar one, for the Specifications section of security classification guides:

"This section includes items of information describing standards for [qualities of materials and parts; methods or modes or construction, manufacture or assembly; and specific dimensions in size, form, shape, and weight that require classification]. Inclusion in this section is required because the items require classification because they

contribute to the national security advantage resulting from this effort, or because they frequently require classification but are unclassified in [identification of this effort]. Classification of specifications pertaining to performance and capability are covered in section 3 of the guide."

Note: Actual figures do not need to be given, merely statements identifying clearly the specific items of information involved. If figures are necessary to establish classification levels, it may be necessary to classify the statements themselves. When necessary for clarity, continuity or ease of reference, specification classification data may be included in sections on the end product or components or parts to which the data apply. Use a "Remarks" column for explanations, limitations, special conditions, associations, etc.

Section 5: Critical Elements

The Critical Elements section is used only when there are specific critical components that need to be called out separately because of their uniqueness and importance to the overall classified item. For example, computer chips with safe-fail components which eliminate the shutdown of an entire system or a radar that is an integral component of a weapons system would be considered critical components.

List each critical element along with its classification. Include classification of components, parts, and materials and any relevant performance data.

Note that the items listed under Critical Elements do not need to also be listed in the Performance and Capabilities and Specifications sections of the guide.

Section 6: Vulnerabilities and Weaknesses

The Vulnerabilities and Weaknesses section provides details on any information that shows weakness or vulnerability in the classified item. For example, the fact that your program's weapon system can be defeated by another is a vulnerability that would be included in this section.

The vulnerabilities and weaknesses are classified to protect against exploitation. The countermeasures used to protect against exploitation are also classified.

Section 6: Vulnerabilities and Weaknesses
Provides information on the **vulnerabilities and weaknesses** of the system, plan, program, or project and the **applicable countermeasures** taken to mitigate the potential risks.

Section 6 rollover: "This section is used to specify classification to be assigned to details of information that disclose inherent weaknesses that could be exploited to defeat or minimize the effectiveness of the end product of this effort. Classification assigned to details of information on countermeasures and counter-countermeasures should also be included in this section."

Section 7: Administrative Data

The Administrative Data section is used only when particular elements of administrative data warrant classification.

For example, program information, procurement schedules, production quantities, schedules, programs, status of the effort, manuals, training, and data on shipments, deployment, or transportation may require classification and inclusion in the guide. The reason for classification must appear in the SCG, either in the Administrative Data section, or in individual tables.

List each administrative item along with its classification, declassification date, and any remarks.

TOPIC	CLASS	DECLASSIFY ON	REMARKS
1. Planned delivery rate	"C"	20160313	See Item 3, below
2. Actual routing of delivery of end terms	"C"	See remarks	Classify upon selection of route and declassify upon completion of last delivery to site.
3. Shipping dates and times	"C"	See remarks	Classify upon decision to ship and declassify upon arrival at site.

Section 8: Hardware

The Hardware section describes the hardware elements that comprise the classified item or hardware that is used by the item. It includes both end item hardware and hardware components.

The classification for each end item and component is listed, along with the declassification date, and any remarks. When you write the Hardware section of a classification guide, there are several factors to consider when determining the level of detail to include.

INFORMATION REVEALING	CLASS	DECLASSIFY ON	REMARKS
End item hardware:			
a. AN/APR-999	"C"	20150820	External views of the assembled AN/APR-999
(1) Analyzer unit	"C"	20150820	
(2) Threat display unit	"U"		
(3) Preamplifier	"U"		
b. AN/APR-0000	"U"		

Level of Detail popup:

Consider the following factors. First is the level from which the guide is issued. For example, classification issued from the headquarters level will likely apply to the end item itself. Second is the channels the guidance travels through to reach the user. Does the guide travel to reach the user? The closer the issuer is to the user, the more detailed the guidance may become.

Third is the ease of determining when classified information could be revealed by a particular hardware item. It's important to obscure any connections and associations the items may have. Finally, there are the factors that require consideration and action at a headquarters level in case there is information that would normally not be available to below the headquarters level.

More popup:

The level from which issued: When issued from a headquarters level, the classification is most likely to be applied to the hardware end item itself, rather than its individual components.

The channels or hands through which the guidance will travel to the ultimate user: is removed from the user, intermediate levels of guidance may be required to expand or elaborate on the guidance provided by the basic classification guide and to cover more details concerning materials, parts, components, assemblies, and subassemblies, and the classification, if any, to be assigned. Any such expansion or elaboration should be fully coordinated with the headquarters issuing the basic guide.

The ease of determining when classified information could be revealed by a particular hardware item: Obscure connections and associations that could reveal classified information may require the issuer of the guide to state the classification for certain hardware items. In such cases, it would probably be advisable to explain why classification is necessary.

Whether there are factors that require consideration and action at a headquarters level: National or DoD policy, intelligence data, broad operational requirements, extraneous factors, or other matters not ordinarily available below headquarters, or that require high level consideration may result in decisions to classify certain hardware items.

Classifying Specific Types of Information

When developing SCGs, there are specific types of information you must consider. This includes hardware items, military operations, intelligence, and foreign relations information. In these cases, it is important that you consult DoDM 5200.45 to ensure you are considering the essential factors for each.

Hardware
Classify **only** if it reveals information or information can be obtained from it

Military Operations
Classify information that:

- Assesses enemy force capabilities and intentions
- Conceals our capabilities and intentions

Intelligence
Classify information **only** when disclosure could reasonably be expected to cause damage to national security

Foreign Relations
Generally a Department of State responsibility, under certain instances Defense projects or programs classify foreign government information

> **Hardware popup:** Hardware items may be classified if they reveal information or information can be obtained from them. An item of hardware does not necessarily need to be classified simply because it is part of a classified product or effort. For example, a wrench used for maintenance on Air Force One is not classified. However, if the wrench is specialized for a specific piece of equipment associated with a classified weapons system on Air Force One, it may be classified.
>
> There are several factors to consider when classifying hardware. Unclassified off-the-shelf items generally cannot be classified, though unique and unusual uses for unclassified items may be classified.
>
> You may be able to use engineering and production plans and diagrams to identify and isolate classification requirements. Test equipment rarely embodies classified information but may be classified if it is set in such a way that it reveals classified information.
>
> Hardware (DoDM 5200.45)
>
> - Classify hardware only if it reveals information or information can be obtained from it.

EXAMPLE popup:

INFORMATION REVEALING	CLASS	DECLASSIFY ON	REMARKS
End item hardware:			
a. AN/APR-999	"C"	20150820	External views of the assembled AN/APR-999
(1) Analyzer unit	"C"	20150820	
(2) Threat display unit	"U"		
(3) Preamplifier	"U"		
b. AN/APR-0000	"U"		

MORE popup:

Unclassified, off-the-shelf (OTS) items: Unclassified off-the-shelf (OTS) items, unless modified in some particular way to make them perform differently, can never be classified, even though they constitute a critical element, become an integral part of a classified end product, or produce a properly classified effect.

The association, however, of otherwise unclassified hardware with a particular effort or product may reveal something classified about that effort or product. Decisions regarding what aspect of the system to classify may be difficult but are necessary to delineate for users of the guide, what information requires protection.

Unique and unusual uses for unclassified items: Unusual, unique, or peculiar uses or modifications of ordinarily available unclassified materials or hardware may create a classifiable item of information. In another instance, just using a particular material in a particular effort might reveal a classifiable research or development interest. In such cases, it is especially important to accurately identify the classified information to determine whether it is the hardware or material that reveals classified information or the association of uses of the hardware with a particular effort that reveals such information.

Engineering and production plans and diagrams: At some stage in a production effort, production and engineering plans are drawn. Usually a family-tree type diagram is prepared to assist in determining what components, parts, and materials will be required. This diagram provides a good basis for determining where and when classified information will be involved in the production effort.

Further along in the development process, diagrams and drawings are created for each individual element, showing design data, functions, and specifications. From these drawings it is possible to determine exactly which elements of the final product will reveal classified information. It is also possible to determine associations that may reveal classified information.

This is a prime opportunity to identify and isolate classification requirements.

Users: Management and staff supervisory personnel usually need to have a fairly broad knowledge of classification requirements. Farther down the line, however, foremen and workers usually need to know only which hardware items are classified, the appropriate levels of classification, and which items are unclassified.

Therefore, as soon as possible in the production planning process, make a listing of all classified hardware items according to part number or other identifier, and when necessary for understanding, a listing of unclassified items. Such a listing will be valuable to procurement and logistics (e.g., shipping, handling, and storage) personnel. The listing should preferably be unclassified and should be reviewed carefully to ensure that the listing itself does not reveal classified information.

Production: When planning a production line, careful attention is needed to delay as long as possible the insertion of classified hardware items.

Test equipment: Test equipment rarely embodies classified information. When such equipment is used to test tolerances, specifications, performance, and other details that are classified, the equipment would still be unclassified unless it was calibrated or set in such a way as to reveal the classified information pertaining to the item being tested. Do not, however, confuse test equipment, which is usually unclassified, with test equipment data of a classified item, which could very easily be classified.

Military Operations

Military Operations popup:

The classification of military operations information depends upon multiple factors. While there is nothing written in stone for the classification of military operations information or the operations security, or OPSEC, of each military service and command basic concepts can be applied.

Successful battle operations depend largely upon our ability to correctly assess the capabilities and intentions of enemy forces at each stage of battle while concealing our own capabilities and intentions. You must consider what is known about the enemy, such as the strength, location, and morale of opposing forces, what must be concealed about us, such as the details of locations, target characteristics, and operational plans that are not publicly discernable.

Military Operations rollover:

Military operations are defined as information pertaining to a strategic or tactical military action, including training, movement of troops and equipment, supplies, and other information vital to the success of any battle or campaign.

OPSEC rollover: A process of identifying critical information and analyzing friendly actions attendant to military operations and other activities including:

- Identifying those actions that can be observed by adversary intelligence systems.
- Determining indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical intelligence in time to be useful to adversaries.
- Selecting and executing measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

Example popup:

TOPIC	CLASS	DECLASSIFY ON	REMARKS
C5.3.3.1. Overall operational plans	"S"	Date-event-date within 10 years	
C5.3.3.2. System operational deployment or employment	"C"	After deployment or employment	
C5.3.3.3. Initial Operational Capability (IOC) date	"C"	After IOC Date	
C5.3.3.4. Planned location of operational units	"S"	After arrival on site	
C5.3.3.5. Equipage dates-readiness dates-operational employment date	"S"	After these events	
C5.3.3.6. Total Manpower or personnel requirements for total operational force	"C"	After operation	
C5.3.3.7. Coordinates of selected operational sites	"S"	"C" after site activation; "U" on termination of site	
C5.3.3.8. Specific operational performance data that relates to the effectiveness of control of forces and data on specific vulnerabilities and weaknesses	"S"	Date/event-date within 10 years	
C5.3.3.9. Existing OPSEC and COMSEC	"S"	Date/event-date within 10 years	
C5.3.3.10. Target characteristics	"S"	Date/event-date within 10 years	

In considering classification guidance for military operations, there may be good reason to classify more information about the operations in the beginning than will be necessary later on in the operation. Certain elements of information such as troop movements may no longer require protection after a certain date or event.

When this point is reached, downgrading or even declassification should be considered. Examples of military operations information that may require classification may be found in the chart displayed in the graphic.

Intelligence

Intelligence popup: Information should not be classified unless it could reasonably be expected to cause some degree of damage to national security; for example, if it reveals some aspect of the intelligence mission and its revelation would jeopardize the effectiveness of a particular function.

There are several factors to consider when classifying intelligence, including the intelligence source, intelligence requirements, relationships to foreign intelligence organizations, and counterintelligence activities. Further, many DoD OCAs do not have jurisdiction over intelligence information and may not be qualified to originally classify intelligence. That does not mean, however, that an OCA may not include guidance on intelligence related to the guide topic in the SCG.

EXAMPLE popup:

TOPIC	CLASS	DECLASSIFY ON	REMARKS
C6.3.1. Biographic information taken exclusively from open source, where no intelligence connection is shown.	"U"		
C6.3.2. Positive identification of an individual as potential source to a U.S. intelligence agency.	"S-TS"	Date/event within 10 years, or 10 years from origination	"TS" if identified as an actual source.
C6.3.3. Identity of a target installation or target personality when not linked to a specific collection operation.	"S"	Date/event within 10 years, or 10 years from origination	"TS" when linked to an actual source or Specific collection operation.
C6.3.4. Interest in specific events for collection exploitation, including specific areas of technology.	"S"	Date/event within 10 years, or 10 years from origination	
C6.3.5. Names of collection agency case officers in conjunction with a specific collection operation.	"C"	Date/event within 10 years, or 10 years from origination	
C6.3.6. Information on collection agency HUMINT policy plans, plans, methods, or accomplishments.	"S"	Date/event within 10 years, or 10 years from origination	

MORE popup: Categories of typically classified intelligence information:

- Cryptologic, cryptographic, signals intelligence, or imagery intelligence
- Counterintelligence
- Special access programs
- U.S. nuclear programs and facilities
- U.S. military space programs
- Information that identifies clandestine organizations, agents, sources, or methods
- Information on personnel under official or nonofficial cover, or revelation of a cover arrangement
- Covertly obtained intelligence reports and the derivative information that would divulge intelligence sources or methods
- Personnel recruiting, hiring, training, assignment, and evaluation policies
- Foreign nuclear programs, facilities, and intentions

Intelligence sources: Intelligence identifying a sensitive source or method is classified, as well as the evaluation of the particular source or method.

Intelligence that does not identify or reveal a sensitive source or method is usually not classified unless the information contains other classified information such as intelligence activities including intelligence plans, policies, or operations.

Non-DoD sources: Defense users must respect security classification assigned to intelligence received from non-Defense sources.

Intelligence requirements: An intelligence requirement is classified when it reveals what is not known, what is necessary to know, and why. Moreover, the requirement may recommend a sensitive source or method, other military intelligence required, or contain technical and operational characteristics of classified weapons systems.

Foreign Sources: Intelligence that reveals the identity of a conventional source or method normally does not require classification. However, if the information is communicated to the Department of Defense by a foreign government, whether under a formal government-to-government agreement or, simply with the understanding that the information is provided in confidence, the information must be protected at the level and for the length of time agreed to by the US and the transmitting government.

If the information is obtained from a foreign government without any agreement or restrictions, the classification, if any, should be based solely on the content of the information provided.

Foreign/Enemy Intelligence: Intelligence that reveals the identification of all known and

possible enemy capabilities to collect and exploit information from a given or similar operation is classified. This threat would include enemy intelligence collection and analysis capabilities, efforts, and successes. An integral part of this data is an assessment of enemy human intelligence, signal intelligence, and reconnaissance satellite capabilities.

Relationships to foreign intelligence organizations: Normally, the fact of broad, U.S. general intelligence cooperation with foreign countries or groups of countries that the U.S. maintains formal military alliances or agreements (e.g., NATO) is not classified. The fact of intelligence cooperation between the U.S. and a specific governmental component in an allied country or general description of the nature of intelligence cooperation between the United States and any allied country may be classified.

The fact of intelligence cooperation between the U.S. and specifically named countries or their governmental components that the U.S. is NOT allied is always classified.

Details of any intelligence exchange agreements are classified. In some instances, the mere existence of such an agreement may be classified. The identities of foreign governmental or military personnel who provide intelligence under such agreements or liaison relationships may be classified.

Counter-intelligence activities: Information that reveals counterintelligence activities, identities of undercover personnel or units or clandestine human agents, methods of operations and analytical techniques for the interpretation of intelligence data is classified.

Cryptographic and electronic information: Cryptologic information is classified, including cryptologic sources and methods. Information concerning electronics intelligence, telemetry intelligence, and electronic warfare is usually classified.

Foreign Relations

Foreign Relations popup:

Although the Department of State is the primary agency responsible for the security classification of foreign government information, there are instances where Defense projects and programs involve foreign government information for which security classification guidance must be developed. This includes program matters where both the U.S. and a foreign government are jointly responsible for a program.

There are several types of information or material involving foreign government information that can require consideration for classification, including U.S. Government positions or options in negotiations and contingency plans that involve other countries.

Consider:

- U.S. Government positions or options in negotiations
- Comments on Foreign government officials
- Unpublished correspondence between heads of state or governments
- Statements of U.S. intent to defend or not defend, or to attack or not attack, identifiable regions in foreign countries
- Agreements with foreign countries to use or have access to military or naval facilities
- Contingency plans that involve other countries
- Information concerning relationships with foreign intelligence organizations or related to foreign collection activities

Comments on Foreign government officials rollover:

Types of information covered in this category are records revealing a foreign official:

- Speaking in a highly critical manner of his own government's policy
- Suggesting how pressure might effectively be brought to bear on another part of his own government
- Acting in unusually close concert with U.S. officials where public knowledge of this might be harmful to that foreign official
- Whose professional advancement would be beneficial to U.S. interest, especially if any implication has been made of U.S. efforts to further his advancement, or if public knowledge of this might place the person or his career in jeopardy

Contingency plans that involve other countries rollover:

- Contingency plans that may involve other countries, the use of foreign bases, territory, or airspace; or the use of chemical, biological, or nuclear weapons
- Defense surveys of foreign territories for purposes of basing or using in contingencies
- Statements relating to any use of foreign bases not authorized under bilateral agreements

EXAMPLE popup: Examples of foreign relations information that may require classification may be found in this graphic. In this example, fictional information pertaining to European countries and

U.S. permissions for military fly-overs is shown.

NOTE: The classification guide in the example would have to be classified Secret because it reveals the information that country 'Y' has determined would result in serious damage.

TOPIC	CLASS	DECLASSIFY ON	REMARKS
C7.3.1.4.1. Fact of U.S. overflights - Europe			
C7.3.1.4.2. (S) Country "Y"	"S"	Requires written approval of foreign government involved	(S) Must be at least 50,000 feet altitude; lower flights not permitted in "Y" and "Z"
C7.3.1.4.3. (C) Country "Z"	"C"	Requires written approval of foreign government involved	(S) Must be at least 50,000 feet altitude; lower flights not permitted in "Y" and "Z"
C7.3.1.4.4. (U) Other European	"U"	Requires written approval of foreign government involved	(S) Must be at least 50,000 feet altitude; lower flights not permitted in "Y" and "Z"

MORE popup:

There are additional markings that may be used when classifying foreign government information.

Dissemination control markings:

Not Releasable to Foreign Nationals (NOFORN):

- Used to indicate that information is not authorized for release to foreign nationals, governments, or organizations
- May only be used on intelligence information that requires originator approval before being disclosed
- Example: the banner line for Top Secret information that is not releasable to foreign nationals would appear as: TOP SECRET//NOFORN

Authorized for Release To (REL TO):

- Identifies classified information that an originator has predetermined as releasable to foreign governments or international organizations (such as NATO), through established foreign disclosure procedures
- Appears with the trigraphic country codes for those nations or organizations authorized to potentially receive the information, beginning with the U.S.
- Examples: the banner line for Secret intelligence information authorized for release to the U.K., Australia, and NATO would appear as: SECRET//REL TO

USA, AUS, GBR, NATO

Format Variations

You have seen several examples of how classified information is presented in security classification guides. When you develop a security classification guide you must use the required format outlined in DoDM 5200.45 for communicating the actual classified information. You may modify the headers and arrangements to suit your style and specific need.

For example, a column for downgrading action would not be necessary if the guide did not provide for it, or if only one or two items of information are to be downgraded. When a column only applies to a few pieces of information, it may be removed, and its information can be placed in a "Remarks" or "Comments" column.

ELEMENT OR CATEGORY OF INFORMATION	CLASS	REASON	DOWN-GRADE	DECLASSIFY ON	REMARKS
1.4.1 System capacity	S	1.4a	"C" Upon reaching IOC	20230630	See Note 1.
1.4.2 Signature characteristics	C	1.4a		20210619	

Note 1: Downgrade to CONFIDENTIAL upon reaching IOC

Distribution of Security Classification Guides

Completed security classification guides should be provided to Administrator, DTIC, along with DD Form 2024 to be indexed in an on-line accessible database maintained by DTIC (Refer to DoDM 5200.01, Volume 1, Enclosure 6 for more information). Before dissemination, Original Classification Authorities are required to approve guides in writing. The guides must be submitted to those organizations and activities that may classify information the guide covers.

For distribution and indexing of a guide, complete the DD Form 2024, DoD Security Classification Guide Data Elements, for inclusion in the online index. If listing the guide in the DTIC online index would be inadvisable for security reasons, issuance of the SCG may be separately reported through appropriate channels with an explanation of why the SCG should not be listed.

The originating organization shall:

- Distribute guides to those organizations and activities that may classify information the guide covers
- Complete DD Form 2024 for submission to DTIC

DTIC rollover: Defense Technical Information Center

MORE popup:
Provide one copy each to:

- Organizations and activities responsible for derivatively classifying information covered by the guide.
- Defense Office of Prepublication and Security Review (DOPSR)*
- Office of the Assistant Security of Defense (Public Affairs) *
- Defense Technical Information Center ATTN: DTIC-OA (Security Classification Guides)

Include appropriate distribution statement required by DoDI 5230.24, Distribution Statements on Technical Documents. Submit a completed DD Form 2024, DoD Security Classification Guide Date Elements with each request.

***Note**: Copies are provided to the DOPSR and Office of the Assistant Secretary for Defense (Public Affairs) as they coordinate responses to Freedom of Information Act (FOIA) requests. Freedom of Information and Security Review and Office of the Assistant Secretary for Defense (Public Affairs) as they prepare FOIA requests and deal with the public.

Overview

At times an SCG is not appropriate or warranted and a less cumbersome form of classification guidance may be issued. Instead, a properly marked source document may be issued. The shorter form of guidance provided in a properly marked source document may be issued to disseminate new or changed information quickly pending a revision to a security classification guide, or when there is limited scope or applicability. DD Form 254, DoD Contract Security Classification Specification, may be used to identify specific classification guides or source documents that are to be referenced during the performance of a contract.

Properly Marked Source Document

There are two types of properly marked documents. An OCA issues a properly marked originally classified document to issue guidance quickly. This may occur when an SCG is pending revision, or when a project or operation has limited scope or applicability. Derivative classifiers must carry original classification forward in a derivatively classified document. The classification level of properly marked source documents is determined by the highest classification level of the document's content.

Properly marked source documents do not have a formal standard format, though specific organizational guidance may dictate format. When determining what format to use, consider the urgency to expedite the classification guidance and the scope of the classification guidance. A limited scope may warrant a letter or memorandum, while a more comprehensive scope may warrant issuance of an order or plan.

Regardless of format – whether it be a letter, memorandum, document plan, or order - the guidance must be concise and clearly explain the information that warrants protection and the

associated classification level, duration of classification and downgrading instructions, and any other special considerations.

DD Form 254

The DD Form 254 is an attachment to the government contractual package and is used to convey derivative classification guidance to DoD contractors. The preferred method is to issue unclassified DD Form 254s.

The form identifies security requirements and guidance for contractors performing classified contracts for the DoD, provides excerpts of an SCG, or references the requirement to use an SCG forwarded under separate cover by the government.

derivative classification rollover:	Derivative classification is the process of determining whether information has already been originally classified and, if it has, ensuring that it continues to be identified and protected as classified information by marking or similar means when included in newly created material.
MORE popup:	The DD Form 254, DoD Contract Security Classification Specification, should be unclassified, and must be reviewed carefully to ensure that it does not reveal classified information. Although the preferred method is to issue an unclassified DD Form 254, for some contracts, they warrant classification. If classified, this may complicate the contractual process. Local contracting and security officials can provide guidance when issuing a classified DD Form 254.

Other Types of Guidance

Security classification guidance must be in accordance with organizational requirements and distribution must be made to all organizations and activities responsible for derivatively classifying information covered by the classification guidance.

When these other types of guidance are used to update or revise existing classification guidance that may have broad application, or if an SCG covering the subject is published in the online index of Security Classification Guides, DTIC must be provided with copies of the revised guidance, using the same procedure as for SCGs.

DTIC does not need to be informed when guidance is issued short-term or contains limited scope information that is used only internally within an organization.

Review Activity 1

How well do you understand the contents of security classification guides?

The performance characteristics of the classified item
Section 3 – Performance and Capabilities

Countermeasures taken to mitigate potential weaknesses
Section 6 – Vulnerabilities and Weaknesses

Hardware components
Section 8 – Hardware

Description of the classification effort
Section 2 – Overall Effort

Crucial items that are unique enough to warrant separation in the guide
Section 5 – Critical Elements

Procurement schedules
Section 7 – Administrative Data

Instructions for reproducing, extracting, and disseminating guide contents
Section 1 – General Instructions

The physical components and assembly of the classified item
Section 4 - Specifications

Review Activity 2

Try answering these questions.

How well do you understand the publishing requirements of each type of classification guidance?

Complete DD Form 2024 as part of the process of indexing and distributing a security classification guide.

Answer: True

Distribute properly marked source documents to all organizations/activities responsible for derivatively classifying the information covered.

Answer: True

Review Activity 3

To which of the following types of information should you apply special consideration when developing a security classification guide?

- □ Intelligence
- □ Military Operations
- □ Administrative data
- □ Manufacturing processes
- □ Hardware
- □ Foreign relations

Answer: Intelligence; Military Operations; Hardware; Foreign Relations

Review Activity 4

Why are properly marked source documents issued?

Which statement best describes why a properly marked source document should be issued?

- A properly marked source document is issued to disseminate new or changed information quickly and to carry original classification forward by a derivative classifier.
- A properly marked source document is issued to convey classification information to cleared contractors.
- A properly marked source document is issued as the preferred means for conveying classification information that has broad scope and applicability.

Answer: A properly marked source document is issued to disseminate new or changed information quickly and to carry original classification forward by a derivative classifier.

Summary

You have completed the Developing Classification Guidance lesson.

Lesson: Developing Declassification Guidance

Introduction

In accordance with Executive Order 13526, classified information is declassified when the potential for damage from compromise is no longer a concern to the national security. Declassification guides are written instructions, similar to security classification guides, describing the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

The guides are prepared to facilitate the declassification of information contained in records determined to be of permanent historical value. They are also useful if a system, plan, program, mission, or project has been cancelled, but some of the information continues to require classification. It is the original classification authority's, or OCA's, responsibility to develop the original declassification guidance.

In this lesson, you will learn about how to develop declassification guides. You will learn what declassification guides contain and the requirements. Here are the lesson objectives. Take a moment to review them.

Lesson Objectives:
- Identify the methods for issuing declassification guidance
- Identify the required content for declassification guidance

Overview

Declassification is an authorized change in status of information from classified to unclassified. Security declassification guides are a written record of declassification decisions and provide comprehensive guidance on the classification and declassification of information concerning any system, plan, program, mission, or project.

If at all possible, declassification guides should be handled and safeguarded as Controlled Unclassified Information, or CUI. They should be carefully reviewed to ensure that classified information is not revealed. And like security classification guides, they must include a distribution statement.

Approval Authority

Within the Department of Defense, or DoD, information may be declassified and downgraded by the Secretary of Defense, the Secretaries of the Military Departments, other officials who have been delegated OCAs, and other officials who have been delegated declassification authority. The authority to declassify information extends only to information for which the specific official has declassification jurisdiction or program or functional responsibility. Classified information that has been declassified without proper authority remains classified. Administrative action shall be taken to restore markings and controls, as appropriate.

Required Content

ISOO, 32 CFR, Parts 2001 and 2003, Classified National Security Information; Final Rule, includes specific requirements on the content of security declassification guides. Security declassification guides must identify the subject matter, the name and position of the OCA or Declassification Authority and the date of issuance or last review.

The declassification guide must precisely state the information to be declassified, downgraded, or to remain classified. If there is information that is exempted from automatic declassification, you must identify it.

Publishing Declassification Guidance

Declassification guides may be published in the applicable form of security classification guidance, or SCG. It may also be published in a separate declassification guide.

Declassification guides may be provided by using declassification instructions within the classification guidance itself. When it is sufficiently detailed and understandable, and identified for both purposes, a security classification guide may also be used as a declassification guide.

A separate declassification guide may be prepared to facilitate the declassification of information contained in records determined to be of permanent historical value. In this case, all existing impacted classification guidance is superseded by the guidance listed in the declassification guide.

Declassification guides are reviewed and updated as circumstances require, but at least once every five years. Some programs may require more frequent review and update.

Distribution and Indexing

Completed declassification guides shall be indexed in an on-line accessible database maintained by DTIC and supplied to other individuals and entities. Declassification guides are distributed and indexed in the same manner as SCGs.

Complete the DD Form 2024, DoD Security Classification Guide Data Elements, for submission to DTIC. Provide copies of the guide to the required parties, including organizations responsible for derivatively classifying information covered by the guide.

MORE popup:

Provide one copy each to:

- Organizations and activities responsible for derivatively classifying information covered by the guide.
- Defense Office of Prepublication and Security Review (DOPSR)*
- Office of the Assistant Security of Defense (Public Affairs) *

- Administrator, Defense Technical Information Center
  ATTN: DTIC-OA (Security Classification Guides)

Include appropriate distribution statement required by DoDI 5230.24, Distribution Statements on Technical Documents. Submit a completed DD Form 2024, DoD Security Classification Guide Date Elements with each request.

***Note**: Copies are provided to the DOPSR and Office of the Assistant Secretary for Defense (Public Affairs) as they coordinate responses to FOIA requests.

Review Activity

Try answering these questions.

What information must declassification guidance contain?

The subject matter of the declassification guide
Answer: Required

The OCA or declassification authority by name or personal identifier and position
Answer: Required

The date of issuance or last review
Answer: Required

Precise statement of the categories or elements of information to be declassified
Answer: Required

Any related files series that have been exempted from automatic declassification
Answer: Required

Summary

You have completed the Developing Declassification Guidance lesson.

Lesson: Course Summary

Course Summary:

The safety and security of the United States depends on the ability to adequately protect classified information.

When an Original Classification Authority, or OCA, determines that information is classified, or a Derivative Classifier carries that classification determination forward, he or she must also develop security classification guidance to communicate that determination to others.

In this course, you learned about the process of developing security classification guidance; that is, the policy documents that govern its creation, the different types of guidance, the classification determination itself, and specifically, how to develop each type of guidance, including declassification guides.

Lesson Review

Here is a list of the lessons in the course.

Lessons
- Lesson 1: Course Introduction
- Lesson 2: Security Classification Guidance Overview
- Lesson 3: Classification Guidance Development Process
- Lesson 4: Developing Classification Guidance
- Lesson 5: Developing Declassification Guidance
- Lesson 6: Course Conclusion

Course Objectives

You should now be able to perform all of the listed activities. Congratulations. You have completed the Security Classification Guidance course.

You should now be able to:
- ✓ Identify the policy documents that govern the development of security classification guidance
- ✓ Identify the types of security classification guidance
- ✓ Identify the classification determination process
- ✓ Identify the principles of developing security classification guidance
- ✓ Identify the process of developing declassification guidance