

This document is made available through the declassification efforts  
and research of John Greenewald, Jr., creator of:

# The Black Vault



The Black Vault is the largest online Freedom of Information Act (FOIA)  
document clearinghouse in the world. The research efforts here are  
responsible for the declassification of hundreds of thousands of pages  
released by the U.S. Government & Military.

**Discover the Truth** at: <http://www.theblackvault.com>

National Aeronautics and Space Administration



**Headquarters**  
Washington, DC 20546-0001

May 9, 2018

Office of Communications

John Greenewald, Jr.  
27305 W. Live Oak Rd.  
Suite #1203  
Castaic, CA 91384  
[john@greenewald.com](mailto:john@greenewald.com)

FOIA: 18-HQ-F-00488

Dear Mr. Greenewald:

Thank you for your Freedom of Information Act (FOIA) request dated and received on March 29, 2018, at the NASA Headquarters FOIA Office. Your request was assigned FOIA Case Number 18-HQ-F-00488 and was for:

I respectfully request a copy of records, electronic or otherwise, of the following:  
a copy of the NASA Handbook for Writing Security Classification Guides.

The NASA Headquarters program office(s) conducted a search for Agency records, using the above criteria. We have located 1 document consisting of 18 page responsive to your request. Attached is the responsive document.

Fees for processing this request are less than \$50.00 and are not being charged in accordance with 14 CFR §1206.503(c). If you have further questions, please feel free to contact me at [hq-foia@nasa.gov](mailto:hq-foia@nasa.gov) or (202) 358-2462, or to discuss any aspect of your request you may contact NASA's Chief FOIA Public Liaison, Ms. Nikki Gramian at (202) 358-0625.

Sincerely,

A handwritten signature in black ink, appearing to read "Josephine Sibley".

Josephine Sibley  
Headquarters  
FOIA Public Liaison Officer



# **HANDBOOK for WRITING SECURITY CLASSIFICATION GUIDES (SCG)**

**APRIL 2014**

**National Aeronautics and Space Administration  
Office of Protective Services  
Washington, DC 20546-0005**

## Purpose

This handbook is issued in accordance with Executive Order (E.O.) 13526, "Classified National Security Information" to provide guidance for the development of NASA security classification guides.

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. The SCG is an invaluable tool created and approved personally and in writing by an Original Classification Authority (OCA) and published to facilitate the proper and uniform derivative classification of information. It is used to communicate an OCA's predetermined classification decisions on what elements of program-specific information should or should not be classified.

## References

- Executive Order 13526, "Classified National Security Information"
- Information Security Oversight Office (ISOO) Implementing Directive 32 CFR, Part 2001, "Classified National Security Information; Final Rule"
- NASA Procedural Requirement (NPR) 1600.2, NASA Classified National Security Information

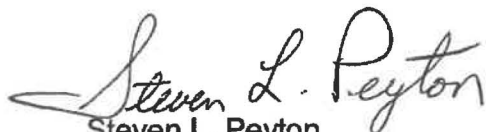
## Contact Information

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

NASA HQ  
Office of Protective Services  
Washington, D.C. 20546

Telephone: (202) 358-2188 or (202) 358-0191  
Unclassified Fax: (202) 358-3238  
E-mail: [HQ-Classification@mail.nasa.gov](mailto:HQ-Classification@mail.nasa.gov)

This SCG Handbook Writing Guide is approved by:



Steven L. Peyton  
Director, Security Management Division  
Office of Protective Services

## **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 the type of information the SCG will cover. (Page 4)
  
- **STEP 2:** Determine the specific elements of information the guide will cover. (Page 4)
  
- **STEP 3:** Consult with internal subject matter experts and other government agencies with similar activities to ensure consistent and uniform classification guidance. (Page 5)
  
- **STEP 4:** Determine the "Reason" for classification of each individual element addressed in the SCG. (Page 6)
  
- **STEP 5:** Determine a "Classification Level" for each individual element addressed in the SCG. (Page 7)
  
- **STEP 6:** Determine the "Duration" for classification for each individual element addressed in the SCG. (Page 8)
  
- **STEP 7:** SCG Content and Format. (Page 9)
  
- Examples (Pages 10-12)
  
- **STEP 8:** Have SCG reviewed by the Director, Security Management Office. (Page 16)
  
- **STEP 9:** Finalize SCG – personally signed and approved by an authorized Original Classification Authority. The OCA will obtain Technical Concurrence from the Associate Administrator (signature required) for the appropriate Mission Directorate. (Page 14)
  
- **STEP 10:** Disseminate SCG. (Page 16)
  
- Definitions (Page 17)
  
- NASA Original Classification Authorities (Page 18)



## 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 Protective Services - 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.

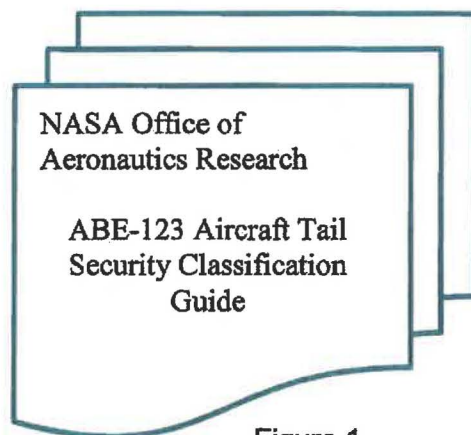


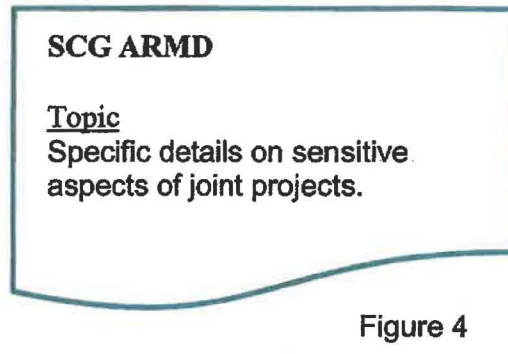
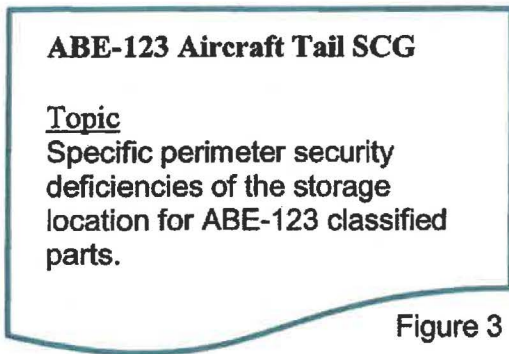
Figure 1



Figure 2

## Step 2: Determine Elements

Based on the type of information the SCG will cover, determine the specific elements of information, or topic, 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 of the storage location for ABE-123 classified parts, if released, could result in the loss, theft, or compromise of classified information (Figure 3), or, "Specific details on sensitive aspects of joint projects." (Figure 4), etc.



### **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 13526 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 covert actions), 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;
- 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; and
- 1.4(h) the development, production, or use of weapons of mass destruction.

<b>ABE-123 Aircraft Tail SCG</b>	
<u>Topic</u>	<u>Reason</u>
Specific perimeter security deficiencies of the storage location for ABE-123 classified parts.	<b>1.4(g)</b>

Figure 5

<b>SCG ARMD</b>	
<u>Topic</u>	<u>Reason</u>
Specific details on sensitive aspects of joint projects.	<b>1.4(e)</b>

Figure 6



**STEP 5: Determine a Classification Level**

When the OCA determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security and the OCA is able to identify or describe the damage, the information may be classified at one of three levels; Top Secret, Secret or Confidential. Each element within the SCG must identify one of the three levels of classification assigned to it (Figures 7 & 8). 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."

**ABE-123 Aircraft Tail SCG**

<u>Topic</u>	<u>Reason</u>	<u>Classification</u>
Specific perimeter security deficiencies of the storage location for ABE-123 classified parts.	1.4(g)	<b>Secret</b>

Figure 7

**SCG ARMD**

<u>Topic</u>	<u>Reason</u>	<u>Classification</u>
Specific details on sensitive aspects of joint projects.	1.4(e)	<b>Confidential</b>

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 four general options for duration of classification under Executive Order 13526 and defined in the 32-CFR, Part 2001. The Executive Order also states that no information may be classified indefinitely.

- A specific date or event for declassification that corresponds to the lapse of the information’s national security sensitivity, which is equal to or less than 10 years from the date of original classification.
- A date not to exceed 25 years from the date of original classification, if the original classifier determines the sensitivity of the information will remain beyond ten years.
- Exception to 25 year duration: Information that should clearly and demonstrably be expected to reveal the identity of a confidential human source, human intelligence source, or key design concepts if weapons of mass destruction are exempt from automatic declassification at 50 years; and an exemption code of 50x1-HUM or 50x1 WMD, respectively, may be applied to the information. This means the information may be classified up to 75 years, but does not require a specific date of event. Just the exemption code is required.
- Exception to 25 year duration: Agencies may incorporate exemptions from automatic declassification that have been approved by the Information Security Classification Appeals Panel (ISCAP) into the classification guide. The ISCAP panel must be notified of the intent to take such action for specific information in advance of approval and the information remains in active use. Information that falls into this category may be classified for up to 50 years for the date of original classification. **Contact the Office of Protective Services, Security Management Division for more information on using this option.**

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 ABE-123 Aircraft Tails is issued on September 30, 2011. The duration instruction for “*specific perimeter deficiencies...*” is 5 Years from origination. On August 5, 2013 a deficiency is noted that meets the SCG criteria for classification. The declassification date for that particular information would then be August 5, 2018.– not September 30, 2016 – because the information originated on August 5, 2013 – not September 30, 2011.

<b>ABE-123 Aircraft Tail SCG</b>			
<u>Topic</u>	<u>Reason</u>	<u>Classification</u>	<u>Duration</u>
Specific perimeter security deficiencies of the storage location for ABE-123 classified parts.	1.4(g)	Secret	<b>10 years from date of origination</b>

Figure 9

## SCG ARMD

<u>Topic</u>	<u>Reason</u>	<u>Classification</u>	<u>Duration</u>
Specific details on sensitive aspects of joint projects.	1.4(e)	Confidential	Upon completion of project

Figure 10

### STEP 7: SCG Content and Format

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

1. Title Page. The subject matter of the SCG. This could be project specific or office/organizational element-wide guidance.
2. Classification level or handling/dissemination requirements for the guide
3. The concurring Associate Administrator for the Mission Directorate by name and position title usually indicated on an Approval page
4. The approving Original Classification Authority by name and position title usually indicated on an Approval page.
5. An agency point-of-contact(s) for questions regarding the SCG.
6. The date of issuance and last review.
7. A log page where changes and revisions are noted and dated.
8. Table of Contents and pages numbered
9. General Instructions that may be useful to the users of the guide.
10. Classification Topics:
  - The precise elements of information to be protected.
  - The reason for classification per Section 1.4 of Executive Order 13526 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 is covered by the Director of National Intelligence, Intelligence Community Directive 710, Classification and Control Markings System and Control Access Program Coordination Office (CAPCO) Register Manual. Coordinate use of special handling caveats with the applicable Center Security Office.
  - Prescribe declassification instructions as explained on page 8 of this guide, for each element of information.
11. Definitions Section.



# Title Page Example

SENSITIVE BUT UNCLASSIFIED (SBU) 

Classification Level or handling instructions at the top and bottom of every page.

## **ABE-123 SECURITY CLASSIFICATION GUIDE**

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION  
ABE-123 AIRCRAFT TAIL

15 July 2013

**THIS SCG PROVIDES INSTRUCTIONS FOR SAFEGUARDING UNITED STATES GOVERNMENT EQUIPMENT FOR ABE-123 AIRCRAFT BASED AT XYZ FIELD, SOMEWHERE, TEXAS**

SENSITIVE BUT UNCLASSIFIED (SBU) 

Classification Level or handling instructions at the top and bottom of every page.

# Change Log Page Example

SENSITIVE BUT UNCLASSIFIED (SBU)

## REVISION SUMMARY PAGE

Version	Editor	Date	Change Page	Reason
Original	John Doe	30SEP2011	None	Initial Issue
1	Jane Smith	05APR2013	5	Change to classification section 1.2

SENSITIVE BUT UNCLASSIFIED (SBU)



# Table of Contents Example

SENSITIVE BUT UNCLASSIFIED (SBU)

## TABLE OF CONTENTS

1.0	REVISION SUMMARY PAGE	1
2.0	CONCURRENCES	2
3.0	TABLE OF CONTENTS	3
4.0	GENERAL INSTRUCTIONS	4
5.0	RELEASE OF INFORMATION	7
6.0	DEFINITIONS	8
7.0	FUNDING, PROCUREMENT, AND PRODUCTION	8
8.0	PERFORMANCE AND CAPABILITIES	10
9.0	SPECIFICATIONS	10
10.0	VULNERABILITIES	12
11.0	OPERATIONS	12
12.0	COMMUNICATIONS SECURITY	14
13.0	ABE-123 PAYLOAD CLASSIFICATION ASSOCIATIONS	16
14.0	ABE-123 DEBRIS RECOVERY	17
	APPENDIX A - COMSEC/CCI MATERIAL	18

SENSITIVE BUT UNCLASSIFIED (SBU)

# General Instructions Section Format

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION WASHINGTON, D.C. 20546  
Security Classification Guide (SCG)  
Office of Protective Services  
Physical Security Configuration and Design Vulnerabilities

**Date of Guide:** September 30, 2013

**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 13526, "Classified National Security Information."

**Authority:** This guide is approved by the Assistant Administrator for Protective Services, a delegated Top Secret Original Classification Authority, and issued in accordance with Executive Order 13526 and Information Security Oversight Office (ISOO), Directive 1 (32 CFR, Part 2001), "Implementing Directive for Executive Order 13526."

**Classification Criteria:** Executive Order 13526, 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...

**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 "ABE-123 SCG, Dated....." on the "Derived From" line, followed by the declassification instruction as specified in the guide. For Example:

Derived From: ABE-123 SCG, Dated 30 September 2011

Declassify On: (Insert declassification instruction as cited in the SCG) **should be written as yyyyymmdd.**

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.

**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 ISOO pamphlet titled "Marking Classified National Security Information." Training on marking classified materials can be obtained by contacting the Office of Protective Services at (202) 358-2188 or (202) 358-0191.



## Topics for Classification Section Example

Topic Number	ELEMENT	REASON	CLASSIFICATION, DESSEMINATION or HANDLING	DURATION
1.0	1.0 Specific perimeter security deficiencies, if released, could result in the loss, theft, or compromise of classified information.	1.4(g)	Confidential	2 Years From Date of origination or 1 day after neutralization of the deficiency, whichever occurs first
2.0	2.0 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)	Secret	Upon completion of upgrades neutralizing the potential exploitation of the vulnerability, or, 10 years from the date of origination, whichever occurs first.
2.1	<b>General information on deficiencies in security on general work areas</b>		<b>Sensitive But Unclassified</b>	
2.2	Permanent 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)	Secret	<b>10 years from date of origination.</b>

## **STEP 8: SCG Review Process**

First, forward a copy of the guide to your Center Office of Protective Services/Security Office. They will then forward a draft copy of the SCG to the NASA HQ, Director of Security Management Division (DSMD) for review. This is an essential step in the SCG creation process. The DSMD can provide overall guidance, reduce needless duplication and assist in interagency questions concerning classification issues. The DSMD will also assist you with the initial preparation of your SCG upon request. The guide must also be reviewed by the Associate Administrator for the appropriate Mission Directorate.

**\*\*Please ensure that your guide is transmitted by proper required channels. If the guide is SBU, make sure it is transmitted with encryption if submitted electronically, contains the NASA form 1686 (SBU cover page), and/or double wrapped in opaque envelopes. For classified guides, please use classified channels to submit.\*\***

## **STEP 9: Finalizing the SCG**

1. The SCG must be approved and signed by the appropriate Mission Directorate Associate Administrator.
2. The SCG must be personally approved and signed by an authorized Original Classification Authority. Within NASA, the Office of Protective Services 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  
ATTN: Director, Security Management Division  
Office of Protective Services  
300 E. Street, SW  
Washington DC 20546-0005

The Office of Protective Services is responsible for maintaining 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 13526, 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** - 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 13526, as amended by Executive Order 13292.

### **National Aeronautics and Space Administration Original Classification Authorities**

Under Executive Order 13526, the President has designated the NASA Administrator with Original Classification Authority. Delegation of this authority is by "position," and has been designated by NPR 1600.2. 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 in writing by the Administrator. Contact your local Center Office of Protective Services or Security Office or the NASA Office of Protective Services for additional information.

#### **Original Top Secret Classification Authority is granted to:**

NASA Administrator NASA Deputy Administrator [Delegated] NASA Associate Administrator [Delegated] Assistant Administrator for the Office of Protective Services [Delegated] Deputy Assistant Administrator for the Office of Protective Services {Delegated}
--