NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

HANDBOOK FOR WRITING SECURITY CLASSIFICATION GUIDES (SCG)

National Aeronautics and Space Administration
Office of Security and Program Protection
Washington, DC 20546-0005

Forward

Justice Potter Stewart noted in his opinion in the Pentagon papers case, *"when everything is secret, nothing is secret."* Conversely, the price of under-classification or failing to properly classify information ranges from harm to the national security to the loss of economic competitiveness, and at worst, the loss of lives.

Original Classification Authority is an important responsibility. It must be exercised with sound judgment, integrity, thoughtfulness, and prudence. The consequences of an undefined and inconsistent classification management program are wasted resources, lack of public trust, and potential harm to national security. Over-classification creates undue administrative burden, requires the expenditure of funds and commitment of resources, and dilutes the legitimacy of properly classified information.

Original Classification Authorities are encouraged to publish "Security Classification Guides (SCG)" to facilitate a standardized and efficient classification management program. A SCG provides detailed classification guidance on program specific information for use by derivative classifiers in applying appropriate security classification markings. A SCG is an extension of your original classification authority. It is used to communicate your predetermined classification decisions on what elements of program-specific information should, or should not, be classified, your reasons for classification, and how long the information is to remain classified. The SCG is an invaluable tool created and approved personally and in writing by an Original Classification Authority and published to facilitate the proper and uniform derivative classification of information.

This handbook was developed to assist you in writing and publishing a security classification guide. We hope it serves you well. If you have any comments or recommendations for improvement please feel free to give us a call at (202) 358-2054.

John A. Piasecky
Director, Security Management Office

References

Executive Order 12958, "Classified National Security Information," as amended by EO 13292

Information Security Oversight Office (ISOO) Directive No. 1 (32 CFR, Part 2001), "Implementing Directive for Executive Order 12958"

NASA "Original Classification Authority" Information Handbook

Contact Information

Questions or comments relating to this handbook can be addressed to:

NASA HQ
Office of Security and Program Protection
Washington D.C. 20546

Telephone: (202) 358-0773
Fax: (202) 358-3238
E-mail: wmorrison@nasa.gov

Steps in Creating a Security Classification Guide

The following steps are for assisting writers in the preparation and publication of a Security Classification Guide (SCG). Details can be found on the page identified after each step.

STEP 1: Determine Information Type

The SCG writer must first determine the type of information the SCG will address. The type of information will be reflected in the title of your guide as well as provide an indication of the elements of information the guide covers. For example, a guide title and the type of information it covers might be “NASA Office of Space Operations– Project Overland Umbrella” or, “NASA Office of Security and Program Protection - Physical Security Configuration and Design Vulnerabilities” (Figure 1), etc.

The SCG can also be issued by office or organizational element to combine all classification guidance from distinct programs into a single, all-inclusive Code/enterprise guide. For example; “Security Classification Guide for the Office of Space Flight” (Figure 2)” or, “Security Classification Guide for the Office of Science,” etc.

In the first instance, the SCG would cover a defined type of information and the specific elements of information within the SCG would correspond with the type. In the latter instance, the type of information covered by the SCG is not defined and the specific elements of information covered by the guide might be a collection of diverse categories of information under the jurisdiction of the issuing office/organizational element.

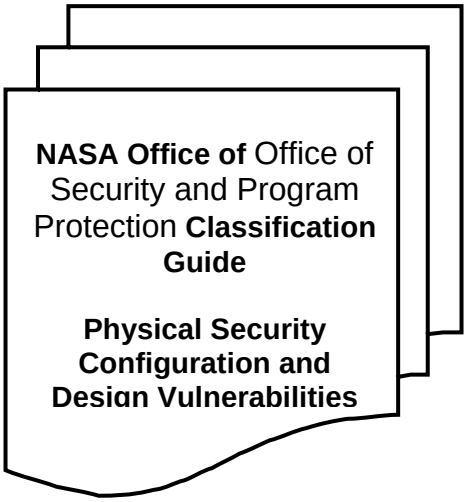

Figure 1

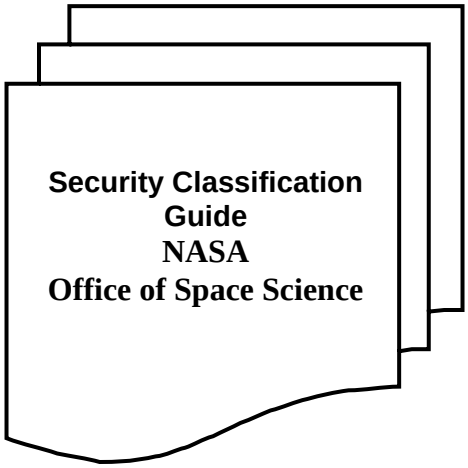

Figure 2

Step 2: Determine Elements

Based on the type of information the SCG will cover, determine the specific elements of information to be addressed in the SCG. Be precise. Write for the user. The user of the SCG must be able to know and understand the specific element of information the classification guidance addresses. For example; an element of information might be “Specific perimeter security deficiencies, if released, could result in the loss, theft, or compromise of classified information (Figure 3), or, “Particulars of the DoD payload for STS-xxx.” (Figure 4), etc.

SCG Element Examples

SCG Physical Security Configuration and Design Vulnerabilities

Element of Information

Specific perimeter security deficiencies, if released, could result in unauthorized access, compromise physical security and safety, or the loss, theft, or compromise of classified information.

Figure 3

SCG OSO

Element of Information

Particulars of the DoD payload for STS-xxx.

Figure 4

STEP 3: Consult Experts

Consult with internal subject matter experts and the potential users of the SCG. Consulting with other agencies with interests in similar programs and information is also encouraged to ensure uniformity and consistency in classification guidance. For example, when writing a SCG that addresses aircraft propulsion methods, it might be advisable to coordinate the guidance with counterparts in the Department of Air Force.

Interacting between writers and users is especially important to ensure changing situations are brought to the attention of the appropriate officials for inclusion in updated SCG's.

SCGs are living documents to be reviewed and updated as circumstances require, but no later than five years from the date of issue.

STEP 4: Determine Reason(s)

Determine the reason(s) for classification for each element within the SCG.

Executive Order 12958, as amended, lists eight categories of information to be considered for classification. If the element of information does not fall within one of these eight categories, then the information cannot be considered for classification. On the other hand, just because information falls within one of these eight categories does not mean the information should automatically be classified.

For each element of information cited in the SCG, cite the "Reason" for classification by including the applicable category of information from Section 1.4 of the Executive Order (Figures 5 & 6). The eight categories are:

1.4 (a) Military plans, weapons systems, or operations

1.4 (b) Foreign government information

1.4 (c) Intelligence activities (including special activities), intelligence sources or methods, or cryptology

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

1.4 (e) Scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism

1.4 (f) United States Government programs for safeguarding nuclear materials or facilities

1.4 (g) Vulnerabilities or capabilities of systems, installations, infrastructure, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism

1.4(h) Weapons of mass destruction

SCG Element and "Reason" for Classification Examples

SCG Physical Security Configuration and Design Vulnerabilities

Element	Reason
Specific perimeter security deficiencies, if released, could result in the loss, theft, or compromise of classified information.	**1.4(g)**

Figure 5

SCG OSO

Element	Reason
Particulars of the DoD payload for STS-xxx.	**1.4(a)**

Figure 6

STEP 5: Determine A Classification Level

Each element within the SCG must have one of three levels of classification assigned to it (Figures 7 & 8). The resulting degree of damage to the national security if the information were released determines the level of classification to be assigned. SCG authors should base decisions on the following criteria:

TOP SECRET

"Information the unauthorized disclosure of which reasonably could be expected to cause ***exceptionally grave damage*** to the national security that the original classification authority is able to identify or describe."

SECRET

"Information the unauthorized disclosure of which reasonably could be expected to cause ***serious damage*** to the national security that the original classification authority is able to identify or describe."

CONFIDENTIAL

"Information the unauthorized disclosure of which reasonably could be expected to cause ***damage*** to the national security that the original classification authority is able to identify or describe."

SCG Element, Reason, and Classification Level Examples

SCG Physical Security Configuration and Design Vulnerabilities

Element	Reason	Classification
Specific perimeter deficiencies, if released, could result in the loss, theft, or compromise of classified information.	1.4(g)	**Confidential**

Figure 7

SCG OSO

Element	Reason	Classification
Particulars of the DoD payload for STS-xxx	1.4(a)	**Secret**

Figure 8

STEP 6: Determine Duration

Determine the "Duration" for classification for each individual element addressed in the SCG (Figures 9 & 10). The "duration" identifies a point in time in the future when the information will be automatically declassified. There are three general options for duration of classification under Executive Order 12958, as amended.

- Specific Date or Event: When possible, apply a date or event for declassification corresponding with the decline of the information's national security sensitivity. The date or event will be less than 10 years from the date of origination.
- Ten-Year Duration: When a specific date or event within 10 years cannot be determined, apply a date 10 years from the date of origination.
- Beyond Ten Years: If the original classifier determines the sensitivity of the information will remain beyond ten years, then apply a date or event for declassification up to 25 years from the date of origination.

As used in the SCG, the date of origination pertains to the date the specific information is first recorded in NASA records. For example, the SCG for Physical Security Configuration and Design Vulnerabilities is issued on July 1, 2003. The duration instruction for *"specific perimeter deficiencies, which if released, could result in the loss, theft, or compromise of classified information"* is 5 Years from origination. On August 5, 2007 a deficiency is noted that meets the SCG criteria for classification. The declassification date for that particular information would then be August 5, 2012 – not July 1, 2008 – because the information originated on August 5, 2007 – not July 1, 2003.

SCG Duration Example

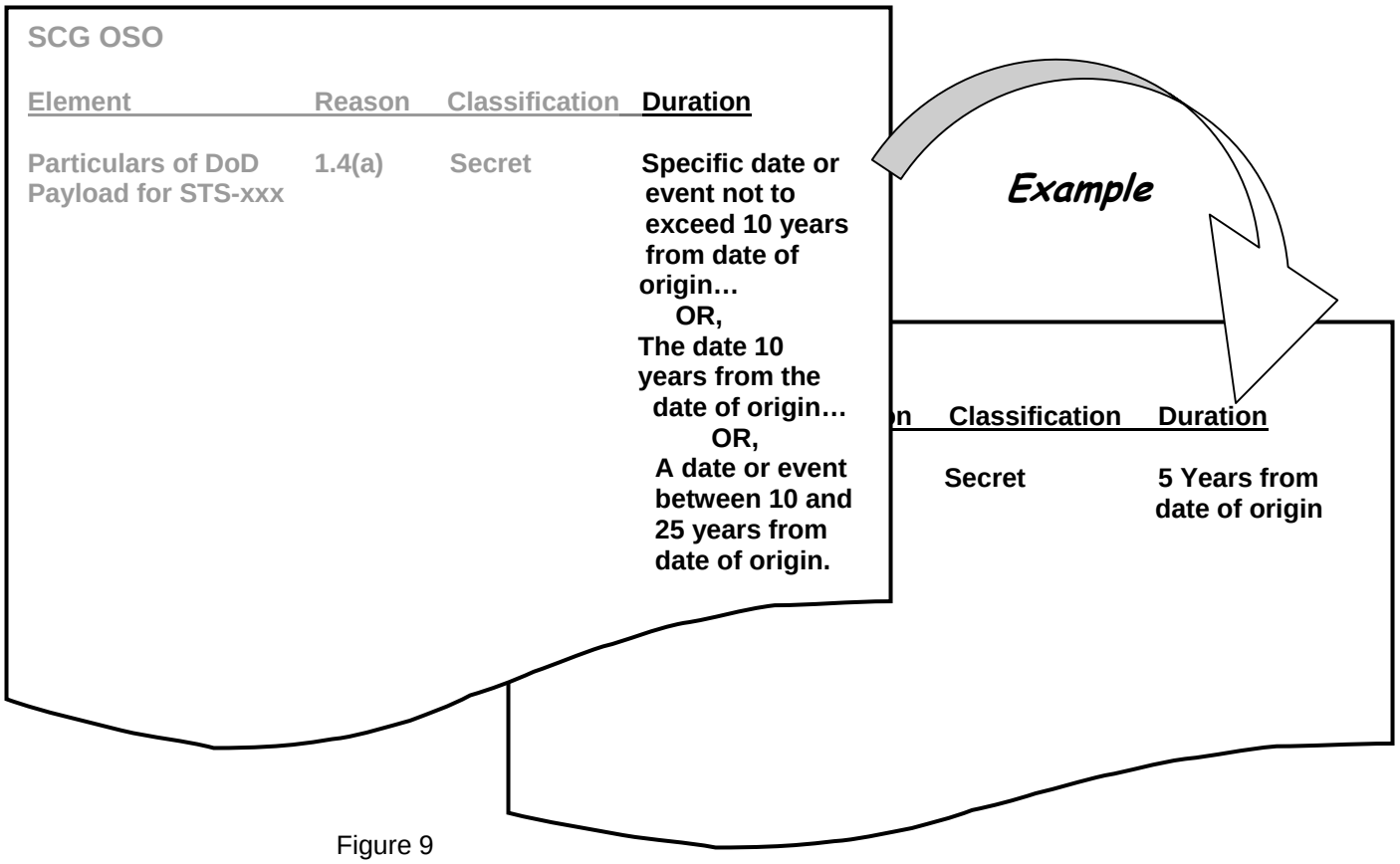

Figure 9

SCG Duration Example

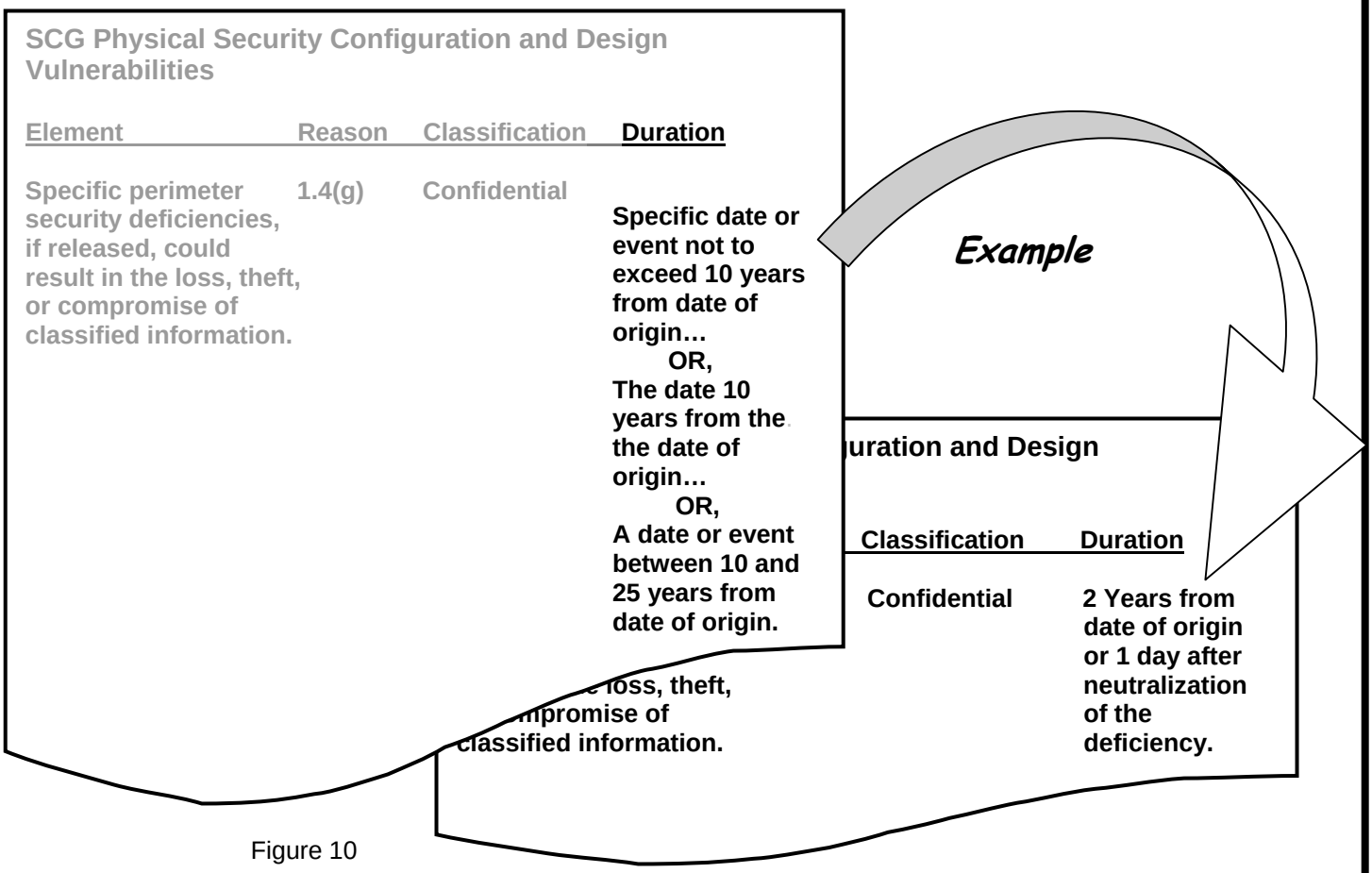

Figure 10

STEP 7: SCG Content and Format

NASA SCG's will include the following (See Figure 11 for a sample SCG format):

- The subject matter of the SCG. This could be project specific or office/organizational element-wide guidance.
- The approving original classification authority by name and position title.
- An agency point-of-contact(s) for questions regarding the SCG.
- The date of issuance and last review.
- The precise elements of information to be protected.
- The reason for classification per Section 1.4 of Executive Order 12958, as amended, and as cited on page 4 of this guide.
- The classification level, as listed on page 6 of this guide, applicable to each element of information, and, when useful, specify the unclassified elements of information.
- When applicable, identify special handling caveats. The use of caveats covered by DCID 1/7, Security Controls on the Dissemination of Intelligence Information, e.g., NOFORN; ORCON; etc. Coordinate use of special handling caveats with the applicable NASA Security Office.
- Prescribe declassification instructions as explained on page 8 of this guide, for each element of information.

Sample Guide Format

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
WASHINGTON, D.C. 20546

Security Classification Guide (SCG)
Office of Security and Program Protection
Physical Security Configuration and Design Vulnerabilities

Date of Guide: July 1, 2003

Date of Last Review:……

Purpose: This classification guide is issued for the purpose of identifying specific elements of information requiring classification and protection in accordance with Executive Order 12958, "Classified National Security Information," as amended.

Authority: This guide is approved by Jim Smith, Director, Security Management Office, a delegated Top Secret Original Classification Authority, and issued in accordance with Executive Order 12958, as amended, and Information Security Oversight Office (ISOO), Directive 1 (32 CFR, Part 2001), "Implementing Directive for Executive Order 12958."

Classification Criteria: Executive Order 12958, as amended, Section 1.4, specifies that only certain categories of information can be considered for classification. This guide provides classification guidance for the following type of information and the associated category per the order: Physical Security Configuration and Design Vulnerabilities: Executive Order 12958, Category 1.4(g), "vulnerabilities or capabilities of systems, installations, projects or plans relating to national security."

Use of the Guide: This guide is for the use of NASA employees performing derivative classification actions when addressing the elements of information covered by this guide.

For the purpose of marking documents containing classified information covered by this guide, derivative classifiers will cite "NASA Office of Security and Program Protection SCG, Dated……" on the "Derived From" line, followed by the declassification instruction as specified in the guide. For Example:

> Derived From: NASA Office of Security and Program Protection SCG, Dated Jul 1, 2003
> Declassify On: (Insert declassification instruction as cited in the SCG)

If classified information covered by this guide, as well as classified information from other classified sources, is included in the same document, the document will be marked as follows:

> Derived From: Multiple Sources
> Declassify On: (Carry forward the single most restrictive declassification instruction from all source documents)

NOTE: If "Multiple Sources" are used for a derivatively classified document, a record of the sources will be maintained with the file copy of the document.

Where the declassification instruction of the source(s) is marked "OADR" or "Originating Agency Determination Required," the declassification instructions for the newly created document will state: "Source Marked OADR," followed by the date of the most recent source.

Classified Processing: Classified information will not be processed on any automated data processing equipment unless the equipment has been specifically accredited and approved for classified processing. Consult office/organizational element security officials for instructions on what equipment may be used.

Marking: Detailed instructions for marking classified materials can be found in the NPG 1620.1 and the ISOO pamphlet titled "Marking." Training on marking classified materials can be obtained by contacting the Office of Security at (202) 358-2054.

Reproduction and Dissemination: This guide may be reproduced and disseminated within NASA as needed. Coordinate dissemination outside of NASA through:

NASA HQ
Office of Security and Program Protection
Washington DC 20546-0005
(202) 358-0773

Approved by: *Jim Smith* **Date:**

Title: Director, Security Management Office

Point of Contact: John Doe (555) 555-5555

Classification Guidance

ELEMENT	REASON	CLASSIFICATION	DURATION
Specific perimeter security deficiencies, if released, could result in the loss, theft, or compromise of classified information.	1.4(g)	Confidential (or the same level as the level of classified information subject to potential compromise)	2 Years From Date of Origin or 1 day after neutralization of the deficiency, whichever occurs first
Deficiencies in the perimeter security of a classified open storage area, if released, could result in the loss, theft, or compromise of classified information.	1.4(g)	Classify at the same level as the level of classified authorized for open storage.	Upon completion of upgrades neutralizing the potential exploitation of the vulnerability, or, 10 years from the date of discovery, whichever occurs first.

STEP 8: SCG Review

Forward a draft copy of the SCG to the NASA HQ, Director of Security Management Office (DSMO) for review. This is an essential step in the SCG creation process. The DSMO can provide overall guidance, reduce needless duplication and assist in interagency questions concerning classification issues. The DSMO will also assist you with the initial preparation of your SCG upon request.

STEP 9: Finalizing the SCG

The SCG must be personally approved and signed by an authorized Original Classification Authority. Within NASA, the Office of Security and Program Protection will normally approve all SCGs.

STEP 10: Disseminate SCG

Once approved, SCG's should be disseminated as widely as necessary to ensure the proper and uniform derivative classification of information. Offices/organizational elements issuing SCGs should maintain a distribution list in order to send recipients any updates or to rescind their authority as applicable.

One copy of the completed and signed SCG will be forwarded to:

NASA HQ
Office of Security and Program Protection
300 E. Street, SW
Washington DC 20546-0005

The Office of Security and Program Protection will maintain an index of NASA published SCG's for use and reference by NASA and other government agencies as appropriate.

DEFINITIONS

Automatic Declassification - Declassification of information based solely upon: Occurrence of a specific date or event as determined by the original classification authority; or expiration of a maximum time frame for duration of classification established under Executive Order.

Classification - The act or process by which information is determined to be classified.

Classified National Security Information (Classified information) - Information determined, pursuant to Executive Order 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure and marked to indicate its classified status when in documentary form.

Classification by Compilation – An aggregation of pre-existing unclassified items of information that when combined, reveal an additional association or relationship not otherwise revealed individually and meeting the standards for classification under the Executive Order.

Confidential Source - Any individual or organization who has provided, or might reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation the information or relationship, or both, are to be held in confidence.

Damage to the National Security - Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of the information.

Declassification - The authorized change in the status of information from classified information to unclassified information.

Declassification Authority - The official who authorized the original classification, if the official is still serving in the same position; the originator's current successor in function; a supervisory official of either; or officials delegated declassification authority in writing by the agency head or the senior agency official.

Derivative Classification - The act of incorporating, paraphrasing, restating, or generating in new form information already classified, and marking the newly developed material consistent with the markings present on the source(s) from where the information was obtained or as directed by a security classification guide.

Downgrading - A determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

Foreign Government Information - Information provided to the U.S. Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence; information produced by the U.S. Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or information received and treated as "Foreign Government Information" under the terms of a predecessor order.

National Security - The national defense or foreign relations of the United States.

Original Classification - An initial determination information requires, in the interest of national security, protection against unauthorized disclosure.

Original Classification Authority - An individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to classify information in the first instance.

Unauthorized Disclosure - A communication or physical transfer of classified information to an unauthorized recipient.

Unclassified – Information not meeting criteria for classification set forth in Executive Order 12958, as amended by Executive Order 13292.

National Aeronautics and Space Administration
Original Classification Authorities

As provided for in 14CFR1203.800, the NASA officials listed below have been permanently delegated Original Classification Authority. Delegation of this authority is by "position." NASA officials filling a delegated position either permanently or temporarily, have original classification authority. Once an official no longer fills a delegated position they no longer have original classification authority.

In addition to those listed below, other NASA officials may be delegated original classification authority when approved by the Director, Security Management Office (DSMO) or the Administrator. Contact your local security office or the NASA Office of Security and Program Protection for additional information.

Original Top Secret

Administrator
Deputy Administrator
Assistant Administrator for Security and Program Protections (AA/OSPP)
Deputy, AA/OSPP
Director, Security Management Office (DSMO)