

ISOO HANDBOOK 2018-02: This guidance document does not have the force and effect of law and is not meant to bind the public, except as authorized by law or regulation or as incorporated into a contract. Accordingly, with regard to the public, this document only provides clarity regarding existing requirements under the law or agency policies. This guidance document is binding on agency actions as authorized under applicable statute, executive order, regulation, or similar authority.

Developing and Using Security Classification Guides

October 2018

INFORMATION SECURITY OVERSIGHT OFFICE
NATIONAL ARCHIVES *and* RECORDS ADMINISTRATION
700 PENNSYLVANIA AVENUE, NW, ROOM 100 WASHINGTON, DC 20408-0001
www.archives.gov/isoo



Table of Contents

Purpose	3
References	3
Introduction	4
OCA Responsibilities	5
Recommended Format for Guides	7
Steps in Creating a Security Classification Guide	9
Exercise	11

Purpose

This handbook is issued in accordance with Executive Order (E.O.) 13526, “Classified National Security Information” and 32 CFR Part 2001, “Classified National Security Information” to provide guidance for the development of security classification guides.

Classification management procedures call for the timely issuance of comprehensive guidance regarding classification of information concerning any system, plan, program, project, or mission under the jurisdiction of the original classification authority (OCA), the unauthorized disclosure of which reasonably could be expected to cause damage to national security. Precise classification guidance is a prerequisite to effective and efficient information security and ensures security resources are expended to protect only information truly warranting protection in the interests of national security.

There is no single document that has a more significant and long-lasting effect on the information security community than a classification guide. This single execution of authority by an OCA requires derivative classifiers who use it as a classification source to expend time and resources to protect the information derived from it at various levels. It is imperative that security classification guides are created in accordance with the Order and Directive, and properly updated or cancelled when the information no longer warrants protection at the classified level.

This book contains baseline guidance that is applicable throughout the executive branch. Agencies are welcome to use this or develop their own guidance.

References

Executive Order (E.O.) 13526, “Classified National Security Information”

Sec. 2.2. *Classification Guides.*

Sec. 1.9. *Fundamental Classification Guidance Review.*

32 CFR Part 2001, “Classified National Security Information”

2001.15 *Classification guides.*

2001.16 *Fundamental classification guidance review.*

E.O. 13556, “Controlled Unclassified Information”

32 CFR Part 2002, “Controlled Unclassified Information”

Introduction

A security classification guide is a record of original classification decisions that can be used as a source document when creating derivatively classified documents. OCAs are encouraged to publish security classification guides to facilitate a standardized and efficient classification management program.

Properly Constructed Classification Guide WILL...

- Allow users to build products at a desired classification level
- Enable accurate classification
- Refer you to release processes and authorities
- Improve your derivative classification decisions
- Focus on your agency's/component's equities

A Properly Constructed Classification Guide WILL NOT...

- Make your information unclassified
- Make classification decisions for you
- Allow unclassified public release
- Make you an original classification authority
- Classify external agency equities

The purpose of security classification guidance is to communicate classification decisions and provide a means for uniform derivative classification and consistent application of classification decisions. This is critical to ensure all users of the information are applying the same level of protection and the same duration of classification for the same information.

SCGs provide detailed classification guidance on program-specific information for use by derivative classifiers in applying appropriate classification markings and facilitate the proper and uniform derivative classification of information. They are used to communicate an OCA's predetermined classification decisions on what elements of program-specific information should or should not be classified. The OCA does not make these decisions unilaterally. Subject matter experts, security experts (including your Foreign Disclosure Office), and users of the guide should be involved in developing the guidance as well.

Security classification guides should be cancelled when the information prescribed in the guide no longer requires protection, or the information has been included in another guide.

OCA Responsibilities

An original classification authority is an individual authorized by the President, the Vice President, or by agency heads or other officials designated by the President, to classify information in the first instance. OCAs are responsible for preparing and approving classification guides to facilitate the proper and uniform derivative classification of information.

Criteria for classifying information:

✓ **Government Information**

The information to be classified must be owned by, produced by or for, or is under the control of the U.S. Government.

“Owned by” is information that belongs to the U.S. government.

“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 of” 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.

✓ **Eligibility**

The information must fall within one or more of the categories of information listed in E.O. 13526, Sec. 1.4. These are the eight categories of information eligible for classification:

(a) Military plans, weapons systems, or operations

(b) Foreign government information

(c) Intelligence activities (including covert action), intelligence sources or methods, or cryptology

(d) Foreign relations or foreign activities of the United States, including confidential sources

(e) Scientific, technological, or economic matters relating to national security

(f) U.S. Government programs for safeguarding nuclear materials or facilities

(g) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to national security

(h) The development, production, or use of weapons of mass destruction.

Prohibitions: 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.

Limitations: 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

Research existing guides: Determine that classification guidance is not already available in the form of SCGs, plans, or other memorandums

✓ **Classification Level**

The OCA determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security. The OCA must be able to identify or describe the damage.

Confidential – applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

Secret – applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

Top Secret – applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

✓ **Duration of Classification**

At the time of original classification, the OCA shall establish a specific date or event for declassification up to 25 years based on the duration of the national security sensitivity of the information.

For each element of information, the OCA must apply a classification level and duration of classification not to exceed 25 years. This decision is based on the best information available at that point in time. The sensitivity of information changes, so it is critical that SCGs are reviewed at least once every five years and updated as necessary to reflect those changes.

Recommended Format for Guides

Element of Information	Classification Level	Reason (1.4)	Declassification Date	Dissemination Controls	Controlled Unclassified Information	Remarks
Speed of aircraft	Secret	1.4(a)	25 years			
Personnel Information	Unclassified				CUI//SP-PERS	
VALUE: <i>Explains why the information is being protected</i>						
DAMAGE: <i>Describes the potential impact to national security should an unauthorized disclosure occur</i>						
UNCLASSIFIED STATEMENT: <i>Identifies how a user can address a classified item in an unclassified manner</i>						



Enhancement Statements

Even if you don't include the enhancement statements (Value, Damage, Unclassified Statement) in the guide, these are things you should be considering when writing your classification guide.

Element of Information:

The core of a classification guide is the identification of the specific items or elements of information warranting security protection; specific statements describing aspects of each program, plan, project, system, etc. The elements must describe those items that would be classified if used in a document. You may also indicate elements of information that would be unclassified to add clarity and specificity. It is recommended that you identify **controlled unclassified information (CUI)**.

Classification Level:

The level of classification assigned to each element of information. Only **Top Secret, TS, Secret, S, Confidential, C, Unclassified** or **U** should be placed in this block. Be consistent. Either spell out all of the classification levels, or use only the approved abbreviations.

Reason:

The program, plan, project, etc. must fall under one of the reasons for classification as described in E.O. 13526, Sec. 1.4. It is possible to use multiple reasons within an SCG.

Declassification Date:

How long the information must remain classified. OCAs can only classify information for a maximum of 25 years. Consider circumstances under which information may be downgraded.

Dissemination Controls:

Dissemination controls include those approved for use by the Intelligence Community (NOFORN, ORCON, REL TO, RELIDO, etc.) or other dissemination controls not covered under CUI.

Controlled Unclassified Information:

It is recommended that CUI information that is applicable to the program be annotated in the guide, along with any applicable dissemination control markings. (See the [CUI Registry](#) for more information)

Remarks:

Any other pertinent information may be placed here.

Potential circumstances of classification by compilation must be addressed in the classification guide.

Classification by compilation is when you take two or more pieces of unclassified information and put them together in a way that discloses classified information. Similarly, you can apply this to items of information that are classified at a specified level, but when combined, becomes classified at a higher level.

Example 1

Element of Information	Classification Level	Reason (1.4)	Declassification Date	Dissemination Controls	Controlled Unclassified Information	Remarks
Mission	Unclassified					
Geographic Location	Unclassified					
Compilation of both mission and geographic location within the same document	Secret	1.4(a)	25 years *			

* This indicates that the “Declassify On:” date in the classification authority block would be 25 years from the date the document was created.

Example 2

Element of Information	Classification Level	Reason (1.4)	Declassification Date	Dissemination Controls	Controlled Unclassified Information	Remarks
Mission	Secret	1.4(a)	25 years			
Geographic Location	Secret	1.4(a)	25 years			
Compilation of both mission and geographic location within the same document	Top Secret	1.4(a)	25 years	NOFORN		

Example 3

Element of Information	Classification Level	Reason (1.4)	Declassification Date	Dissemination Controls	Controlled Unclassified Information	Remarks
Single theater-wide operation failure report, outage report, or problem report.	Unclassified					
Compilation of two or more theater-wide operation failure reports, outage reports, or problem reports within the same document.	Secret	1.4(a)	25 years			

Steps in Creating a Security Classification Guide

General content of a guide:

- Identify the subject matter of the classification guide (title of guide).
- Provide the date of issuance or last review.
- Identify the original classification authority by name and position, or personal identifier.
- Identify an agency point of contact for questions regarding the guide.
- State precisely the elements of information to be protected, including controlled unclassified information.
- State the classification level for each element of information.
- State a concise reason for classification (E.O. 13526, Sec. 1.4).
- Prescribe a specific date or event for declassification.
- State, when applicable, dissemination controls and special handling caveats.

1. Determine the type of information the SCG will cover. Will it cover a program, a process, a specific weapon, an airframe? The title of the guide will identify the subject matter.

2. Determine if any classification guidance exists elsewhere that is applicable to items of information concerning the system, plan, program, project, or mission.

- Research existing SCGs. There may be other guides issued along the same functional lines by other activities. Talk to other agencies that may be using the same equipment or have similar programs.
- If similarities are identified, the OCA must ensure consistent, horizontal classification of the information.
- If there is a conflict in classification guidance between the guide the OCA is developing and a previously approved guide, there lies a risk of unauthorized disclosure.

3. Identify specific items of information that require classification.

- The statements and descriptions identifying the items of information to be classified must be clear and specific enough to minimize the probability of error by the derivative classifiers who will use the guide.
- Do not make the statements so broad that derivative classifiers are forced into essentially making original classification decisions.
- Consider potential instances of classification by compilation and include those in the guide.
- General rules to follow:
 - Be precise.
 - Be descriptive.
 - **Write for the user.** The user of the guide must be able to understand the specific topic of information the guide addresses and must be able to apply the correct markings to their document. Write in plain language and spell out acronyms.

3. Assign a classification level to each element of information identified in the guide. Do not use ranges, such as “Unclassified to Secret” unless you can specifically identify the criteria for that element of information to be classified at different levels.

4. Identify the reason for classification. In order for information to be classified, it must meet the requirements of one or more of the categories of information listed in E.O. 13526, Sec. 1.4.
5. Determine the duration of classification. OCAs may classify information up to 25 years from the date of document origin.
6. Identify any applicable dissemination control markings or special handling caveats. If using foreign dissemination controls (e.g. REL TO), you should consult your Foreign Disclosure Office for guidance.
7. Identify any CUI markings that apply.

Example

Element of Information	Classification Level ¹	Reason for Classification	Declassify On (duration of classification)	Dissemination Controls ²	Controlled Unclassified Information	Remarks
1. Fact of U.S. overflights – Europe	Unclassified					
a. Country X	Secret	1.4(d)	25 years	REL TO USA, GBR		
b. Country Y	Confidential	1.4(d)	25 years			
2. Personnel Information	Unclassified				CUI//SP-PVCY	

¹ Only the following will be annotated in the “Classification Level” column – Top Secret or TS, Secret or S, Confidential or C, Unclassified or U.

² Dissemination controls are markings approved for use by the Intelligence Community (NOFORN, ORCON, REL TO, RELIDO, etc.) or other dissemination controls not covered under CUI.

Following is a basic exercise on marking a document using a security classification guide. The purpose of the exercise is to familiarize you with using a security classification guide as a source document.

Exercise

Security Classification Guide

Project Three Little Pigs

August 15, 2018

Issued By: Information Security Oversight Office
National Archives and Records Management

Office of Primary Responsibility: Classification Management
Information Security Oversight Office
202-357-5250

--SIGNED--

James Halliwell-Phillipps
Author/Original Classification Authority

Element of Information	Classification Level	Reason	Duration of Classification	Dissemination Controls	Controlled Unclassified Information	Remarks
Project name	Unclassified					
The existence of pigs	Unclassified					
The existence of the wolf	Unclassified					
Building material of houses	Secret	1.4(a)	10 years			
Methods used to destroy houses	Secret	1.4(c)	25 years			
Entry points into houses	Top Secret	1.4(c)	25 years	NOFORN		
Advice from Mom	Unclassified					

Based on the security classification guide, mark the document on the next page.

This is an exercise. Classification markings are for training use only.

() Project Three Little Pigs

() Once upon a time there were three little pigs and the time came for them to leave home and seek their fortunes.

() Before they left, their mother told them "Whatever you do, do it the best that you can because that's the way to get along in the world." The first little pig built his house out of straw because it was the easiest thing to do.

() The second little pig built his house out of sticks. This was a little bit stronger than a straw house.

() The third little pig built his house out of bricks.

() One night the big bad wolf, who dearly loved to eat fat little piggies, came along and saw the first little pig in his house of straw. He said "Let me in little pig or I'll huff and I'll puff and I'll blow your house in!"

() "Not by the hair of my chinny chin chin", said the little pig.

() But of course the wolf did blow the house in and ate the first little pig. The wolf then came to the house of sticks.

() "Let me in little pig or I'll huff and I'll puff and I'll blow your house in." "Not by the hair of my chinny chin chin", said the little pig. But the wolf blew that house in too, and ate the second little pig.

() The wolf then came to the house of bricks. "Let me in." cried the wolf. "Or I'll huff and I'll puff till I blow your house in."

() "Not by the hair of my chinny chin chin," said the pig.

() Well, the wolf huffed and puffed but he could not blow down that brick house. But the wolf was a sly old wolf and he climbed up on the roof to look for a way into the brick house. The little pig saw the wolf climb up on the roof and lit a roaring fire in the fireplace and placed on it a large kettle of water. When the wolf finally found the hole in the chimney he crawled down and KERSPLASH right into that kettle of water and that was the end of his troubles with the big bad wolf.

Classified By:

Derived From:

Declassify On:

Answer Key for Exercise

This is an exercise. Classification markings are for training use only.

TOP SECRET//NOFORN

September 4, 2018

(S) Project Three Little Pigs

(U) Once upon a time there were three little pigs and the time came for them to leave home and seek their fortunes.

(S) Before they left, their mother told them "Whatever you do, do it the best that you can because that's the way to get along in the world." The first little pig built his house out of straw because it was the easiest thing to do.

(S) The second little pig built his house out of sticks. This was a little bit stronger than a straw house. The third little pig built his house out of bricks.

(S) One night the big bad wolf, who dearly loved to eat fat little piggies, came along and saw the first little pig in his house of straw. He said "Let me in little pig or I'll huff and I'll puff and I'll blow your house in!"

(U) "Not by the hair of my chinny chin chin", said the little pig.

(S) But of course the wolf did blow the house in and ate the first little pig. The wolf then came to the house of sticks.

(U) "Let me in little pig or I'll huff and I'll puff and I'll blow your house in." "Not by the hair of my chinny chin chin", said the little pig. But the wolf blew that house in too, and ate the second little pig.

(S) The wolf then came to the house of bricks. "Let me in." cried the wolf. "Or I'll huff and I'll puff till I blow your house in."

(U) "Not by the hair of my chinny chin chin," said the pig.

(TS/NF) Well, the wolf huffed and puffed but he could not blow down that brick house. But the wolf was a sly old wolf and he climbed up on the roof to look for a way into the brick house. The little pig saw the wolf climb up on the roof and lit a roaring fire in the fireplace and placed on it a large kettle of water. When the wolf finally found the hole in the chimney he crawled down and KERSPLASH right into that kettle of water and that was the end of his troubles with the big bad wolf.

Classified By: Peggy Ushman, Senior Program Analyst, ISOO
Derived From: Project Three Little Pigs SCG, dated Aug 15, 2018
Declassify On: September 4, 2043

TOP SECRET//NOFORN