U.S. Department of Commerce
Office of Security

U.S. DEPARTMENT OF COMMERCE
NATIONAL SECURITY INFORMATION
CLASSIFICATION GUIDE
(DOC NSICG)

Version 1.1

May 2024

Issued and Approved By:
Nicholas M. Schnare
Director for Security

United States Department of Commerce

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

U.S. Department of Commerce
Office of Security

(U) FOREWORD

(U) This document provides classification guidance for Department of Commerce (DOC) national security information based on Executive Order (EO) 13526, *Classified National Security Information* and its implementing directive, 32 Code of Federal Regulations (CFR), Part 2001.

(U) This guide is a source of derivative classification guidance for the Department and provides for the protection of DOC originated national security information. All Department personnel have a responsibility to ensure the information we work with every day is properly classified, marked, and safeguarded.

(U) This guide is not a classification source for Sensitive Compartmented Information (SCI) or Special Access Program (SAP) information, or other categories regulated by their own, specialized program classification guides. Classifiers will refer to the applicable agency or program guide for derivative classification guidance involving SCI or SAP.

(U) This version is effective immediately.

(U) This guide is produced and maintained by the Office of Security, Information Security Division (OSY/ISD) on my behalf and will be updated as necessary. Direct unclassified questions or comments to OSY/ISD via email to osy_infosec@doc.gov.

(U) This guide is issued under the authority of EO 13526 and 32 CFR Section 2001.15. As Designated Original Classification Authority (OCA) of the Department of Commerce and as Director, Office of Security, I hereby approve the issuance of this classification guide and authorize its use by the Department and subordinate Bureaus and Offices.

NICHOLAS SCHNARE
Digitally signed by NICHOLAS SCHNARE
Date: 2024.05.22 09:47:46 -04'00'

Nicholas M. Schnare
Original Classification Authority
Director for Security
Office of Security

Date: May 22, 2024

(U) DOCUMENT CHANGE LOG

Change Number	Date of Change Notice
Version 1.1: Administrative changes. Removed references to Information and Personnel Security Division (IPSD) and replaced with Information Security Division (ISD), clarified definitions, and updated and relocated classification INT-3 from Table 1.5 to FOR-8 in Table 1.4 .	May 22, 2024

(U) Refer to Section 1.5 for the procedure to submit a change request to the guide.

1. (U) GENERAL INFORMATION

1.1 (U) PURPOSE

(U) The *Department of Commerce (DOC) National Security Information Classification Guide (DOC NSICG)*, hereafter referred to as the "Guide," identifies frequently recurring items of national security information and provides guidance on whether information in these categories should be designated UNCLASSIFIED (U), CONFIDENTIAL (C), or SECRET (S).

(U) Classification is reserved for specific categories of information or the compilation of related information meeting the standards and criteria for classification as defined in EO 13526 and falling within one or more of the categories of information eligible for classification per Section 1.4 of EO 13526. The Guide does not provide classification guidance or protection for Top Secret (TS), Sensitive Compartmented Information (SCI) or Special Access Programs (SAP). Derivative classifiers must refer to the specific and appropriate SCI or SAP source document(s) or classification guide(s) to mark and protect such information. The Department's classification authority only extends to information originated by the Department of Commerce. This guide shall be cited as the basis for classification, reclassification, and declassification of information produced by DOC. Information produced and classified by another Federal agency shall retain the classification and markings of the originating agency, even if that guidance conflicts with this Guide.

(U) This guide also provides information that does not meet the criteria for classification under EO 13526, but are nonetheless sensitive and require protection against unauthorized disclosure. This information shall be categorized as Controlled Unclassified Information (CUI).

(U) All DOC and bureau personnel with appropriate security clearances and accesses are authorized to derivatively classify DOC produced information by reference to, and in accordance with the Guide.

(U) ***All classification markings used in the Guide are for illustration purposes only.***

1.2 (U) AUTHORITY

(U) The authority to cite this Guide is based upon EO 13526, "Classified National Security Information," Information Security Oversight Office (ISOO) Implementing Directive, "Classified National Security Information" (32 CFR Part 2001), and the DOC Manual of Security Policies and Procedures. This guide is approved by the Director for Security, DOC, a delegated SECRET Original Classification Authority.

1.3 (U) SCOPE AND APPLICABILITY

(U) The primary mission of the DOC is to create economic growth. For this reason, the DOC is largely a consumer of classified national security information as opposed to an originator of said information, therefore the majority of derivative classification actions will be based on source document(s). This Guide is a tool to supplement instances where source document(s) are unavailable or insufficient. Only information that meets the specific requirements of EO 13526 may be designated as Classified National Security Information (CNSI). Law enforcement and criminal information does not meet EO 13526 classification standards and should ONLY be designated as classified when there is a clearly identifiable and describable national security nexus. The over-classification of information, including law enforcement and criminal information, shall be avoided.

(U) This Guide is for the use of DOC employees, contractors, and personnel detailed to DOC from other agencies—the "Users"—performing derivative classification actions when addressing the elements of national security information. Anyone who disseminates national security information which requires classification are obligated to classify the information based upon the source document(s), this Guide, and/or a compartmented program guide/manual. Users of this Guide are expected to use their subject matter expertise and professional judgement prior to applying classification to ensure that only information that meets the requirements of EO 13526 is classified. Individuals who fail to protect classified national security information may be subject to criminal, civil, and administrative sanctions outlined in section 5.5 of EO 13526.

(U) Guidance for marking and protecting Controlled Unclassified Information is available in the U.S. Department of Commerce Controlled Unclassified Information (CUI) Policy dated August 2019, published by the Office of the Chief Information Officer (OCIO).

1.4 (U) REPRODUCTION AND RELEASE OF THE GUIDE

(U) This Guide may be reproduced and disseminated within the DOC as needed. Dissemination of this Guide or information herein to government agencies outside of the DOC will be coordinated through the Office of Security, Information Security Division (ISD).

(U) Requests for public release of information will be addressed in accordance with Federal statutes, rules, and regulations, which provide for access to this material.

(U) Requests for copies of this Guide by non-government officials will be addressed in accordance with the Freedom of Information Act (FOIA). The procedures for filing FOIA and Privacy Act requests with the DOC can be found on the DOC Office of Privacy and Open Government (OPOG) website.

1.5 (U) OFFICE OF PRIMARY RESPONSIBILITY

(U) This Guide is produced and maintained by OSY/ISD and will be updated as necessary. Change requests may be sent to OSY/ISD using the Change Request Form provided in Appendix B. Requests will be reviewed within seven business days. Determinations will be made as soon as possible, but no more than 90 days from the date of receipt.

(U) Requestors will receive written notice of determination on each change request. If a request is denied, the rationale for the denial will be included in the notification. Accepted requests will be incorporated into the Guide. Revisions will be accomplished periodically and as circumstances require, but at least once every five years.

The Office of Primary Responsibility for the DOC NSICG	
Department of Commerce	Office of Security (OSY) Information Security Division (OSY/ISD)
Street Address	1401 Constitution Ave NW
City, State and Zip Code	Washington, D.C. 20230
E-mail	osy_infosec@doc.gov

1.6 (U) WHEN THE GUIDE IS INADEQUATE

(U) Should the Guide not provide adequate classification guidance, an Original Classification Authority

must classify the data.

(U) The primary mission of the Department of Commerce continues to be the promotion of economic growth. As such, components should carefully consider operational issues when proposing or evaluating new classification guidance. Law enforcement information may only be classified when there is a clear and describable risk to national security. Over-classification of law enforcement information may have significant impact on the ability to share information appropriately with law enforcements partners.

1.7 (U) EXCEPTIONAL CIRCUMSTANCES

(U) If a determination is made that information or a compilation requires classification or should be classified at a different level, the information will be handled and safeguarded in accordance with the level of classification the holder believes appropriate.

(U) The information should be marked with the tentative level of classification with the notation *"Pending Classification Review"* added and transmitted by a means approved for the level of classification to OSY/ISD for a coordinated classification determination with the appropriate OCA. Commonly occurring information not covered in this or any other classification guide will be added to the appropriate classification guide by an OCA.

(U) When information is derivatively classified from source documents, the classifier shall observe and respect the original classification decision and carry forward to any newly created document the pertinent classification markings. Superseded or obsolete markings may be checked against the Intelligence Community (IC) Register and Manual. Additional questions may be directed to the originating office or OSY/ISD .

1.8 (U) SUPPLEMENTAL GUIDANCE

(CUI) Users of this Guide are encouraged to supplement it with additional classification guidance tailored to their specific operational requirements or functional responsibilities. All such supplemental guidance developed by Commerce Offices and Bureaus must be coordinated with OSY/ISD . OSY/ISD will insure they reflect current DOC policies, Executive Orders, and ISOO directives. All DOC supplemental guides must be provided to OSY/ISD for entry into the DOC central repository.

(U) The absence of an item in the Guide does not imply it is Unclassified. If this Guide does not address information that appears to meet the criteria for classification, contact OSY/ISD for guidance. Until specific guidance is received, treat the information as classified and mark it at its likely level, with the following notation: "Pending Classification Review by OSY/ISD ." Address unresolved classification and dissemination questions to OSY/ISD .

2. (U) CLASSIFICATION MANAGEMENT

2.1 (U) CONFLICTS

(U) Regarding the use of DOC information classified and marked in accordance with prior classification guidance, DOC personnel will use their subject matter expertise and professional judgement to determine whether a conflict exists between the guidance provided prior to this Guide.

(U) If there is a conflict, the instructions in the current Guide will prevail and information will be remarked with the classification level derived from the Guide. If the information was marked with a

specific date for declassification, that date will not be changed. If the information was not marked with a specific date, the declassification date will be determined in accordance with the Guide, with calculations of 10 years, 15 years, 25 years, or 50 years made from the date the information itself was originated as opposed to the date of new document creation. The declassification date will be determined in accordance with the version of the Guide in effect when the source document was originated. It is not necessary to re-mark information in files or databases until the information is extracted or otherwise used.

(U) Conflicts between this Guide and other classification guides regarding the marking of information should be reported to the OSY/ISD for de-confliction of guidance with the appropriate OCA(s). Generally, the information at issue will be protected at the highest level required by any of the opposing classification guides.

2.2 (U) LEVELS OF CLASSIFICATION

(U) Information is classified at one of the following three levels based upon the potential *damage to national security*, which refers to the level of 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, and utility:

(U) *TOP SECRET* applies to information, the unauthorized disclosure of which reasonably could be expected to cause ***exceptionally grave damage*** to the national security;[1]

(U) *SECRET* applies to information, the unauthorized disclosure of which reasonably could be expected to cause ***serious damage*** to the national security;

(U) *CONFIDENTIAL* applies to information, the unauthorized disclosure of which reasonably could be expected to cause ***damage*** to the national security.

(U) Classified information must be safeguarded in accordance with EO 13526, 32 CFR Part 2001, and the DOC Manual of Security Policies and Procedures.

2.3 (U) ELIGIBILITY FOR CLASSIFICATION

(U) Classification may be applied ONLY to information that is owned by, produced by or for, or is under the control of the United States Government. Section 1.4 of EO 13526 states that information shall not be considered for classification unless it concerns the following, which are noted as "Reasons" with their letters in parentheses (e.g., 1.4(a)):

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 the national security;
f. United States Government programs for safeguarding nuclear materials or facilities;

[1] This is for informational purposes only. This guide does not allow for the classification above SECRET.

g. Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or
h. The development, production, or use of weapons of mass destruction.

(U) Section 1.7(a) of EO 13526 mandates that information shall not be classified, continue to be maintained as classified or fail to be declassified to:

- Conceal violations of law, inefficiency, or administrative error;
- Prevent embarrassment to a person, organization, or agency;
- Restrain competition; or
- Prevent or delay the release of information that does not require protection in the interest of the national security.

2.4 (U) CLASSIFICATION BY COMPILATION

(U) Data that individually is unclassified or classified at a lower level, may become classified or classified at a higher level when combined or compiled in a single document if the information reveals an additional association or relationship, not otherwise revealed in the individual data items, that meets the standards for classification under EO 13526. Likewise, data that is not individually controlled may become controlled when combined or compiled in a single document, if the compiled information meets the criteria for applying control marking(s) under relevant policy and is not otherwise controlled by classification and control markings of the individual data items. Applying classification and control markings by compilation can be a derivative classification action based on original classification and control marking guidance or an original classification action.

(U) If the classification and control markings by compilation reveals a new aspect of information, that meets the criteria for classification, but that is not yet defined in an applicable classification guide as an approved classification by compilation, it must be referred to an OCA with jurisdiction over the information to make an original classification decision. When a classification or control marking dissemination is made based on compilation, clear instructions must appear with the compiled information as to the circumstances under which the individual portions constitute a classified and/or controlled compilation, and when they do not.

2.5 (U) POTENTIAL FOR CLASSIFICATION OF INFORMATION, REGARDLESS OF SOURCE/AUTHORITY FOR COLLECTION

(CUI) Information collected pursuant to DOC investigative methods are subject to review by DOC personnel for any portion or portions, which could potentially jeopardize the success of a national security investigation, thereby placing United States national security in jeopardy.

(CUI) Regardless of the method used to obtain the information, if the release of a portion or portions could reasonably be expected to jeopardize U.S. national security interests, then the information may require classification pursuant to DOC classification guidelines.

(CUI) While unclassified techniques typically produce unclassified returns/results, there are instances in which information received via an unclassified source is later treated as classified by the DOC. In addition to information received via Confidential Human Sources (CHS), surveillance logs, and

State/Local/Tribal authorities, this can also apply to information collected via criminal search warrant or other investigative means.

2.6 (U) CLASSIFICATION CHALLENGE

(U) If the classification level(s) and duration(s) mandated in this Guide impose requirements considered impractical, or some information is of such a unique nature or extremely sensitive to require higher levels of protection, or any contributory factors indicate a need for change(s) in this Guide, documents and justified recommendations should be made to the OSY/ISD staff. Pending final determination, the information in question will be protected at the highest level of either the current classification or the recommended change. Additional guidance regarding the Department's formal and informal challenge processes can be found in the DOC Manual of Security Policies and Procedures.

2.7 (U) DECLASSIFICATION

(U) Classified information may only be declassified by an OCA or declassification authority with jurisdiction over the information. If there is any uncertainty as to the proper declassification authority, consult OSY/ISD.

2.8 (U) Foreign Disclosure

(U) DOC Offices and Bureaus sometimes require exchanges of information with foreign governments or international organizations. Sharing of information with foreign entities is not automatic and must be in accordance with protocols established in DOC Manual of Security Policies and Procedures and applicable U.S. export control regulations.

(U) Any classified information classified by another U.S. government agency or using another agencies Security Classification Guide shall be reviewed and cleared with the originator prior to release to foreign governments.

2.9 (U) FOREIGN GOVERNMENT INFORMATION

(U) Foreign government information (FGI) is defined as:

- (U) Information provided to the United States 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;
- (U) Information produced by the United States 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;
- (U) Information received and treated as "Foreign Government Information" under the terms of a predecessor order (EO 13526, Section 6.1).

(U) FGI, to include foreign relations or foreign activities of the United States and confidential sources, is among the categories of information that may be classified if an OCA determines the unauthorized disclosure of the information could reasonably be expected to damage U.S. national security (EO 13526, Section 1.2(a); 1.4(d)).

(U) Foreign derived information is often itself sensitive and the need for classification will be clear based upon its substance. This will not always be the case, however. If public release of the information would deter the foreign government or official from sharing information in the future, the information should be classified even if the information is not by itself sensitive. Users of this Guide must, based on their professional experience and subject matter expertise, determine if there is a foreseeable negative reaction of the originating country to the release of its information. If a foreseeable negative reaction exists, the information should be classified to a level commensurate with similar national security information.

3. (U) MARKING GUIDANCE

(U) Derivative classification is the act of incorporating, paraphrasing, restating, or generating in new form information that is already classified and marking the newly developed material consistent with the markings of the source information. The source information ordinarily consists of a classified document or documents, or a classification guide issued by an OCA.

(U) When making a derivative classification decision using the Guide, the instructions provided in the national security classification tables are to be applied to the derivative document. Derivative classifiers will cite ("DOC NSICG, dated month/year) on the derived line, followed by declassification instructions as specified in the guide. Derivative citations in this Guide shall not be used to overrule classification decisions made by outside agencies or entities.

When non-DOC information is to be included in DOC documents, the classification level of that information should remain as marked by the originator.

3.1 (U) DERIVATIVE CLASSIFICATION MARKINGS

(U) Classification markings are the principal means for identifying national security information that requires protection. All classified information (whether derivatively or originally classified) must be uniformly and conspicuously marked to leave no doubt about the classified status of the information, the level of protection required, and the duration of classification. The marking guidance provided here is not all-inclusive and is instructional as to how derivative information should be marked when using the Guide. Please refer to the ISOO Marking Classified National Security Information booklet, consult with your Bureau Security Office, or contact OSY/ISD if you have any questions or require additional instruction on classified marking requirements.

(U) EO 13526 requires the following primary markings on derivatively classified information:

- Portion markings;
- Overall classification markings; and
- Classification authority block consisting of:
    - A **"Classified By"** line to include the identity, by name and position, or by personal identifier of the derivative classifier, in a manner that is immediately apparent on each derivatively classified document;
    - A **"Derived From"** line, which concisely identifies the source document(s) or the classification guide; and
    - A **"Declassify On"** line which identifies the instructions on the "Declassify On" line from the source document(s), or the duration instruction from a classification guide.

(U) Classification marking requirements are not dependent on the medium (e.g., audio recordings, briefings, cables, electronic documents, e-mail, graphics, hardcopy documents, instant messages, memos, spreadsheets, video, web content, and wiki/blog entries etc.). If markings cannot be affixed to classified information or materials, the originator shall provide holders or recipients of the information with written instructions for protecting the information.

3.1.1. (U) PORTION MARKINGS

(U) EO 13526 requires that each portion of a document be marked to indicate its classification level. A portion is ordinarily defined as a paragraph, but also includes subjects, titles, graphics, tables, charts, bullet statements, sub-paragraphs, classified signature blocks, bullets and other portions within slide presentations.

(U) Unclassified portion markings consist of the letters "(U)" for UNCLASSIFIED and "(CUI)" for CONTROLLED UNCLASSIFIED INFORMATION. The abbreviations, in parentheses, are placed before the portion to which they apply.

(U) Classified portion markings consist of the letters "(C)" for CONFIDENTIAL, "(S)" for SECRET, and "(TS)" for TOP SECRET. The abbreviations, in parentheses, are placed before the portion to which they apply.

(U) Dissemination controls apply restrictive caveats to the Classification Level. For instance, some types of classified information may not be shared with foreign nationals, whether allies to the United States, or not. In this instance, a dissemination of "NOFORN" is applied to the classification level of the information. When portion marking, the classifier would place "//NF" after the marking, and the entire document would then be classified with the caveat "//NOFORN."

(U) When using the Guide and its national security classification tables, the classification level indicated will be used to determine the portion markings. For example, if information is being classified based on line item FOR-3, Table 1.7 Foreign Government Information and Relationships (FOR), the classifier portion marks that information as (*EXAMPLE*) "S//NF" (*EXAMPLE*) per the classification level specified in the Guide.

TABLE 1.1 ADMINISTRATIVE (ADM)

Item #	Category of Information	Class Level	Dissemination	Reason	Declass On	Remarks
ADM - 2	(U) Information whose unauthorized disclosure could jeopardize the success of a current or future national security operational activity.	S	See remarks	1.4 c	See remarks	(U) Case dependent and will require consultation from SMEs. (U) Disseminate in accordance with operational activity as necessary. (U) DECL ON - + 25, as an exception declassify after completion of the operational activity if no additional operations in the future might be jeopardized by release of this information.

3.1.2 (U) OVERALL CLASSIFICATION MARKING

(U) All classified documents require an overall classification marking indicating the highest classification level (TOP SECRET, SECRET, or CONFIDENTIAL) of any one portion within the document. The overall classification marking is the principal mechanism for documenting the sensitivity of any information; the failure to include an overall classification marking generally indicates that the information is UNCLASSIFIED. Unclassified documents may have the marking UNCLASSIFIED and if applicable, additional dissemination control markings.

(U) The overall classification marking must appear in all capital letters, centered in the document header and footer of each page using a conspicuous font size and type. If the document contains more than one page, place the overall classification at the top and bottom of the outside of the front cover, on the title page, on the first page, and on the outside of the back cover (if any). Mark other internal pages with the overall classification or with a marking indicating the highest classification level of information contained on that page.

(U) For media formats (such as web pages) that do not allow for standard headers and footers as described above, a good faith effort must be made to ensure that the classification banner is displayed conspicuously and that it will remain with the information.

3.1.3. (U) DERIVATIVE CLASSIFICATION AUTHORITY BLOCK

(U) All classified documents require a classification authority block. EO 13526 requires a **three-line classification block for Derivative classification decisions** consisting of:

- "**Classified By**" line – identifies the derivative classifier.
- "**Derived From**" line– identifies the source document(s) used to make the derivative classification determination.
- "**Declassify On**" line – identifies the duration of classification according to the source document(s) used to make the derivative classification determination.

(U) The classification authority block requirement applies to all classified information regardless of its format or media and must appear on the first page or face of the document. Generally, the block is placed at the bottom-left of the first page; however, it may appear anywhere on the first page of the document as long as it remains conspicuous. For media formats (such as web pages) that do not allow for standard headers and footers, the classification authority block should appear in a conspicuous location near the top of the first page of the document, below the classification header, to ensure that the block always appears on the first page.

(U) The example below shows the derivative classification authority block in the standard vertical format, with each of the required values appearing in its own line. This is the preferred format and should be used whenever practical.

Classified By: John Doe, Program Analyst
Derived From: DOC NSICG 1, FOR-4
Declassify On: 20320910

(U) When necessary for document formatting or other considerations, an abbreviated, single-line

horizontal block is also acceptable, but only if it remains conspicuously placed on the first page of the document. For example:

DRV BY: John Doe, Program Analyst DOC DRV FROM: DOC NSICG 1, FOR-4 DECL ON: 20320910

*3.1.1.1. (U) "***Classified By***" line*

(U) Derivative classifiers shall be identified by name and position, or by personal identifier, in a manner that is immediately apparent on each derivatively classified document. If not otherwise evident, the agency and office of origin shall be identified and placed immediately following the name and position or other personal identifier provided in the "**Classified By**" line.

(U) Do not confuse the "**Classified By**" line requirement with an original classification decision. The "Classified By" line identifies you as the derivative classifier and other elements of the classification authority block further identify the document as a derivative decision.

*3.1.1.2. (U) "***Derived From***" line*

(U) Derivative classifiers are required to concisely identify the source document(s) or security classification guide on the "**Derived From**" line, including the agency and where available, the office or origin, and the date of the source or guide. The "**Derived From**" line in the classification authority block is based on the source for the derivative classification determination. Derivative classifiers have three possible sources for their decision:

- One or more classified source document(s);
- A derivative citation from a security classification guide; or
- Another applicable classification guide (e.g., for SCI or specific program).

(U) The line items for classifying information in the Guide are organized into categories for easy reference. The subsections in the section each contain the rules – listed numerically under the "Item No." column – for one category. A fully identified "**Derived From**" citation, when the reason to classify is based on one line item in the national security classification tables in the Guide, will include the following:

- The Security Classification Guide and version number (DOC NSICG 1);
- The category code; and
- The item number within the category.

(U) For example, if a document is classified based on line item INT-3, from Table 1.5 Intelligence (INT), your "**Derived From**" line would be:

TABLE 1.1 ADMINISTRATIVE (ADM)						
Item #	**Category of Information**	**Class Level**	**Dissemination**	**Reason**	**Declass On**	**Remarks**
ADM - 2	(U) Information whose unauthorized disclosure could jeopardize the success of a current or future national security operational activity.	S	See remarks	1.4 c	See remarks	(U) Case dependent and will require consultation from SMEs. (U) Disseminate in accordance with operational activity as necessary. (U) DECL ON - + 25, as an exception declassify after completion of the operational activity if no additional operations in the future might be jeopardized by release of this information.

Derived From: DOC NSICG 1, INT-3

(U) If multiple line items of the Guide apply within a document, it is sufficient to cite DOC NSICG 1 in the "Derived From" line of the classification block.

Derived From: DOC NSICG 1

(U) NOTE: As a security "best practice," we recommend that if multiple line items (up to four) of the Guide apply within a document, those line items should be cited individually in the "Derived From" line of the classification block. For example:

Derived From: DOC NSICG 1, INT-3, INT-8, INT-11[2]

(U) When using multiple source documents, including the Guide, the "Derived From" line shall appear as:

Derived From: Multiple Sources

(U) **NOTE:** When citing multiple sources, the derivative classier shall include a listing of the source materials on, or attached to, each derivatively classified document in accordance with EO 13526 requirements. There is no required placement of the source list within the document, only that it be included in, or attached to, the document.

*3.1.1.3. (U) "***Declassify On***" line*

(U) Derivative classifiers are required to carry forward the instructions on the "**Declassify On**" line from the source document to the derivative document, or the duration instruction from the classification guide. Information derivatively classified based on the Guide shall be marked for declassification in accordance with the "**Declassify On**" national security classification tables of the Guide.

(U) For example, if a document is classified based on line item INT-3, Table 1.5 Intelligence (INT) your "**Declassify On**" line would be:

[2] This is just an example, some of these do not exist.

Declassify On: [enter a declassification date 25 years from the date of the document]

TABLE 1.1 ADMINISTRATIVE (ADM)						
Item #	**Category of Information**	**Class Level**	**Dissemination**	**Reason**	**Declass On**	**Remarks**
ADM- 2	(U) Information whose unauthorized disclosure could jeopardize the success of a current or future national security operational activity.	S	See remarks	1.4 c	See remarks	(U) Case dependent and will require consultation from SMEs. (U) Disseminate in accordance with operational activity as necessary. (U) DECL ON - + 25, as an exception declassify after completion of the operational activity if no additional operations in the future might be jeopardized by release of this information.

(U) If a document is classified based on multiple line items in the Guide, or on the basis of more than one source document, the "Declassify On" line shall reflect the longest classification duration of any of the sources referenced.

(U) "**Declassify On**" dates shall be written using the "YYYYMMDD" format.

3.2 (U) DISSEMINATION CONTROLLED MARKINGS

(U) Dissemination Controls are control markings that identify the expansion and limitation on the distribution of information. These markings are in addition to and separate from the levels of classification defined by EO 13526. Examples of control markings include but not limited to: Originator Control (ORCON), Not Releasable to Foreign Nationals (NOFORN), Authorized For Release To [USA, LIST] (REL TO [USA, LIST], and Releasable by Information Disclosure Official (RELIDO). Additional guidance on the use of control markings is available within the Intelligence Community *Directive (ICD) 710 Classification Management and Control Markings System*.

3.3 (U) FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

(U) The FISA statute provides that information collected pursuant to the statute "may not be disclosed for law enforcement purposes unless the disclosure is accompanied by a statement that such information, or any information derived there from, may be used in a criminal proceeding only with advance authorization of the Attorney General." (50 United States Code [U.S.C.] 1806, 1825, 1845).

(U) In addition to portion marking paragraphs containing FISA derived material, an appropriate FISA warning statement must be included and co-located with the information collected using FISA methods. Users should consult the appropriate National Security Division point of contact for further instructions on marking and handling FISA-derived material.

(U) FISA Warning(s) are required when FISA intelligence information is included in a document. The FISA Warning text is specified by the FISA court with jurisdiction over the information in conjunction with the agency using the information. One or more FISA Warnings may be applicable on a single document. The FISA Warning is to be co-located with the information collected using FISA methods. For media in which the placement of the FISA Warning(s) with the FISA information is not possible, the FISA Warning covering the majority of the FISA information must appear at the top of the first printed or viewed page

of the document.

3.4 (U) UNCLASSIFIED CONTROL MARKINGS

(U) CUI markings will be applied in accordance with the DOC CUI Policy, 32 CFR Part 2002, EO 13556, the National Archives and Records Administration CUI Marking Handbook pursuant to EO 13526 and the Intelligence Community Markings System Register and Manual.

3.5 (U) CLASSIFIED BY COMPILATION: COMPILATIONS OF UNCLASSIFIED INFORMATION

(U) Section 1.7(e) of EO 13526 states that compilations of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that: (1) meets the standards for classification under the Order; and (2) is not otherwise revealed in the individual items of information. EO 13526 also defines compilation as an aggregation of pre-existing unclassified items of information.

(U) For the purpose of marking a document, this means that it may be possible to have a classified document in which all the individual portions are unclassified but because the compilation of the unclassified information reveals an association or relationship not otherwise evident when the portions are used individually, classification of the document and the application of required classification markings are warranted. In these cases, as required by 32 C.F.R. Part 2001.24(g), clear instructions must be provided as to the circumstances under which the individual portions constitute a classified compilation and when they do not.

(U) Two additional crucial points to consider are: (1) as with all other markings, information must be marked in a uniform and conspicuous manner so as to leave no doubt as to the classified status of the information, the level of protection required, the reason for classification, and the duration of classification; and (2) access to or the sharing of unclassified information must not be impeded by unnecessarily or inappropriately applying classification where it's not warranted.

(U) The following are examples of markings that may be applied to documents that are classified by compilation:

> Classified by compilation: The individual portions of this document are unclassified (and may be used, stored, transmitted, and shared as unclassified) except where otherwise noted within the body of the document.
>
> Classified by compilation: The weight of widget "A," when combined with or used in association with the height of widget "A," is classified SECRET. In all other instances the individual portions or combinations of portions of this document are UNCLASSIFIED.

4. (U) NATIONAL SECURITY CLASSIFICATION TABLES

(U) Users should review the classification tables for the subject area pertaining to their topic. Match the citation item to your situation column. The level column provides the classification level of that item. The remaining items are self-explanatory.

(U) Users are reminded that the Guide provides common terminology and common classification baselines that can be used among the various DOC components and agencies involved in national security activities. DOC components are encouraged to supplement the Guide with specialized

classification guidance/instructions tailored to their particular programs or requirements when necessary. Nothing herein is intended to supersede or alter the existing procedures, guidelines, or authorities of the individual DOC components for their internal national security activities.

(U) The line items for classifying information in this Guide are organized into categories for easy reference. The subsections in the section each contain the rules – listed numerically under the "Item No." column – for one category. A fully identified "**Derived From**" reference includes:

- The Security Classification Guide and version number (DOC NSICG 1.0);
- The category code; and
- The item number within the category.

(U) Due to varying policies affecting the use of foreign disclosure and dissemination control markings, the determination and use of applying these restrictive markings, is left to the responsibility of individual components. Users of this Guide shall ensure appropriate coordination of information involving other agency equities is undertaken prior to dissemination. If multiple line items (up to four) of the Guide apply within a document, cite the line items individually in the "**Derived From**" line of the classification block. If more than four line items of this SCG apply within a document, it is sufficient to cite DOC NSICG 1.0 in the "**Derived From**" line of the classification block.

(U) "**Declassify On**" dates are indicated as + 25, + 15, or + 10. Enter a "**Declassify On**" date 25, 15, or 10 years from the date of the document. "**Declassify On**" 50X1-HUM, +DATE is a specific marking that is limited to information that clearly and demonstrably could be expected to reveal the identity of a confidential human source or a human intelligence source. When citing the confidential source or human intelligence source line item, the "**Declassify On**" date will be 50X1-HUM, a date 75 years from the date of the document. For example: 50X1-HUM, 20870101

TABLE 1.1 ADMINISTRATIVE (ADM)

(U) ADMINISTRATIVE (ADM) Reference to an item from this table would be written as DOC NSICG 1, ADM-[item #] "Declass On" + 25, + 15, or + 10 - enter a "Declassify On" date 25, 25, or 10 years from the date of the document.						
Item #	**Category of Information**	**Class Level**	**Dissemination**	**Reason**	**Declass On**	**Remarks**
ADM-1	(U) Information derived from classified legislative or judicial branch documents.	See remarks				(U) Classify per the classification of the source document.
ADM-2	(U) Information whose unauthorized disclosure could jeopardize the success of a current or future national security operational activity.	S	See remarks	1.4 c	See remarks	(U) Case dependent and will require consultation from SMEs. (U) Disseminate in accordance with operational activity as necessary. (U) DECL ON - + 25, as an exception declassify after completion of the operational activity if no additional operations in the future might be jeopardized by release of this information.
ADM-3	(U) The fact that OSY validates and processes all clearance data passed in and out of DOC for its affiliates and visitors	CUI	SP-PERS			
ADM-4	(U) The fact that OSY reviews and approves procedures for the collection and destruction of classified waste.	CUI	PHYS			(U) Details of specific procedures may require handling as CUI or may require classification. (U) Note: classified waste does not include permanent official records.
ADM-5	(U) Staffing levels, grades, personnel qualification, names, supporting vendors and contractors.	CUI	SP-PERS			(U) Compiled lists are unclassified with CUI//SP-PERS handling, as they relate to employees of Federal agencies.

U.S. Department of Commerce
Office of Security

TABLE 1.2 INVESTIGATIONS (INV)

(U) INVESTIGATIONS (INV) Reference to an item from this table would be written as DOC NSICG 1, INV-[item #] "Declass On" + 25, + 15, or + 10 (enter a "Declassify On" date 25, 25, or 10 years from the date of the document.						
Item #	**Category of Information**	**Level**	**Dissemination**	**Reason**	**Declass On**	**Remarks**
INV-1	(U) Identity of a Confidential Human Source, or organization, providing information to the DOC on law enforcement/criminal matters.	CUI	INF			
INV-2	(U) Reports of investigations or information reports that identify classified information derived from another document.	See Remarks				(U) Classify per the classification of the source document.
INV-3	(U) DOC documentation relating to undercover operations which identify sensitive sources or methods.	CUI	INV			
INV-4	(U) Data reports for registered sources or cooperating witness.	CUI See Remarks	INV			(U) Classify per the classification of the source data report.

TABLE 1.3 CONTINUITY OF OPERATIONS (COOP)

(U) CONTINUITY OF OPERATIONS (COOP) Reference to an item from this table would be written as DOC NSICG 1, COOP-[item #] "Declass On" + 25, + 15, or + 10 - enter a "Declassify On" date 25, 15, or 10 years from the date of the document. *(U) Components are instructed to consult the Emergency Operations Center (202-482-5100/ eoc@doc.gov) for additional classification guidance for DOC-owned facilities that warrant protection of classified information.*						
Item #	**Category of Information**	**Class Level**	**Dissemination**	**Reason**	**Declass On**	**Remarks**
COOP-1	(U) Alternate location interagency dependencies.	See remarks				(U) DOC presence and operations at alternate locations will be classified in accordance with security guidance issued by the Federal agency of the owning facility. (U) Minimum classification is CUI//EMGT
JOINT AND FEDERAL CONTINUITY OF GOVERNMENT (COG) CONSIDERATIONS						
FACILITIES						
COOP-2	(U) Identifying alternate location capabilities, vulnerabilities, or occupants/tenants.	See remarks				(U) Classify in accordance with security guidance issued by the Federal agency of the owning facility. (U) Minimum classification is CUI//EMGT
COOP-3	(U) The fact that an individual DOC employee is assigned to relocate to an alternate location as part of the Emergency Relocation Group (ERG).	See remarks				(U) Classify in accordance with security guidance issued by the Federal agency of the owning facility. (U) Minimum classification is CUI//EMGT

(U) CONTINUITY OF OPERATIONS (COOP) Reference to an item from this table would be written as DOC NSICG 1, COOP-[item #] "Declass On" + 25, + 15, or + 10 - enter a "Declassify On" date 25, 15, or 10 years from the date of the document. *(U) Components are instructed to consult the Emergency Operations Center (202-482-5100/ eoc@doc.gov) for additional classification guidance for DOC-owned facilities that warrant protection of classified information.*						
Item #	**Category of Information**	**Class Level**	**Dissemination**	**Reason**	**Declass On**	**Remarks**
COOP-4	(U) Identification of a particular facility as a DOC alternate location.	See remarks				(U) Classify in accordance with security guidance issued by the Federal agency of the owning facility. (U) Minimum classification is CUI//EMGT
COOP-5	(U) The fact of DOC presence at a Federal facility, which happens to be an alternate location.	See remarks				(U) Classify in accordance with security guidance issued by the Federal agency of the owning facility. (U) Minimum classification is CUI//EMGT
RESOURCES, POLICIES, CAPABILITIES						
COOP-6	(U) Specific operational capabilities at alternate locations.	See remarks				(U) Classify in accordance with security guidance issued by the Federal agency of the owning facility, or by other valid guidance as indicated in this Guide. (U) Minimum classification is CUI//EMGT
COOP-7	(U) Specific mission critical data necessary to conduct essential functions.	See remarks				(U) Data will be classified or unclassified per guidance issued specific to the data as may be found in other sections of this Guide.
TESTING, TRAINING, REPORTING						

(U) CONTINUITY OF OPERATIONS (COOP) Reference to an item from this table would be written as DOC NSICG 1, COOP-[item #] "Declass On" + 25, + 15, or + 10 - enter a "Declassify On" date 25, 15, or 10 years from the date of the document. *(U) Components are instructed to consult the Emergency Operations Center (202-482-5100/ eoc@doc.gov) for additional classification guidance for DOC-owned facilities that warrant protection of classified information.*						
Item #	**Category of Information**	**Class Level**	**Dissemination**	**Reason**	**Declass On**	**Remarks**
COOP-8	(U) Detailed COOP after action reports that identify specific vulnerabilities.	See remarks				(U) Classify in accordance with security guidance issued by the Federal agency of the owning facility, or by other valid guidance as indicated in this Guide. (U) Minimum classification is CUI//EMGT
INFRASTRUCTURE, TECHNOLOGY, AND COMMUNICATION						
COOP-9	(U) Vulnerabilities of power, telecommunications, and internet grids servicing alternate locations.	See remarks				(U) Classify in accordance with security guidance issued by the Federal agency of the owning facility, or by other valid guidance as indicated in this Guide. (U) Minimum classification is CUI//CRIT/EMGT
COOP-10	(U) Risk assessments of alternate locations.	See remarks				(U) Classify in accordance with security guidance issued by the Federal agency of the owning facility, or by other valid guidance as indicated in this Guide. (U) Minimum classification is CUI//EMGT/PHYS

(U) CONTINUITY OF OPERATIONS (COOP) Reference to an item from this table would be written as DOC NSICG 1, COOP-[item #] "Declass On" + 25, + 15, or + 10 - enter a "Declassify On" date 25, 15, or 10 years from the date of the document. *(U) Components are instructed to consult the Emergency Operations Center (202-482-5100/ eoc@doc.gov) for additional classification guidance for DOC-owned facilities that warrant protection of classified information.*						
Item #	**Category of Information**	**Class Level**	**Dissemination**	**Reason**	**Declass On**	**Remarks**
COOP-11	(U) Vulnerabilities of communication capabilities at alternate locations.	See remarks				(U) Classify in accordance with security guidance issued by the Federal agency of the owning facility, or by other valid guidance as indicated in this Guide. (U) Minimum classification is CUI//EMGT/ISVI

TABLE 1.4 FOREIGN GOVERNMENT INFORMATION AND RELATIONSHIPS (FOR)

(U) FOREIGN GOVERNMENT INFORMATION AND RELATIONSHIPS (FOR) Reference to an item from this table would be written as DOC NSICG 1, FOR-[item #] "Declass On" + 25, + 15, or + 10 (enter a "Declassify On" date 25, 15, or 10 years from the date of the document.						
ITEM #	**CATEGORY OF INFORMATION**	**CLASS LEVEL**	**DISSEM**	**REASON**	**DECLASS ON**	**REMARKS**
FOR-1	(U) **General** discussions of the benefits and risks of international cooperation.	CUI	INTL			(U) Includes generic discussions of sharing intelligence.

(U) FOREIGN GOVERNMENT INFORMATION AND RELATIONSHIPS (FOR) Reference to an item from this table would be written as DOC NSICG 1, FOR-[item #] "Declass On" + 25, + 15, or + 10 (enter a "Declassify On" date 25, 15, or 10 years from the date of the document.						
ITEM #	**CATEGORY OF INFORMATION**	**CLASS LEVEL**	**DISSEM**	**REASON**	**DECLASS ON**	**REMARKS**
FOR-2	(U) Information received from a foreign government, which the originating government has marked as classified, to include "Restricted".	See remarks		1.4 b	+ 25	(U) Retain the original classification markings or use their U.S. equivalent. See 32 CFR § 2001.54 for additional information. (U) "Restricted" information is considered classified by most foreign governments as a fourth level of classification, which the U.S. does not have. In these instances: CLASS LEVEL – "C/FGI-MOD", for "CONFIDENTIAL – Modified Handling". In addition, FGI, followed by the trigraph of the originating country. (U) Consult the DOC Manual of Security Policies and Procedures on the handling and safeguarding of "CONFIDENTIAL – Modified Handling". (U) Components should consult their appropriate legal and/or international offices for country specific guidance.
FOR-3	(U) Information provided by a foreign government which is unclassified provided in confidence.	CUI See remarks	INTL			(U) Such information shall be classified in accordance with "C/FGI-MOD", for "CONFIDENTIAL – Modified Handling" if the unauthorized disclosure of FGI is presumed to cause damage to the national security. (U) Consult the DOC Manual of Security Policies and Procedures on the handling and safeguarding of "CONFIDENTIAL – Modified Handling".
FOR-4	(U) Information provided pursuant to an existing treaty, agreement, bilateral exchange or other obligation.	See remarks				(U) Classify at the level and for the duration specified in the relevant agreement. (U) Components should consult their appropriate legal and/or international offices for country specific guidance.

(U) FOREIGN GOVERNMENT INFORMATION AND RELATIONSHIPS (FOR) Reference to an item from this table would be written as DOC NSICG 1, FOR-[item #] "Declass On" + 25, + 15, or + 10 (enter a "Declassify On" date 25, 15, or 10 years from the date of the document.						
ITEM #	**CATEGORY OF INFORMATION**	**CLASS LEVEL**	**DISSEM**	**REASON**	**DECLASS ON**	**REMARKS**
FOR-5	(U) Information generated in a joint effort of the United States and one or more foreign governments.	See remarks				(U) CLASS LEVEL – The level and duration of classification agreed upon by participants. See 32 CFR § 2001.54 for additional information. (U) Information may be considered for REL in accordance with established relationships. (U) Components should consult their appropriate legal and/or international offices for country specific guidance.
FOR-6	(U) Information about the extent of DOC cooperation with a particular foreign government **in general**.	CUI	INTL			
FOR-7	(U) Information about the extent of DOC cooperation with a particular foreign government on a particular national security case.	CUI	INTL			(U) If the information about the case is classified, classify per the classification of the source document.
FOR-8	(U) Identification of foreign countries being provided CNSI.	See remarks				(U) If sharing information that has been classified based on this Guide, then identifications of countries being provided CNSI shall be classified as CUI//INTEL//NOFORN. (U) When sharing products that have been classified by another agency or using another agency's classification guide, please refer to that agency for classification guidance.

TABLE 1.5 INTELLIGENCE (INT)

(U) INTELLIGENCE (INT) Reference to an item from this table would be written as DOC NSICG 1, INT-[item #] "Declass On" + 25, + 15, or + 10 (enter a "Declassify On" date 25, 15, or 10 years from the date of the document.						
Item #	**Category of Information**	**Class Level**	**Dissemination Control**	**Reason**	**Declass On**	**Remarks**
INT-1	(U) Complete listing of DOC national security intelligence requirements.	CUI	INTEL			(U) Information obtained in response to an intelligence requirement may be classified.
INT-2	(U) Domestic distribution lists for intelligence products, identifying offices but not names of persons.	CUI	INTEL			

(U) GLOSSARY OF TERMS

(U) Access. The ability and opportunity to gain knowledge of classified information.

(U) Applicable Associated Markings. Markings, other than those that designate classification level, that are required to be placed on classified documents. These include the "Derived From" line, downgrading and declassification instructions, special control notices, Special Access Program caveats, etc.

(U) Automatic Declassification. The declassification of information based solely upon: (1) the occurrence of a specific date or event as determined by the original classification authority, or (2) the expiration of a maximum time frame for duration of classification established under Executive Order 13526.

(U) Classification. The act or process by which information is determined to be classified information.

(U) Classification Guidance. Any instruction or source that prescribes the classification of specific information.

(U) Classification Guide. A documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

(U) Classification Management. The life-cycle management of classified national security information from original classification to declassification.

(U) Classified Document. Any recorded classified information, regardless of its physical form or characteristics, including, without limitation, written or printed matter, tapes, charts, maps, paintings, drawing, engravings, sketches, working notes and papers; reproductions of such things by any means or process; and sound, voice, magnetic, or electronic recordings in any form.

(U) Classified National Security Information. Information that has been determined pursuant to Executive Order 13526, or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. Also known as classified information.

(U) Classifier. An individual who makes a classification determination and applies a security classification to information or material. A classifier may be an original classification authority (OCA) or a person who derivatively assigns a security classification based on a properly classified source or a security classification guide.

(U) Communications Security (COMSEC). Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes crypto security, transmission security, emissions security, and physical security of COMSEC material.

(U) Compilations of Unclassified Information. An aggregation of pre-existing unclassified items of information. Items of information, which are individually unclassified, may be classified if the compiled

information reveals an additional association or relationship that meets the criteria for classification under Executive order 13526, and is not otherwise revealed by the individual items of information.

(U) Component. Any Office, Board, Division, or Bureau that is part of the Department of Commerce.

(U) Controlled Unclassified Information (CUI). Information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. CUI does not include classified information or information a non-executive branch entity possesses or maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Specific details about the types of information considered to be CUI can be found in NARA's final rule, 32 CFR § 2002, as amended.

(U) Confidential. Information, the unauthorized disclosure of which could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

(U) 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.

(U) Cover. Mechanism whereby the affiliation of a person, organization, installation, facility, or activity to U.S. Government intelligence agencies, organizations, or activities, or in some cases even generically to the U.S. Government itself, is disguised and protected from unauthorized disclosure. Cover is provided when that intelligence or governmental affiliation is classified in the interests of national security pursuant to relevant statutes and Executive Orders, and when disclosure of such affiliation reasonably could be expected to cause harm to national security.

(U) Covert. An operation that is planned and executed as to conceal the identity of or permit plausible denial by the sponsor.

(U) Damage to the National Security. Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information.

(U) Declassification. The authorized change in the status of information from classified information to unclassified information.

(U) Declassification Authority. The official who authorized the original classification, if that 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.

(U) Derivative Classification. Incorporating, paraphrasing, restating, or generating in new form information that is already classified and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

(U) Dissemination Controls. Markings that define the distribution limitation of a category of information. They are in addition to and separate from the levels of classification defined by EO 13526. Some require a control-specific warning notice at the beginning of any document conveying those data. Several are assigned solely by their proponent agency. Outside organizations may not be authorized to make those determinations but may only convey the caveat assigned by the proponent.

(U) Downgrading. A determination that classified information requires, in the interest of national security, a lower degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect a lower degree of protection.

(U) Employee. A person, other than the president, and Vice President, employed by, detailed or assigned to, an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head.

(U) Event. An occurrence or happening that is reasonably certain to occur and that can be set as the signal for automatic declassification of information.

(U) 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 of Executive Order 13526.

(U) Foreign Power. (a) A foreign government or any component thereof, whether or not recognized by the United States; (b) a faction of a foreign nation or nations, not substantially composed of United States persons; (c) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments; (d) a group engaged in international terrorism or activities in preparation thereof; (e) a foreign-based political organization, not substantially composed of United States persons; or (f) an entity that is directed and controlled by a foreign government or governments.

(U) Information. Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government.

(U) Intelligence Sources and Methods. Sources are persons, images, signals, documents, data bases, and communications media capable of providing intelligence information through collection and analysis programs (e.g., Human Intelligence, Imagery Intelligence, Signal Intelligence, Geospatial Intelligence, and Measurement and Signature Intelligence); and methods are information collection and analysis strategies, tactics, operations, and technologies employed to produce intelligence products. If intelligence sources or methods are disclosed without authorization, their effectiveness may be

substantially negated or impaired. The term "intelligence sources and methods" is used in legislation and executive orders to denote specific protection responsibilities of the Director of National Intelligence.

(U) Memorandum of Agreement (MOA). Document that describes the specific actions and responsibilities of each party so that their goals may be accomplished. A MOA identifies and describes the specific responsibilities, and actions to be taken, by each of the parties to alleviate any ambiguity of who is to do what and so that the goals of each party may be accomplished.

(U) Memorandum of Understanding (MOU). Document that describes very broad concepts of mutual understanding, goals, and plans between parties. A document used whenever there is agreement to exchange information or coordinate programs where each party is responsible for contributing its own efforts and resources. A MOU describes comprehensive concepts of mutual understanding, goals, and plans shared by the parties. It is used to discuss an agreement in a broad spectrum outlining the overall goal, so it is clear.

(U) Multiple Sources. Two or more source documents, classification guides, or a combination of both.

(U) National Intelligence. All intelligence, regardless of the source from which derived and including information gathered within or outside the U.S., that (A) pertains, as determined consistent with any guidance issued by the President, to more than one U.S. Government agency; and (B) that involves: (i) threats to the U.S., its people, property, or interests; (ii) the development, proliferation, or use of weapons of mass destruction; or (iii) any other matter bearing on U.S. national or homeland security.

(U) National Intelligence Program (NIP). Intelligence activities of the U.S. Government that provide the President, other officers of the Executive Branch, and the Congress with national intelligence on broad strategic concerns bearing on U.S. national security.

(U) National Security. The national defense or foreign relations of the United States.

(U) Need-to-know. A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information to perform or assist in a lawful and authorized governmental function.

(U) Original Classification. The initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

(U) 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.

(U) Overt. Activities that are openly acknowledged by or are readily attributable to the U.S. government, including those designated to acquire information through authorized and open means without concealment. Overt information may be collected by observation, elicitation, or from knowledgeable human sources.

(U) Representative of Foreign Interest. An individual or group that acts on behalf of a foreign government or enterprise.

(U) 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.

(U) Security Classification Guide. A documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

(U) Sensitive Information. Any information, the loss, misuse, modification of, or unauthorized access to, could affect the national interest, law enforcement activities, the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (USC), but that has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy.

(U) Sensitive Compartmented Information (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled exclusively within formal control systems established by the Director of National Intelligence.

(U) Source Document. An existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

(U) Tempest. The study and control of electronic signals emitted by electrical equipment.

(U) Threat. The intention and capability of an adversary to undertake actions that would be detrimental to the interests of the U.S.

(U) 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.

(U) Unauthorized Disclosure. A communication or physical transfer of classified information to an unauthorized recipient.

(U) Vulnerability. Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

(U) APPENDIX A: REFERENCES

a. Executive Order 13526, "Classified National Security Information," December 29, 2009

b. 32 CFR Part 2001, "Classified National Security Information: Final Rule," Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA)

c. 32 CFR Part 2002, "Controlled Unclassified Information (CUI)", Information Security Oversight Office (ISSO), National Archives and Records Administration (NARA)

d. DOC Manual of Security Policies and Procedures

e. DOC Controlled Unclassified Information (CUI) Policy

f. ISOO booklet "Marking Classified National Security Information," latest revision

g. Executive Order 12333, "United States Intelligence Activities," as amended

h. Executive Order 12829, "National Industrial Security Program"

i. Executive Order 12968, "Classified National Security Information"

j. Executive Order 13549, "Classified National Security Information Program for State, Local Tribal and Private Sector Entities"

k. Executive Order 13556, "Controlled Unclassified Information"

l. Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information"

m. Intelligence Community Directive (ICD) 403, "Foreign Disclosure and Release of Classified National Intelligence"

n. ICD 710, "Classification Management and Control Markings System"

o. IC Policy Guidance 710.1, "Application of Dissemination Controls: Originator Control"

p. Homeland Security Presidential Directive (HSPD)-7, "Critical Infrastructure, Identification, Prioritization, and Protection

q. Title 5, USC 552, "Freedom of Information Act "

(U) APPENDIX B: CHANGE REQUEST FORM

CHANGE REQUEST
For the DOC NSICG

To: Director for Security, Office of Security **Date:** _____

From Originator of request:

Name: _____ **Organization:** _____ **Office:** _____

Proposed Change: ☐ New item ☐ Modification ☐ Challenge

Item to be changed:	**Change description (any other items affected)**
Page:	
Topic:	
Item #:	

Rationale for Change:

This section to be completed by OSY/ISD

Change Request Number:
Date of Response:
Action Officer:

OSY/ISD Decision: ☐ Yes (approved) ☐ No (not approved)

If "No" justification for denial of change request: