DoD Manual 5200.45

Original Classification Authority and Writing a Security Classification Guide

Originating Component:	Office of the Under Secretary of Defense for Intelligence and Security
Effective:	January 17, 2025
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Manual 5200.45, "Instructions for Developing Security Classification Guides," April 2, 2013, as amended
Incorporates and Cancels:	See Paragraph 1.2.
Approved by:	Milancy D. Harris, Acting Under Secretary of Defense for Intelligence and Security

Purpose: In accordance with the authority in DoD Directive (DoDD) 5143.01 and the guidance in DoD Instruction (DoDI) 5200.01, this issuance:

- Assigns original classification authority (OCA) responsibilities and provides original classification processes.
- Prescribes procedures to develop security classification guides (SCG) pursuant to Executive Order (E.O.) 13526 or successor order, and Part 2001.15 of Title 32, Code of Federal Regulations (CFR).

TABLE OF CONTENTS

TABLES

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance applies to OSD, the Military Departments (MILDEPs), the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

1.2. SUMMARY OF INCORPORATION AND CANCELLATION.

This issuance incorporates and cancels portions of Volumes 1 and 3 of DoD Manual (DoDM) 5200.01, as described in Tables 1 and 2. Upon publication of this issuance, Volumes 1 and 3 of DoDM 5200.01 will be administratively changed to remove the language canceled by this issuance.

Table 1. Volume 1 of DoDM 5200.01 Cancellation Actions

Enclosure, Paragraph	Action
Enclosure 2, Paragraph 4.	Incorporates and Cancels
Enclosure 2, Paragraph 7.n.	Incorporates and Cancels
Enclosure 3, Paragraph 5.g.	Incorporates and Cancels
Enclosure 4, Paragraphs 1. through 8.	Incorporates and Cancels
Enclosure 4, Paragraph 13.a.	Incorporates and Cancels
Enclosure 4, Paragraph 13.c.	Incorporates and Cancels
Enclosure 4, Paragraph 14.	Incorporates and Cancels
Enclosure 4, Paragraph 15.	Incorporates and Cancels
Enclosure 6	Incorporates and Cancels

Table 2. Volume 3 of DoDM 5200.01 Cancellation Actions

Enclosure, Paragraph	Action
Enclosure 5, Paragraph 5.	Incorporates and Cancels
Enclosure 6, Paragraph 9.	Incorporates and Cancels

SECTION 2: RESPONSIBILITIES

2.1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY (USD(I&S)).

As the DoD Senior Agency Official (SAO) for Security, the USD(I&S):

a. Except for the MILDEPs, approves the delegation of Secret level OCAs.

b. Provides an annual list of DoD officials, by position, delegated OCA to the Director, Information Security Oversight Office.

c. Establishes guidance for SCGs.

d. Oversees the DoD Fundamental Classification Guidance Review (FCGR).

2.2. DIRECTOR FOR DEFENSE INTELLIGENCE (COUNTERINTELLIGENCE, LAW ENFORCEMENT, AND SECURITY) (DDI(CL&S)).

Under the authority, direction, and control of the USD(I&S), the DDI(CL&S) reviews all DoD OCA requests, except MILDEP requests, before USD(I&S) or Secretary of Defense consideration.

2.3. UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING.

The Under Secretary of Defense for Research and Engineering, through the Administrator, Defense Technical Information Center (DTIC), maintains the official DoD repository of SCGs classified at the level of Secret or below, and the SCG index to administer secondary distribution of SCGs.

2.4. DIRECTOR, DOD SPECIAL ACCESS PROGRAM (SAP) CENTRAL OFFICE.

Under the authority, direction, and control of both the Deputy Secretary of Defense and the Performance Improvement Officer and Director of Administration and Management, the Director, DoD SAP Central Office:

a. Establishes guidance on the development, distribution, and maintenance of SAP SCGs.

b. Oversees the FCGR for all SAP SCGs.

2.5. SECRETARIES OF THE MILDEPS.

The Secretaries of the MILDEPs, for their respective Military Services:

a. Delegate OCA at the Top Secret level and below in accordance with E.O. 13526 or successor order.

b. Appoint a senior-level civilian as an SAO to direct, administer, and oversee their respective OCA delegations and development and review of SCGs in accordance with Paragraph 5.3.

c. Verify and annually submit to DDI(CL&S) a listing of officials by position within their respective MILDEPs delegated OCA.

SECTION 3: OCA

3.1. ROLES AND RESPONSIBILITIES.

a. OCAs:

(1) As an integral part of the Defense Security Enterprise, must identify and protect the DoD's critical information, operations, and infrastructure through informed classification decisions.

(2) Are senior-level personnel authorized, by position and in writing, by the Secretary of Defense or the USD(I&S), or by the Secretaries of the MILDEPs for the Military Services, to classify information in the first instance.

(3) Issue and disseminate classification guidance for classified elements of information within each system, plan, program, project, or mission under their authority to facilitate the proper and uniform derivative classification of information. All original classification decisions must be incorporated into an SCG and each SCG must be approved in writing by the appropriate OCA. SCGs containing classification decisions made by multiple OCAs must clearly identify the approving OCA by citation. Approving OCAs must:

(a) Have program or supervisory responsibility over the information or be the SAO.

(b) Be authorized to classify information originally at the highest level of classification prescribed in the SCG.

(4) Determine the classification level for each classified element of information in the system, plan, program, project, or mission, and the duration of classification, not to exceed 25 years in accordance with Paragraph 4.2.a.(3).

(5) Determine and include classification by compilation decisions in the SCG in accordance with Paragraph 6.6.

(6) Record original classification decisions in a memorandum when the OCA determines expediency does not allow the SCG to be updated and incorporate those decisions into an SCG as soon as practical but no later than 1 year from date of decision.

(7) Review classification guidance issued under their authority once every 5 years to ensure currency and accuracy, or sooner when necessitated by significant changes in policy or in the system, plan, program, project, or mission, and update the guides as required.

(8) Ensure coordination with reasonably anticipated internal and external stakeholders on all aspects of the SCG during the drafting, coordination, and updating processes.

(9) Coordinate with the Deputy Assistant Secretary of Defense for Nuclear Matters when developing or revising SCGs with information classified in accordance with Title 42, United

States Code, also known as the "Atomic Energy Act of 1954, as amended," including Restricted Data or Formerly Restricted Data elements of information.

(10) Cancel SCGs once all information in the SCG is declassified or incorporated into a new or existing SCG and submit a DD Form 2024, "DoD Security Classification Guide Data Elements," available at https://www.esd.whs.mil/Directives/forms/ to DTIC and DDI(CL&S) in accordance with Paragraph 5.5.

(11) Provide a machine-readable copy of each SCG to DTIC in accordance with the procedures in Paragraph 5.4.

(12) Support litigation involving matters related to Components' classification responsibilities, in coordination with their servicing legal counsel.

b. The classification authority for foreign government information is the foreign government or organization originating the information. Volume 2 of DoDM 5200.01 contains guidance on foreign government information.

c. OCAs must receive and document initial and annual OCA training. See Paragraph 3.3. for specific information.

3.2. MANAGEMENT.

a. All DoD OCAs are accountable to the Secretary of Defense for their classification decisions and should be prepared to produce a written description of the specific damage to national security, as necessary, for:

(1) Classification challenge.

(2) Security classification review.

(3) Damage assessment.

(4) Request for mandatory review for declassification.

(5) Request for release pursuant to Section 552 of Title 5, United States Code, also known as the "Freedom of Information Act."

(6) When pertinent to judicial proceedings.

(7) As other statutes or regulations may require.

b. Individuals delegated OCA for multiple positions must complete training certification for each position pursuant to Paragraph 3.3. Additionally, they must ensure they use the correct position when making classification and declassification decisions.

c. Delegation of OCA will be limited to the minimum number of officials required for effective operation of the mission or operational requirements. The authority will be delegated

to, and retained by, only those officials who have a demonstrable and continuing need to exercise it. DoD Component heads, or their designated SAO, will review OCA delegations annually to ensure all delegated OCA positions are required.

d. These individuals are authorized to delegate OCA at the Top Secret level and below in accordance with Section 1.3.(a) of E.O. 13526:

(1) Secretary of Defense.

(2) Secretaries of the MILDEPs, for their respective Military Services.

e. These SAOs designated in accordance with Section 5.4.(d) of E.O. 13526, or successor order, may delegate OCA at the Secret level and below, provided they have been delegated Top Secret OCA by the agency head in accordance with Section 1.3.(c)(3) of E.O. 13526:

(1) USD(I&S).

(2) Administrative Assistant to the Secretary of the Air Force. Refer to Air Force policy for SAO delegation and responsibilities.

(3) Department of the Army Deputy Chief of Staff for Intelligence (G2). Refer to Army policy for SAO delegation and responsibilities.

(4) Deputy Under Secretary of the Navy. Refer to Navy policy for SAO delegation and responsibilities.

f. Deputies, vice commanders, and similar immediate subordinates of an OCA may exercise OCA when they have been officially designated to assume the duty position of the OCA in an "acting" or "performing the duties of" capacity during the OCA's absence and have certified in writing they have received OCA training pursuant to Paragraph 3.3.

g. Requests for OCA delegation will be approved only when:

(1) There is a demonstrable and continuing need to exercise OCA during the normal course of operations.

(2) Such demonstrable and continuing need cannot be met through issuance or revision of SCGs by an existing OCA in the chain of command. See Paragraph 3.2.i. for additional guidance.

(3) Sufficient expertise and information are available to the prospective OCA to permit effective classification decision-making.

h. All DoD Component requests for new OCA delegations, excluding from the MILDEPs, will be submitted to DDI(CL&S) at osd.pentagon.rsrcmgmt.list.ousd-intel-infosec-mbx@mail.mil. The Office of the Director, Information and Acquisition Protection in DDI(CL&S) staffs all OCA delegation requests to the appropriate level for approval.

(1) Combatant Commands will send all OCA delegation requests to the Chief, Joint Staff Security Office for endorsement and Joint Staff submission to the DDI(CL&S).

(2) The designated SAOs in the MILDEPs manage the delegation of OCAs within their respective MILDEPs and provide an updated list of OCA positions to DDI(CL&S) annually.

i. OCA delegation requests will:

(1) Identify the official by position title and classification level requested.

(2) Include a description of why the official requires OCA and why the classification level requested is necessary and appropriate. If the position's next-level supervisor has OCA, requests will include a justification why it is either inappropriate or impractical for that official to exercise OCA.

(3) Be submitted and endorsed by an official at least one supervisory level above the official to whom the request seeks delegation of OCA. See Figure 1 for an example of an OCA delegation request memorandum.

Figure 1. Example of Request for OCA

[Letterhead]

[Date]

MEMORANDUM FOR DIRECTOR FOR DEFENSE INTELLIGENCE
(COUNTERINTELLIGENCE, LAW ENFORCEMENT, AND
SECURITY)

SUBJECT: Delegation of [Secret or Top Secret] Original Classification Authority to [position title]

Request delegation of [classification level] original classification authority in accordance with Executive Order 13526 to the [position title].

[Justification for why OCA is required for this position]

[Signature block for senior official requesting the delegation of OCA]

j. All DoD Component requests for these changes to OCAs, excluding those from the MILDEPs, require submission of a memorandum from the Component SAO to the DDI(CL&S) detailing the reason for the change, which includes:

(1) Move of the position delegated OCA due to reorganization or realignment.

(2) Position title change.

(3) Removal or downgrade of OCA delegation.

k. All DoD Components, including the MILDEPs, must verify the officials by position delegated OCA to the DDI(CL&S) annually. See Figure 2 for an example of an OCA verification submission. This verification will include:

(1) A list of OCAs by position title and the classification level delegated.

(2) The date each OCA received the initial or annual refresher training.

Figure 2. OCA Verification Example

Position Title	Classification Level			Date OCA Last Received Annual Training
	Top Secret	Secret	Confidential	
Deputy Under Secretary of Defense for Intelligence and Security	1			12/9/21

3.3. TRAINING REQUIREMENTS.

a. Before exercising OCA, and annually thereafter, officials delegated OCA will certify in writing that they have received the required training. This acknowledgement can be accomplished through any method determined by the DoD Component (e.g., signing a certificate or form). Individuals who hold OCA for multiple positions must complete the certification for each position delegated OCA.

b. Personnel assigned responsibility for creating, reviewing, and managing SCGs and submitting information to OCAs for original classification decisions require additional knowledge of the original classification decision process and will take the OCA training annually in addition to all other security training requirements. Completion of this training will be tracked by the activity security manager and will not give the individual the authority to make original classification decisions.

c. The activity security manager, or other designated personnel, will ensure:

(1) OCA training is conducted as required. Training may be completed through individualized Component-developed training or through the OCA training course available on the Defense Counterintelligence and Security Agency Center for Development of Security Excellence Website at https://www.cdse.edu/Training/eLearning/IF102/.

(2) Copies of the training records are maintained in accordance with DoDI 5015.02.

(3) Training records are available when requested by appropriate authorities.

d. At a minimum, the OCA training will address:

(1) Classification standards and authority.

(2) Prohibitions and limitations on classifying information including the need to avoid over-classification.

(3) Classification principles and procedures, including marking and information sharing requirements, and sharing limitations. See Section 4 for additional details.

(4) Proper application of safeguarding protections when using, storing, reproducing, transmitting, disseminating, and destroying classified information.

(5) Criminal, civil, and administrative sanctions that may be brought against an individual who fails to classify information properly or fails to protect classified information from unauthorized disclosure.

e. OCAs who do not receive this training at least once within a calendar year will have their classification authority suspended by the agency head or SAO until the training is completed and acknowledgement has been signed. The agency head or SAO may grant a waiver of this requirement if the official delegated OCA is unable to receive the training due to unavoidable circumstances. In such cases, the official delegated OCA must take the training as soon as practicable.

3.4. RESPONSIBILITIES WHEN CLASSIFIED INFORMATION IS COMPROMISED.

Pursuant to Volume 1 of DoDM 5200.01, OCAs will:

a. Verify the classification and duration of classification initially assigned to the information.

b. Immediately reevaluate the assigned classification level to determine whether the classification will be continued or changed. This classification review should consider these possibilities:

(1) The information has lost all or some of its sensitivity since it was initially classified and may be downgraded or declassified;

(2) The information has been so compromised by a security incident that attempting to protect it further as classified is unrealistic or inadvisable and should be declassified; or

(3) The information should continue to be classified at its current level. In rare cases, it may be the sensitivity of the information has increased and the classification should be upgraded.

c. Upon completion of the damage or impact assessment in accordance with Volume 3 of DoDM 5200.01, advise the activity reporting the compromise of the outcome of the classification review or damage assessment.

d. Assess the impact of the compromise on the affected system, plan, program, or project. Consider countermeasures that may be taken to minimize, mitigate, or limit damage to national security and prevent further loss or compromise.

e. Assess the cost implications of information, operational, or technology losses; developmental and integration costs of countermeasures; likelihood of countermeasure success; and programmatic impacts of the unmitigated loss or compromise of specific classified information.

f. Initiate or recommend adoption of countermeasures.

(1) Countermeasures should be applied as quickly as possible and may be initiated before completion of the classification review or damage assessment.

(2) Countermeasures may include changing plans or system design features, revising operating procedures, providing increased protection to related information, or other appropriate actions.

g. Follow security incident procedures and conduct a damage assessment in accordance with Volume 3 of DoDM 5200.01.

SECTION 4: ORIGINAL CLASSIFICATION

4.1. PRINCIPLES.

a. Information can be originally classified only if:

(1) An OCA is classifying the information.

(2) The information is owned by, produced by or for, or is under the control of the U.S. Government (USG).

(3) The information meets the criteria for classification pursuant to E.O. 13526 or a successor order.

(4) Another OCA has not already classified the information. Review the DTIC SCG index at https://discover.dtic.mil/ to determine if an SCG exists that covers the same or similar information. See Paragraph 5.11. for more information on horizontal coordination.

(5) The OCA determines the unauthorized disclosure of the information reasonably could be expected to result in damage to national security, and the OCA can identify or describe the damage. Table 3 shows the decision process for determining the classification level.

Table 3. Classification Level Decision Process

Classification Level	Confidential	Secret	Top Secret
Impact Level	High Impact	Extreme Impact	Catastrophic Impact
Unauthorized disclosure would reasonably be expected to cause damage	**Damage** to operations, assets, or individuals	**Serious damage** to operations, assets, or individuals	**Exceptionally grave damage** to operations, assets, or individuals
Potential impact to operations, capabilities, or service deliveries	Degradation in (or loss of) a capability to an extent and duration that one or more primary functions cannot be performed	Degradation in (or loss of) a capability to an extent or duration that a significant proportion of the primary functions cannot be performed	Catastrophic or disastrous degradation in (or loss of) an operation, capability, or service
Guidelines for assigning classification levels	Development of operation of policies are impeded	• Disruption of foreign relations • Substantial impairment of a program or policy directly related to national security • Disclosure of significant military plans or intelligence operations • Compromise of significant scientific or technological developments relating to national security	• Armed aggression against the U.S. or its allies • Interference with foreign relations which vitally affects national security • Compromise of vital national defense plans or complex cryptologic and communication intelligence systems • Disclosure of sensitive intelligence operations or sources • Release of state-of-the-art scientific or technological developments vital to national security • Loss of life

b. The OCA will determine the appropriate duration of classification to be applied to the information in accordance with Paragraph 4.2.a.(3).

c. The OCA will document classification decisions clearly and concisely in writing.

d. If there is significant doubt about the need to classify information, it will not be classified.

e. Classified information will not be declassified automatically because of any unauthorized disclosure of identical or similar information.

f. Information will not be classified, continue to be maintained as classified, or fail to be declassified to:

(1) Conceal violations of law, inefficiencies, or administrative errors;

(2) Prevent embarrassment to a person, organization, or agency;

(3) Restrain competition; or

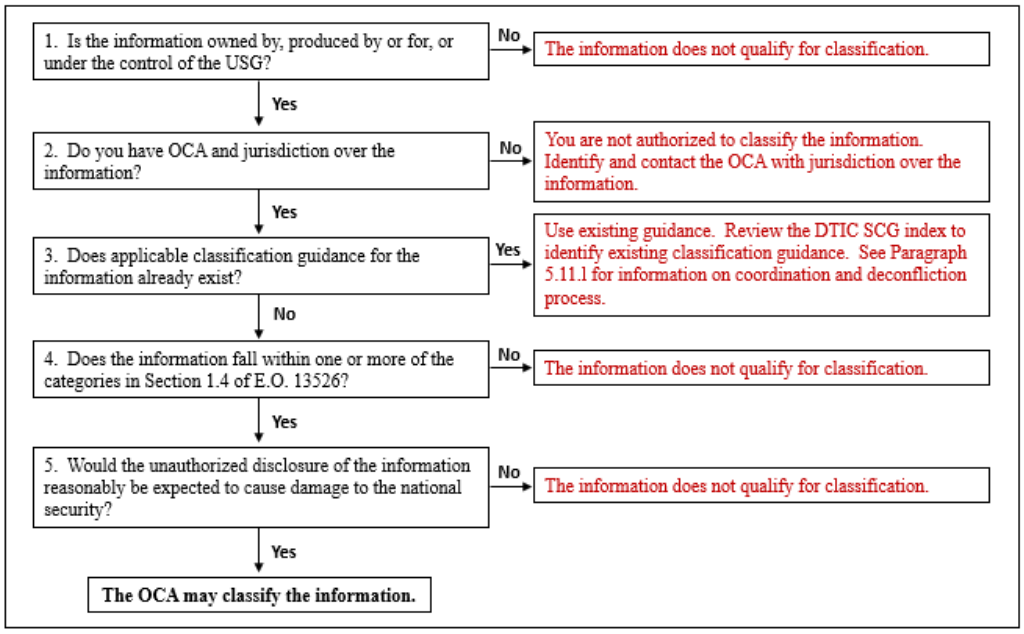
(4) Prevent or delay the release of information that does not require protection in the interest of national security.

g. Basic scientific research information not clearly related to national security will not be classified.

h. The unauthorized disclosure of foreign government information is presumed to cause damage to national security.

i. Figure 3 shows the steps taken to determine if the information can be classified.

Figure 3. Process to Determine if Information Can be Classified



4.2. PROCESS.

a. At the time of original classification, the following will be determined:

(1) Reason for classification as defined in Section 1.4. of E.O. 13526.

(2) Classification level.

(a) Downgrading information to a lower level of classification in an established timeframe is appropriate when the information no longer requires protection at the originally assigned level and can be properly protected at a lower level.

(b) Consider including downgrading instructions during the original classification process. Downgrading instructions do not replace declassification instructions but are used with declassification instructions. An example of this is in Volume 2 of DoDM 5200.01.

(3) Duration of classification.

(a) The OCA will establish a specific date or independently verifiable event for declassification up to 25 years based on the duration of the national security sensitivity of the information.

(b) The duration of classification is determined by how long the OCA determines the information requires protection. It is not determined by the classification level.

(c) Exemptions from automatic declassification for information that would clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source (marked as 50X1-HUM) or key design concepts of weapons of mass destruction (marked as 50X2-WMD) are approved in E.O. 13526. Pursuant to Part 2001 of Title 32, CFR, these exemptions can be applied at the time of original classification provided:

1. The Interagency Security Classification Appeals Panel (ISCAP) has been notified.

2. The OCA has program or supervisory responsibility over the information.

3. The information is captured in an SCG.

(d) Exemptions from automatic declassification, other than those indicated in Paragraph 4.2.a.(3)(c) must be approved by the ISCAP in accordance with Paragraph 6.5.b.(4).

(e) When using an event for declassification, include a date not to exceed 25 years from the date of the document (e.g., upon conclusion of mission or June 23, 2046, whichever is sooner). This ensures the classification does not extend beyond 25 years and will be reviewed for automatic declassification.

b. Detailed markings instructions and the derivative classification process are provided in Volume 2 of DoDM 5200.01.

c. Figure 4 shows the original classification process. Factors to consider when determining classification are listed in Figure 5.

Figure 4. Original Classification Process

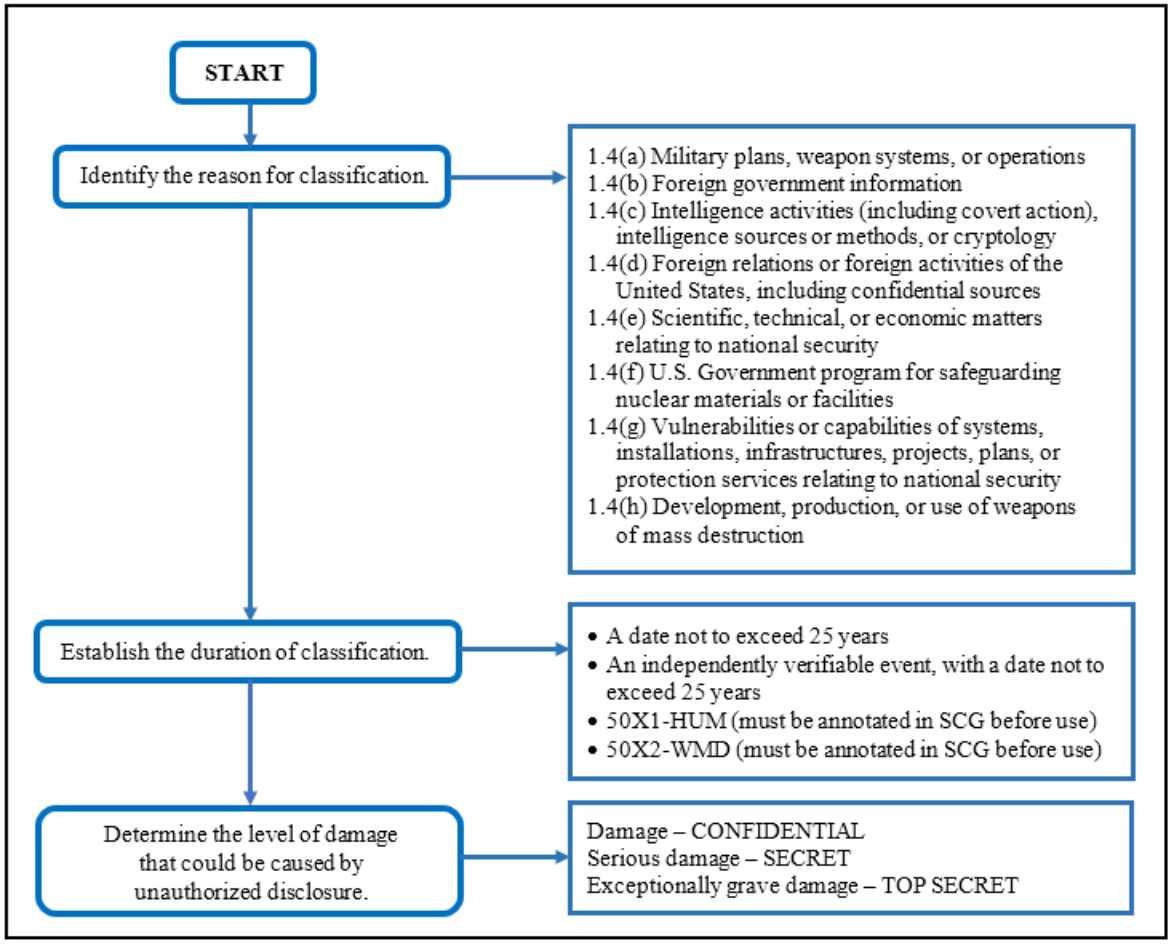
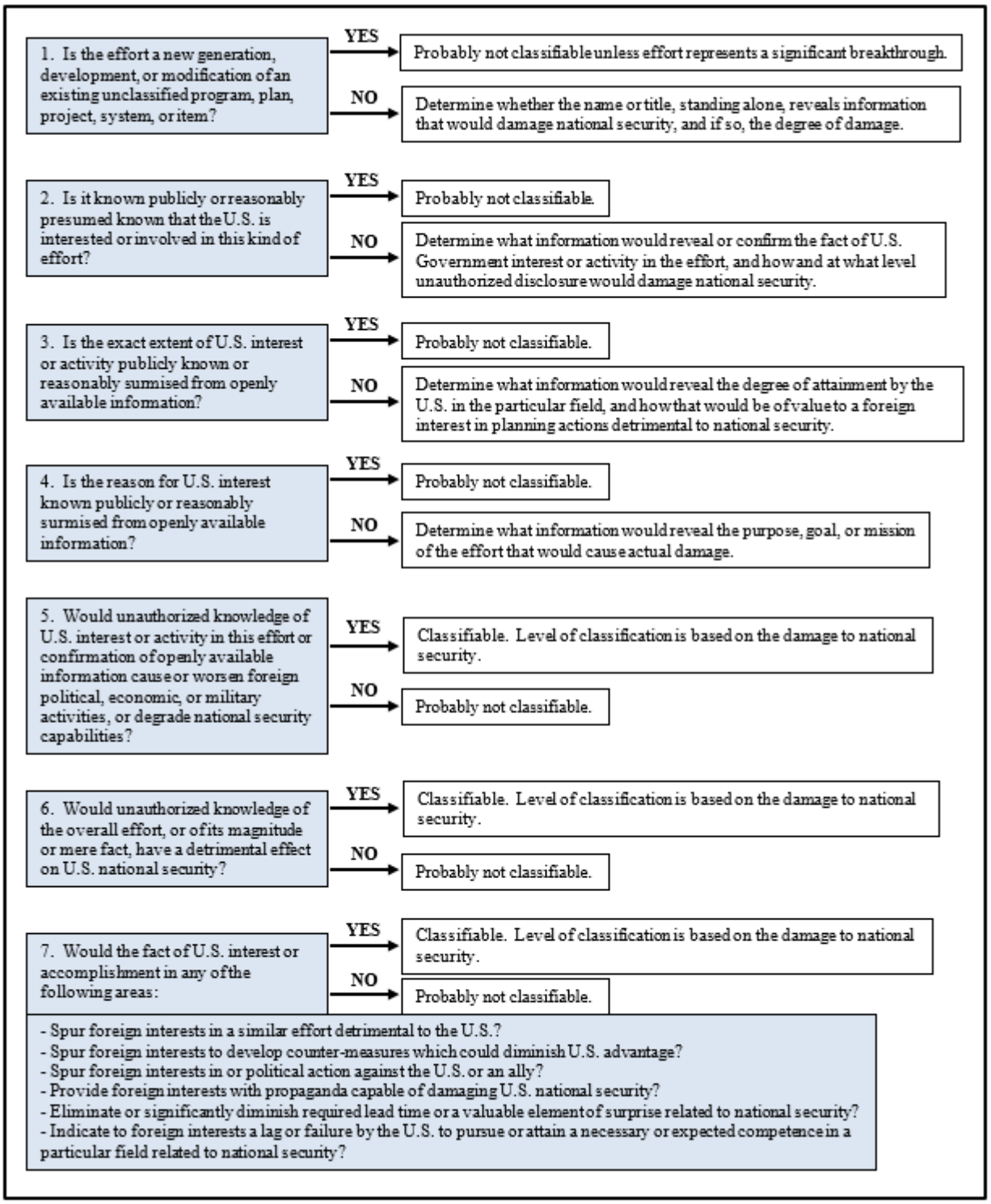


Figure 5. Classification Factors to Consider



SECTION 5: SCGS

5.1. PURPOSE.

a. Classification management procedures require the timely issuance of comprehensive guidance regarding classification of information concerning any system, plan, program, project, or mission under the OCA's jurisdiction, the unauthorized disclosure of which could reasonably be expected to damage national security. Timely and precise classification guidance is a requirement for effective and efficient information security and assures security resources are expended to protect only information truly warranting protection in the interests of national security.

b. OCAs will issue SCGs to:

(1) Facilitate a standardized and efficient classification management program.

(2) Identify DoD information that warrants protection pursuant to E.O. 13526, Part 2001 of Title 32, CFR, and Volumes 1 through 3 of DoDM 5200.01; and identify the classification level, reason for classification, and duration of classification for each element of information.

(3) Promote information sharing, facilitate efficient use of resources, and simplify management of classified national security information (CNSI) and controlled unclassified information (CUI).

(4) Protect information designated CNSI, including classified military information, and CUI from unauthorized disclosure by providing guidance on how to appropriately mark, safeguard, disseminate, declassify or decontrol, and destroy when no longer needed.

5.2. RECORDS MANAGEMENT.

OCAs will ensure SCGs and related content that document the classification process for government records are retained in accordance with their component records management policies and records disposition schedules and DoDI 5015.02 and pursuant to Section 3303 of Title 44, United States Code. Organizations should consult their local records management office for guidance regarding retention requirements.

5.3. MANAGEMENT.

a. SAOs and OCAs oversee the development and review of SCGs.

b. OCAs will issue classification guides as early as practical in the life cycle of the classified elements of each system, plan, program, project, or mission. OCAs should review the requirements of Volumes 1 through 3 of DoDM 5200.01 regarding classification, declassification, downgrading, and marking of CNSI before writing an SCG.

c. SCGs will not be published as a DoD issuance nor included in a DoD issuance. Any SCGs currently approved as an issuance will be rescinded and replaced as soon as practicable in the proper SCG format.

d. Interim classification decisions may be issued in a memorandum format for expediency but must follow the standardized SCG table format. Interim guidance will be incorporated into a formal SCG within 1 year of its signature date. See Paragraph 6.7. for additional information on interim classification decisions.

e. Unclassified SCGs are not authorized for public release and may be protected as CUI as the aggregation of unclassified information may identify critical information that meets the criteria of CUI. Follow the CUI marking instructions in DoDI 5200.48.

f. The Component SAO will maintain a list of their SCGs and will ensure all SCGs are reviewed at least once every 5 years to ensure currency and accuracy and update as necessary. A complete list of current SCGs will be provided annually to DDI(CL&S) at osd.pentagon.rsrcmgmt.list.ousd-intel-infosec-mbx@mail.mil and DTIC at dtic.belvoir.ecm.mbx.acquisitions@mail.mil. If the title of an SCG is classified, an unclassified short title can be used instead.

5.4. DISTRIBUTION.

The originating organization will:

a. Distribute SCGs, including interim classification guidance, to organizations and activities that use information contained in the respective guide.

b. Submit new or revised SCGs (excluding those containing Top Secret, sensitive compartmented information (SCI), or SAP information, or guides deemed by the OCA to be too sensitive for automatic secondary distribution) to DTIC with the DD Form 2024. Secondary distribution allows DTIC to distribute the SCG based on the distribution statement without going back to the originator for permission.

c. For those SCGs that cannot be sent to DTIC (Top Secret, SCI, or SAP information, or guides deemed by the OCA to be too sensitive for automatic secondary distribution), a DD Form 2024 will be sent to DTIC and DDI(CL&S) in accordance with the procedures in Paragraphs 5.5. and 5.6. for accountability and horizontal protection referendums.

5.5. DD FORM 2024.

a. The DD Form 2024 constitutes the sole input to DoD's SCG index managed by DTIC. By submitting the form as required, DTIC can maintain an accurate listing of SCGs.

b. A DD Form 2024 is required for all SCGs, including those not sent to the DTIC repository. Attach the form to the SCG when uploading the documents to DTIC's repository. A copy of all DD Forms 2024 will be sent to DDI(CL&S) at osd.pentagon.rsrcmgmt.list.ousd-intel-

infosec-mbx@mail.mil. If an SCG cannot be sent to DTIC, the reason will be documented on the DD Form 2024 and the form will be uploaded to DTIC.

c. DD Forms 2024 submitted for these reasons will be emailed to DDI(CL&S) and DTIC at dtic.belvoir.ecm.mbx.acquisitions@mail.mil:

(1) SCG cancellation.

(2) OCA transfer.

d. SCGs must be reviewed when required, but at least once every 5 years. The OCA will annotate the review date on the SCG, even if no changes are made during the review, and submit a copy of the SCG and a new DD Form 2024 annotated with the date of review to DTIC and a copy of the DD Form 2024 to DDI(CL&S).

5.6. DTIC.

a. DTIC maintains an index and repository of SCGs on both the Non-Classified Internet Protocol Router Network (NIPRNET) and the SECRET Internet Protocol Router Network (SIPRNET). DTIC does not have a repository for Top Secret SCGs. These links will take you to the DTIC SCG index and repository.

(1) NIPRNET: https://www.dodtechipedia.mil/dodwiki/x/Q4BMHg.

(2) SIPRNET: https://www.dodtechipedia.smil.mil/dodwiki/display/techipedia/Security+Classification+Guide.

b. A copy of all SCGs (excluding Top Secret, SAP, SCI SCGs and SCGs protected by alternative compensatory control measures) with the DD Form 2024 attached will be uploaded to DTIC at:

(1) NIPRNET: https://www.dodtechipedia.mil/dodwiki/x/mgM6BQ.

(2) SIPRNET: https://www.dtic.smil.mil/ecms.

c. Each SCG submitted to DTIC is assigned an accession document (AD) number. This number is automatically emailed to the submitter and will be annotated on the DD Form 2024 for all future actions (e.g., revision, review, cancellation).

d. Once an SCG has been uploaded, notify DTIC of the title of the guide and the AD number at dtic.belvoir.ecm.mbx.acquisitions@mail.mil. DTIC will add the SCG to the index. If uploading a revised SCG, provide the AD number of the previous version so it can be removed from the index and repository.

5.7. TRANSFERRING OWNERSHIP.

a. SCGs belonging to an organization impacted by a realignment become the responsibility of the absorbing organization.

b. SCGs belonging to a disestablished organization become the responsibility of the parent organization.

c. If an SCG is transferred to an office or DoD Component outside the OCA's organization, the originating OCA will report the transfer to DTIC and DDI(CL&S) on a DD Form 2024, and the inheriting organization will report either the re-issuance or administrative rescission of the SCG within the 120-business day timeframe.

d. If classification guidance within an existing SCG is transferred to another SCG, the absorbing SCG will be updated and the original SCG will be superseded. Both actions can be accomplished on the same DD Form 2024.

e. All actions will be recorded on the DD Form 2024 and submitted to DTIC and DDI(CL&S). See Paragraph 5.5. for information about submissions to DTIC.

5.8. CANCELING.

The impact on systems, plans, programs, or projects must be considered when deciding to cancel an SCG.

a. SCGs will be canceled only when:

(1) All information the guides specify as classified has been declassified; or

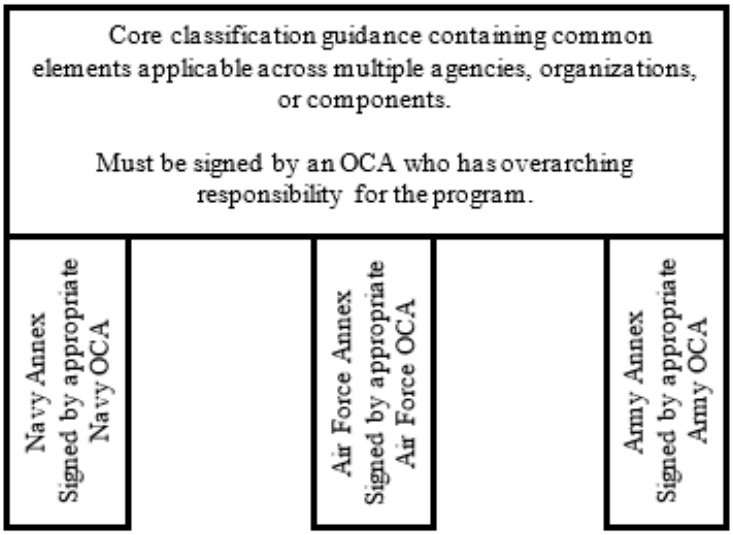
(2) A new SCG incorporates the classified information covered by the old SCG and there is no reasonable likelihood any information not incorporated by the new SCG will be the subject of derivative classification.

b. Declassified information is not approved for public release until a public release review is done in accordance with DoDIs 5230.09 and 5230.29.

5.9. CORE SCG.

Core SCGs are useful when programs cross multiple DoD Components or organizations. A core SCG is developed by incorporating information common to multiple organizations. The signatory OCA would be at a sufficiently high level to have jurisdiction over all affected DoD Components or organizations. The lower-level organizations, in accordance with Component policy requirements, can then develop organization-specific annexes. See Figure 6 for an example of a core SCG.

Figure 6. Example of Core SCG



5.10. FCGR.

a. Pursuant to E.O. 13526, every DoD Component with OCA will receive a tasking memo with instructions on completing the FCGR once every 5 years. The purpose of the review is to:

(1) Ensure all SCGs have been reviewed and updated as necessary, but at least once every 5 years. A schedule should be established to review 20 percent of SCGs each year to alleviate this potential burden where many SCGs may exist under one OCA.

(2) Ensure the guidance reflects current circumstances.

(3) Identify classified information that no longer requires protection and can be declassified.

b. At a minimum, the FCGR will focus on:

(1) Does the classification guidance conform to current operational and technical circumstances, meet the standards for classification in accordance with Section 1.4. of E.O. 13526, or successor order, and assess the likely damage in accordance with Section 1.2. of E.O. 13526?

(2) Has research been conducted to ensure there are no classification conflicts with another OCA's SCG?

(3) Is the dissemination and availability of SCGs appropriate, timely, and effective?

(4) Does the guidance take into consideration new and emerging threats?

c. The Component SAO will oversee their Component's FCGR.

d. Subject matter experts will participate in the FCGR to obtain the broadest possible range of perspectives.

e. Completed FCGR reports will be sent to USD(I&S) for consolidation.

f. The USD(I&S) will provide a detailed report summarizing the results of the review to the Director, Information Security Oversight Office and release an unclassified version to the public except when the existence of the guide or program is itself classified.

g. The FCGR completion will be documented on the DD Form 2024 as the "5-Year Review."

h. As part of the review process, organizations will review DTIC's index and repository and ensure they are up to date.

5.11. WRITING THE SCG.

Follow Component-specific policy. At a minimum, these steps should be taken to write an SCG.

a. Step 1. Read this manual. To effectively write an SCG, follow the guidance provided in this manual as it identifies the processes and procedures to be applied in a step-by-step manner.

b. Step 2. Determine eligibility for classification in accordance with Paragraphs 3.1.a.(3)(a) through (b) and 4.1.

c. Step 3. Review associated SCGs.

(1) Before writing a new SCG or updating a current SCG, it is necessary to find out if any classification guidance exists applicable to items of information concerning the system, plan, program, project, or mission for which the new SCG is being written. Because programs and systems can cross multiple DoD Components, horizontal coordination to ensure consistent classification is critically important. Review the DTIC SCG index to determine if an SCG exists that covers the same or similar information.

(2) Refer to Paragraph 5.6. for information on how to access DTIC's SCG repository. Simple and advanced searches can be conducted via DTIC's Research and Engineering Gateway at https://www.dtic.mil (NIPRNET) or https://www.dtic.smil.mil (SIPRNET).

(3) SCGs dealing with DoD National Intelligence budgetary matters should be compared with and aligned to guidance in the Intelligence Community (IC) budget and associated SCGs.

d. Step 4. Conduct an analysis.

(1) An analysis should be conducted to determine which elements of information warrant protection. This process will identify capabilities providing a programmatic or national advantage, thus requiring classification. See Appendix 5A for detailed information about this analysis. Providing answers to these questions will systematically refine the scope of the analysis.

(2) Consider the state-of-the-art status.

(a) Reasonable classification determinations cannot be made in the scientific and technical field without analysis of what has been accomplished, what is being attempted, and by whom.

(b) Make use of scientific and information services. Consult technical and intelligence specialists. Obtain assistance available from any appropriate source.

(c) Learn about the state-of-the-art, the state of development, attainment in the field of work, and what is known and openly published, including:

1. The known or published status (foreign and domestic).

2. The known but unpublished (possibly classified) status in the United States.

3. The known but unpublished status in friendly and unfriendly countries.

4. The extent of foreign knowledge of the unpublished status in the United States.

(3) Consider the national advantage.

(a) The guide's subject matter must be reviewed as a totality.

(b) Decide what the system, plan, program, project, operation, or mission does or seeks to accomplish resulting in a capability providing an advantage to the United States.

(c) In the final analysis, the decision to classify will be related to one or more of these factors producing, directly or indirectly, the actual or expected national advantage:

1. Fact of interest by the USG in the effort as a whole or in specific parts being considered or emphasized.

2. Fact of possession by the United States.

3. The product's capabilities in terms of quality, quantity, and location.

4. Performance, including operational performance, as it relates to capabilities.

5. Vulnerabilities, weaknesses, countermeasures, and counter-countermeasures.

6. Uniqueness – exclusive U.S. knowledge.

7. Lead time – related to state-of-the-art.

8. Surprise – related to possession and capability to use.

9. Specifications – may be indicative of goals, aims, or achievements.

10. Manufacturing technology.

11. Associations with other data or activities.

(4) Consider the use of framing components for intelligence information. Framing components help users identify information most likely to require protection from unauthorized disclosure. There are three components inherent to the value of all intelligence: From where data comes (source), how data is collected and turned into intelligence (method), and why intelligence is created (mission). See Appendix 5B for more detailed information about framing components for intelligence information.

e. Step 5. Identify specific items of information requiring classification.

(1) The primary function of a classification guide is the identification of the specific items or elements of information requiring protection.

(2) Determine each element of information's safeguarding and dissemination requirements. This includes information meeting the thresholds for classification and CUI.

(3) Identify critical program information in accordance with DoDI 5200.39 when writing SCGs on research, development, and acquisition projects and programs to ensure proper protection, including required distribution statements and warnings for technical documents.

(4) Statements or descriptions identifying the items of information to be classified must be clear and specific to minimize the probability of error by those who use the SCG.

(5) Failure to provide a sufficient level of detail will result in derivative classifiers making their own interpretations potentially resulting in over- or under-classification of information, impacting information sharing, and potentially resulting in unauthorized disclosure.

f. Step 6. Determine the reason for classification of each element of information. Pursuant to E.O. 13526, information will not be considered for classification unless it falls within one of the reasons listed in Section 1.4. of E.O. 13526.

g. Step 7. Determine the classification level for each element of information.

(1) The OCA determines if unauthorized disclosure of the information could reasonably be expected to result in damage to national security. The OCA must be able to identify or describe the damage and is determined for each element of information.

(2) The level of classification to be applied to each item of information identified in the guide must be specified precisely and clearly. Broad guidance such as "U-S", meaning "Unclassified to Secret" or "at a minimum" does not provide sufficient guidance to users of the guide and will not be used. Clearly delineate the exact circumstances under which each level of classification will be applied.

(3) Recurring themes emerge in the classification of intelligence content and services. As users familiarize themselves with SCGs and start making derivative classification determinations, they will become more adept at identifying the broad categories of information likely to be classified. These general areas should be treated with caution and scrutinized for potentially classified information. Table 4 identifies these recurring themes. Users who reach a derivative classification deviating from these general rules should validate their assessment and consider discussing their determination with a subject-matter expert.

Table 4. Classification Justification

Item	Classification	Value	Damage	Unclassified	Remarks
Responsibility to provide insight on worldwide issues and threats related to U.S. national security interests.	Unclassified	N/A	N/A	N/A	Details with potential to reveal classified sources, methods, or mission support would be classified appropriately.
Information which, if compromised, would significantly and demonstrably change an adversary's behavior in ways harming national security interests.	Classified	Provides access and insight into adversarial activities threatening U.S. national security interests.	Adversarial operations security (OPSEC) or denial and deception (D&D) measures reduce U.S. decision advantage by denying insight from sources and methods.	Products from non-sensitive sources and methods covering topics or targets where adversaries will not modify behavior to harm national security interests.	N/A
Information revealing activity an adversary actively protects from discovery or revealing gaps in our knowledge.	Classified	Products and assessments provide indicators of adversarial D&D activity.	Adversarial OPSEC or D&D measures reduce U.S. decision advantage by denying insight from sources and methods.	Intelligence Agency's responsibilities to provide insight on issues and threats related to our national security interests.	Reporting revealing the effectiveness of decoys, deception, disinformation, signatures, analytic methods, or other capabilities merit protection.
Information revealing classified aspects of an agency's relationship, to include international or mission partners.	Classified	Protects Intelligence Agency's accesses and relationships.	Exposure could jeopardize the relationship or defeat the effectiveness of the mission.	Intelligence Agency has classified and unclassified accesses and relationships.	N/A
Products in support of mission partner operations that would reveal classified aspects of the operation.	Classify in accordance with operation	N/A	N/A	N/A	Classification determination is derived from the customer and can range from unclassified but sensitive diplomatic engagements to covert or clandestine operations.
Intelligence revealing sources or methods exceeding what is in use in academia, the private sector, or acknowledged by the national security enterprise.	Classified	Protects technical advantage and superior capabilities.	Adversaries adopt similar technologies and tailor D&D measures to advance their interests or to nullify the technical advantage.	Intelligence Agency seeks to capitalize on new and emerging technologies, sources, and methods.	Reflects ongoing research and development programs, some of which involve partnerships with academic institutions and are protected at an extremely high level.

h. Step 8. Determine the duration of classification. The duration of classification is based on how long the OCA determines the information requires protection as explained in Paragraph 4.2.a.(3). It is not determined by the level of classification.

i. Step 9. Identify elements of information meeting the criteria of CUI. Assess elements of unclassified information against the DoD CUI Registry at https://www.dodcui.mil to determine if they are CUI. See Paragraph 6.5.b.(6) and Figure 21 for additional information.

j. Step 10. Consider the value, damage, and unclassified enhancement statements. To help derivative classifiers understand why specific information requires protection, three amplifying statements will be used for each line item that requires a classification. The enhancement statements are labeled as "Value," "Damage," and "Unclassified" and are intended to help users understand why certain portions of information are classified. See Paragraph 6.5.b.(8) for more details.

k. Step 11. Write the guide.

(1) Once the classifier has identified specific items of information warranting classification, start writing the SCG.

(a) Be precise and clear.

(b) Write for the user. The user of the guide must be able to understand the specific information the guide addresses and apply the correct markings to their document. Write in plain language in accordance with DoDI 5025.13 and define acronyms.

(2) The issuing office should consult with subject matter experts, potential users, and their local security office as the SCG is written.

(3) General content of an SCG (See Section 6 for format) will:

(a) Identify the subject matter of the SCG (i.e., the title). Place the most significant words of the title first, (e.g., "FA-5B Aircraft Security Classification Guide").

(b) Provide the date of issuance and last review, when applicable.

(c) Identify the OCA(s) by name and position, or personal identifier.

(d) Identify an agency point of contact or office of primary responsibility for questions regarding the guide.

(e) State precisely the elements of information to be protected, including CUI.

(f) State the classification level for each element of information. Do not use ranges, such as "Unclassified to Secret" or state "at a minimum."

(g) State a concise reason for classification.

(h) Prescribe a specific date or event for declassification.

(i) State, when applicable, dissemination controls, special handling caveats, and CUI categories.

(4) Machine-readable SCGs are being created throughout the DoD. Additional guidance will be required as the capability develops. Initial steps to aid machine-readable conversion of SCGs are as follows.

(a) Provide all portions of the SCG used to determine guidance in a single excel workbook (.xlsx file type) at a minimum. This includes but is not limited to classification tables, classification by compilation tables, critical program information, and classification threshold guidelines.

(b) Digital formats in an excel workbook will be provided if used to create an SCG.

(c) The content of the delivered machine-readable portions of an SCG must match the human-readable SCG and cannot constitute new material until changed by follow-on guidance.

l. Step 12. Conduct coordination. Ensure appropriate horizontal coordination across organizations, DoD Components, Military Services, agencies, foreign disclosure office, and SAP is conducted. This includes reviewed SCGs that cover similar information. If similar information is classified at different levels in different organizations, ensure both OCAs are aware of the difference, and it is accurately addressed in both SCGs. Coordination with the SAP office is required to ensure information in your guide does not overlap or conflict with SAP guidance. Completion of these actions will be recorded on the DD Form 2024.

m. Step 13. Complete the DD Form 2024. Follow the instructions in Paragraph 5.5.

5.12. INCORPORATING CHANGES INTO AN SCG.

a. Administrative changes are modifications to an SCG not requiring an OCA signature as they in no way change the interpretation of classification. Administrative changes may include, but are not limited to, changes to punctuation, spelling, spacing, and capitalization within the SCG.

b. Classification changes are modifications requiring an OCA signature and are SCG revisions. Changes falling into this category may include, but are not limited to:

(1) Changes to the information that is classified.

(2) Proposed changes to the level, duration, or dissemination of information.

(3) Changes or additions to the line items that would clearly change the interpretation of classification.

c. When incorporating previously approved interim changes, no additional coordination is required.

d. Classification changes to the SCG require the submission of the revised SCG and DD Form 2024 to DTIC with a copy of the DD Form 2024 to DDI(CL&S) in accordance with Paragraph 5.5.

APPENDIX 5A: DETERMINING WHICH ITEMS WARRANT CLASSIFICATION

5A.1. IDENTIFY CAPABILITIES.

Conducting an analysis helps identify capabilities providing a programmatic or national advantage and requiring protection from unauthorized disclosure to protect the advantage. Providing answers to these questions can help determine which items may warrant protection through classification pending an evaluation of the damage it may cause and in compliance with the requirements in Paragraph 4.1.

a. Analysis of Performance or Capability.

(1) What will this do (actual or planned) that is better, faster, or cheaper (in terms of all types of resources) than anything like it?

(2) How does this degree or kind of performance contribute to or create a national security advantage? How much of an advantage?

(3) How long can this data be protected? What is the advantage?

(4) How would knowledge of these performance details help an enemy or damage the success of the effort?

(5) Would statement of a particular degree of attained performance or capability be of value to hostile intelligence in assessing U.S. capabilities? Would such a statement spur a foreign nation to similar effort, or to develop or plan countermeasures?

(6) What, if any, counterintelligence implication does system performance have? Is the performance measure of a system something that should be made known as a show of force or should it be protected so system weaknesses are not revealed?

b. Analysis of Uniqueness.

(1) What information pertaining to this effort is known or believed to be the exclusive knowledge of the United States?

(2) Is it known or reasonable to believe other nations have achieved a comparable degree of success or attainment?

(3) What information, if disclosed, would result in, or assist other nations with developing a similar item or arriving at a similar level of achievement?

(4) How does the uniqueness of this item contribute to a national security advantage?

(5) How has the end product of this effort or any of its parts been modified, developed, or applied so as to be unique to this kind of effort? How unique is this?

(6) Is the method of adaptation or application of the end product or any of its parts the source of the uniqueness and a national security advantage? In what way? Is it a unique adaptation?

c. Analysis of Technological Lead Time.

(1) How long did it take to reach this level of performance or achievement?

(2) How much time and effort have been expended? Was this a special concerted effort or only a gradual developmental type of activity?

(3) If all or some of the details involved in reaching this stage of development or achievement were known, how much sooner could this goal have been reached? Which details would contribute materially to a shortening of the time for reaching this goal? Can these details be protected? For how long?

(4) Have other nations reached this level of development or achievement?

(5) Do other nations know how far the United States has advanced in this kind of effort?

(6) Would knowledge of this degree of development or achievement spur a foreign nation to accelerate its efforts to diminish our lead in this field? What details would be likely to cause such acceleration?

(7) How important, in terms of anticipated results, is the lead time gained?

(8) What national security advantage results from this lead time?

(9) How long is it practical to believe this lead time will represent an actual advantage?

(10) How long is it practical to expect to be able to protect this lead time?

d. Analysis of the Element of Surprise.

(1) Do other nations know about this level of development or achievement?

(2) Would operational use of the end item of this effort reduce or eliminate the immediate U.S. advantage if this goal's achievements were known?

(3) What is the advantage resulting from surprise use of this end item?

(4) When will this element of surprise be lost?

e. Analysis of Vulnerabilities and Weaknesses.

(1) What are the weak spots in this effort that make it vulnerable to failure? What is the rate or effect of this failure?

(2) How will the failure of the effort in whole or in part affect the national security advantage expected upon completion of this effort, or use of the resulting end item?

(3) What elements of this effort are subject to countermeasures?

(4) How would knowledge of these vulnerable elements assist in planning or carrying out countermeasures?

(5) Can information concerning these weak or vulnerable elements be protected from unauthorized disclosure or are they inherent in the system?

(6) Can these weaknesses or vulnerabilities be exploited to reduce or defeat the success of this effort? How could this be done?

(7) Are the counter-countermeasures obvious, special, unique, or unknown to outsiders or other nations?

(8) How would knowledge of these counter-countermeasures help carry out or plan new countering efforts?

(9) Would knowledge of specific performance capabilities help develop or apply specific countermeasures? How? What would be the effect on the expected national security advantage?

(10) Is this capability susceptible to data aggregation from artificial intelligence or is the encryption technology resistant to quantum computing speeds?

f. Analysis of Specifications.

(1) Would details of specification reveal:

(a) A special or unusual interest contributing to the resulting or expected national security advantage?

(b) Special or unique compositions contributing to the resulting or expected national security advantage?

(c) Special or unique levels of performance indicative of a classifiable level of achievement or goal?

(d) Special or unique use of certain materials revealing or suggesting the source of a national security advantage?

(e) Special or unique size, weight, or shape contributing to the resulting or expected national security advantage?

(2) Are any specification details contributory to the resulting or expected national security advantage? How?

(3) Can details of specifications be protected? For how long?

g. Analysis of Critical Elements.

(1) What are the things that really make this effort work?

(2) Which of these critical elements contribute to the resulting or expected national security advantage? How? To what extent?

(3) Are these critical elements a source of weakness or vulnerability to countermeasures?

(4) What details of information pertaining to these critical elements disclose or reveal the national security advantage, weakness, or vulnerability?

(5) Can details of information pertaining to these critical elements be protected by classification? For how long?

h. Analysis of Manufacturing Technology.

(1) What manufacturing methods, techniques, or modes of operation were developed to meet the requirements of this effort?

(2) Which of these manufacturing innovations are unique to this effort or this product? Are they generally known or suspected?

(3) Are these manufacturing innovations essential to successful production of the product?

(4) What kind of lead time results from these innovations?

i. Analysis of Associations.

(1) Are there any associations between this effort and others that raise classification questions?

(2) Are there associations between information in this effort and already publicly available (unclassified) information that raise classification problems?

(3) Are there associations with specific personnel, commands, companies, or other programs that are sensitive and should be protected or that may reveal classified information?

(4) Is it necessary or possible to classify items of information in this effort because their association with other unclassified or classified information would diminish or result in the loss of a national security advantage?

j. Analysis of Ability to Protect.

(1) Is it possible to protect the information effectively from unauthorized disclosure by classifying it? For how long?

(2) What alternative means can be used to ensure protection from unauthorized disclosure? Are they as effective as classification?

5A.2. SPECIFIC ITEMS OF INFORMATION TO CONSIDER.

Paragraphs 5A.2.a. through 5A.2.f. present elements of information that could disclose present or future strategic or tactical capabilities and vulnerabilities and should be considered when preparing classification guidance. This is intended to help the user identify specific items of information that may warrant protection by classification, pending an evaluation of the damage it may cause and in compliance with the requirements in Paragraph 4.1.

a. Performance and capability related data.

(1) Accuracy.

(2) Alert time.

(3) Altitude: maximum, optimum.

(4) Ballistics: initial, terminal.

(5) Control.

(6) Countermeasures (e.g., decoys, electronic, penetration aids, shield materials).

(7) Depth or height.

(8) Duration: flight.

(9) Effectiveness.

(10) Frequencies: bands, specific, command, operating, infrared, microwave, radio, communications security.

(11) Heating.

(12) Impulse.

(13) Intercept.

(14) Lethality or critical effects.

(15) Lift.

(16) Limitations.

(17) Maneuverability.

(18) Military strength: actual, planned, predicted, anticipated.

(19) Miss distance.

(20) Noise figure.

(21) Payload.

(22) Penetration.

(23) Range.

(24) Rate of fire.

(25) Reaction time.

(26) Reliability or failure rate data.

(27) Resolution.

(28) Sensitivity.

(29) Sequence of events.

(30) Signature characteristics: acceptance, analysis, distinguishing, identification.

(31) Speed and velocity: acceleration or deceleration, cruise, intercept, landing, maximum, minimum, optimum.

(32) Stability.

(33) Target data: details, identification, illumination, impact predicted, preliminary, priority, range determination.

(34) Threshold.

(35) Thrust.

b. Specifications related data.

(1) Balance.

(2) Burn rate.

(3) Capacity – system.

(4) Center of gravity.

(5) Codes.

(6) Composition.

(7) Configuration.

(8) Consumption.

(9) Energy requirements.

(10) Filter.

(11) Fineness.

(12) Grain configuration.

(13) Hardness, degree.

(14) Input data.

(15) Loading or loads.

(16) Mass factor – propellant.

(17) Moment of inertia.

(18) On-station time.

(19) Output data.

(20) Payload.

(21) Power requirements.

(22) Purity.

(23) Size, weight, shape.

(24) Stability: static, dynamic.

(25) Strength of members, frames.

(26) Stress.

(27) Thickness.

(28) Type.

(29) Connectivity, to include wireless capability.

c. Vulnerability related data.

(1) Countermeasures and counter-countermeasures.

(2) Dynamic pressure (supersonic).

(3) Electromagnetic pulse (radiation).

(4) Ground or air shock.

(5) Jamming.

(6) Signature characteristics: acoustic, electrical, infrared, magnetic, pressure, radar, static overpressure.

d. Procurement, production, and logistics related data.

(1) Completion date(s).

(2) Numbers.

(3) Dispersion: numbers per unit of force.

(4) On-hand stockpile.

(5) Planned or programmed: total, scheduled.

(6) Rate of delivery or production.

(7) Requirements.

(8) Spares.

(9) Progress and schedules: milestones.

(10) Stock density.

(11) Supply plans and status.

(12) Tactical deployment.

(13) Timelines.

(14) Logistical resupply.

(15) Maintenance and repair cycle.

e. Operations related data.

(1) Countdown time.

(2) Deployment data.

(3) Environment.

(4) Location.

(5) Numbers available.

(6) Objectives: mission or program, specific or general, or broad or detailed test.

(7) Plans.

(8) Results: analysis, conclusions, reports.

(9) Sequence of events.

(10) Staging techniques.

(11) Statement or concept.

(12) Tactical: buildup, units per force.

(13) Activation and capability dates.

(14) Personnel.

f. Testing related data.

(1) Dates.

(2) Location.

(3) Objectives: general, specific.

(4) Output: raw, analyzed.

(5) Plans.

(6) Required equipment or personnel.

(7) Results: analysis, conclusions, reports.

(8) Schedule.

5A.3. IDENTIFY POTENTIAL CLASSIFICATION REQUIREMENTS.

Paragraphs 5A.3.a. through 5A.3.d. present examples of elements of information that could disclose present or future capabilities and vulnerabilities and should be considered when preparing classification guidance. This is intended to help the user identify specific items of

information that may warrant protection by classification, pending an evaluation of the damage it may cause and in compliance with the requirements in Paragraph 4.1.

a. Classifying Hardware Items.

An item of hardware may convey information that is as sensitive as the words printed on a piece of paper. Hardware items may be classified if they reveal or could be exploited to reveal classified information. Some basic considerations are:

(1) An item of hardware does not necessarily need to be classified simply because it is part of a classified product or effort.

(2) Unclassified commercial-off-the-shelf items, unless modified in a particular way to make them perform differently, cannot be classified even when they constitute a critical element, become an integral part of a classified end product, or produce a properly classified effect. However, the association of otherwise unclassified hardware with a particular effort or product may reveal something classified about that effort or product. Common integrated circuits that control frequencies are notable examples. In such cases, it is the association with the effort or product that reveals the classified information, not the circuits themselves.

(3) Frequently, classified information pertaining to a hardware item can be restricted to the documentation associated with it.

(4) Unusual, unique, or peculiar uses or modifications of ordinarily available unclassified materials or hardware may create a classifiable item of information. The use of a particular material in a particular effort might reveal a classifiable research or development interest. In such cases, accurately identifying the classified information to determine whether it is the hardware or material that reveals classified information or the use of the hardware with a particular effort that reveals such information is especially important.

(5) During the production effort, manufacturers draw production and engineering plans and usually prepare a family-tree type diagram to assist in determining what components, parts, and materials will be required. This diagram provides a good basis for determining where and when classified information will be involved in the production effort.

(6) Another step in production engineering is the development of drawings for all of the individual elements that will go into the final product. These drawings show design data, functions, and specifications, all of which are closely tied to items of information that may be classified. From these drawings, classifiers may determine exactly which elements of or associations with the final product will reveal classified information, providing a prime opportunity to identify and isolate classification requirements.

b. Classifying Military Operations Information.

(1) Successful military operations depend largely upon DoD's ability to correctly assess the capability and intention of enemy forces at each stage of the operation while concealing its own capabilities and intentions, and to communicate effective battle plans and orders throughout U.S. forces. Classifiable information may include:

(a) The number, type, location, and strengths of opposing units.

(b) The capabilities and vulnerabilities of weapons in enemy hands, and how the enemy normally applies the weapons.

(c) The morale and physical condition of the enemy force.

(2) There may be a good reason to classify more information about the operations in the beginning than will be necessary later. Certain elements of information may no longer require the same level of protection after a certain date or event. When this point is reached, classifiers should consider downgrading or declassification. Examples of information to consider include:

(a) Overall operational plans.

(b) System operational deployment or employment.

(c) Initial operational capability date.

(d) Planned location of operational units.

(e) Equipage dates, readiness dates, operational employment dates.

(f) Total manpower or personnel requirements for total operational force.

(g) Coordinates of selected operational sites.

(h) Specific operational performance data relating to the effectiveness of the control of U.S. forces and data on specific vulnerabilities and weaknesses.

(i) Existing OPSEC and communications security measures.

(j) Target characteristics.

c. Classifying Intelligence Information.

(1) Producers of intelligence must avoid over-classification and be wary of applying so much security that they are unable to provide a useful product to their consumers. An intelligence product should be classified only when its disclosure could reasonably be expected to cause some degree of damage to national security. Only OCAs with jurisdiction over intelligence matters may classify intelligence information. Basic considerations include:

(a) In general, resource information should not be classified unless it reveals some aspect of the intelligence mission, and its revelation would jeopardize the effectiveness of a particular function.

(b) Intelligence concerning foreign weapons systems is typically classified based on what is generally known about a particular system or its components. Normally, the less that is known publicly about a particular system or component the higher its level of classification.

(c) Intelligence identifying a sensitive source or method and the evaluation of the particular source or method should always be classified.

(d) Intelligence not identifying or revealing a sensitive source or method is usually not classified unless the information contains other classified information such as intelligence activities including intelligence plans, policies, or operations.

(e) Intelligence revealing the identity of a conventional source or method normally does not require classification.

1. If, however, the information is communicated to DoD by a foreign government, whether under a formal government-to-government agreement or simply with the understanding the information is provided in confidence, the information must be protected at the level and for the length of time agreed to by the USG and the foreign government.

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

(f) Intelligence revealing known and possible enemy capabilities to collect and exploit information from a given or similar operation should be classified. This would include enemy intelligence collection and analysis capabilities, efforts, and successes.

(g) An intelligence estimate is normally classified since it is likely to contain sensitive sources or methods or raw or unevaluated intelligence.

(h) An intelligence requirement should be classified when it reveals what is not known, what is necessary to know, and why. Moreover, the requirement may recommend a sensitive source or method, other military intelligence required, or contain technical and operational characteristics of classified weapon systems.

(2) The classification of relationships with foreign intelligence organizations is related to these considerations:

(a) Normally, broad U.S. general intelligence cooperation with foreign countries or groups of countries with which the United States maintains formal military alliances or agreements (e.g., the North Atlantic Treaty Organization) is not classified.

(b) Intelligence cooperation between the United States and a specific governmental component in an allied country or general description of the nature of intelligence cooperation between the United States and any allied country may be classified. Ongoing intelligence cooperation between the United States and specifically named countries or their governmental components with which the United States is not allied with should always be classified. Such classification is applied to U. S. intelligence activities to prevent harm to national security should the cooperation be revealed through unauthorized disclosure.

(c) Details of any intelligence exchange agreements should be classified. Additionally, the mere existence of a specified intelligence agreement should be classified as the agreement is evidence of on-going intelligence cooperation.

(d) The identities of foreign government or military personnel who provide intelligence under such agreements or liaison relationships may be classified in accordance with the instructions of the foreign government or in the national security interest of the United States.

(3) Defense users must respect the classification assigned to intelligence received from non-DoD sources. The level of classification depends upon the degree of identifiable harm to national security that would reasonably be expected to occur from unauthorized disclosure. OCAs within the IC normally consider this information to be classified:

(a) Cryptologic information (including cryptologic sources and methods), cryptographic information, signals intelligence, imagery intelligence, electronic intelligence, telemetry intelligence, and electronic warfare.

(b) Information revealing counterintelligence activities, investigations, or operations, identities of undercover personnel or units, methods of operations, and analytical techniques for the interpretation of intelligence data is classified.

(c) Intelligence SAPs.

(d) Information identifying clandestine organizations, agents, sources, or methods.

(e) Information on personnel under official or nonofficial cover, or revelation of a cover arrangement.

(f) Covertly obtained intelligence reports and the derivative information potentially divulging intelligence sources or methods.

(g) Methods or procedures used to acquire, produce, or support intelligence activities.

(h) Intelligence organizational structure, size, installations, security, objectives, and budget.

(i) Information divulging intelligence interests, value, or extent of knowledge on a subject.

(j) Training provided to or by an intelligence organization indicating its capability or identifying personnel.

(k) Intelligence personnel recruiting, hiring, training, assignment, and evaluation policies.

(l) Information potentially leading to foreign political, economic, or military action against the United States or its allies.

(m) Events leading to international tension potentially affecting U.S. foreign policy.

(n) Diplomatic or economic activities affecting national security or international security negotiations.

(o) Information affecting U.S. plans to meet diplomatic contingencies affecting national security.

(p) Non-attributable activities conducted abroad in support of U.S. foreign policy.

(q) U.S. surreptitious collection in a foreign nation that would affect relations with that country.

(r) Covert relationships with international organizations or foreign governments.

(s) Information related to political or economic instabilities in a foreign country threatening American lives and installations.

(t) Information divulging U.S. intelligence and assessment capabilities.

(u) Defense plans and capabilities of the United States and its allies with potential to enable a foreign entity to develop countermeasures.

(v) Information disclosing U.S. systems and weapons capabilities or deployment.

(w) Information on research, development, and engineering that enables the United States to achieve or maintain a significant national security advantage.

(x) Information on technical systems for collection and production of intelligence.

(y) U.S. nuclear programs and facilities.

(z) Foreign nuclear programs, facilities, and intentions.

(aa) Contractual relationships revealing the specific interest and expertise of an intelligence organization.

(ab) Information that could place someone in jeopardy.

(ac) Information on secret writing when it relates to specific chemicals, reagents, development, microdots, or steganography.

(ad) U.S. military space programs.

(ae) U.S. cyber capabilities.

(af) Information on weapons of mass destruction, whether U.S. or foreign.

(ag) Classified information systems configurations such that vulnerabilities may be identified and exploited.

d. Classifying Foreign Relations Information.

The Department of State is primarily responsible for the development and execution of U.S. foreign policy and is the principal agency responsible for the security classification of foreign relations information. Most DoD classification determinations in the area of foreign relations will be derivative in nature, but in some instances, DoD must provide security classification guidance for projects and programs involving foreign relations information. Examples of the types of information or material involving foreign relations warranting classification include:

(1) All information or material recommending or revealing USG positions or options in a negotiation with a foreign government or group of governments, or comments on the merits of foreign government positions in such negotiations.

(2) All information or material commenting on the quality, character, or attitude of a serving foreign government official, whether elected or appointed, and regardless of whether the comment is favorable or critical. Illustrations of the types of information covered in this category are records revealing a foreign official:

(a) Speaking in a highly critical manner of their own government's policy.

(b) Suggesting how pressure might effectively be brought to bear on another part of their own government.

(c) Acting in unusually close concert with U.S. officials where public knowledge of this might be harmful to the foreign official.

(d) Whose professional advancement would be beneficial to U.S. interest, especially if any implication has been made of U.S. efforts to further their advancement, or if public knowledge of this might place the person or their career in jeopardy.

(3) All unpublished adverse comments by U.S. officials on the competence, character, attitudes, or activities of a serving foreign government official.

(4) All material constituting or revealing unpublished correspondence between heads of state or heads of government.

(5) Statements of U.S. intent to defend, or not to defend, identifiable areas, in any foreign country or region.

(6) Statements of U.S. intent militarily to attack identifiable areas in any foreign country or region.

(7) Statements of U.S. policies or initiatives in collective security organizations such as the North Atlantic Treaty Organization.

(8) Agreements with foreign countries to use, or have access to, military facilities.

(9) Contingency plans as they involve other countries, the use of foreign bases, territory, or airspace; or the use of chemical, biological, or nuclear weapons.

(10) DoD surveys of foreign territories for purposes of basing or using in contingencies.

(11) Statements relating to any use of foreign bases not authorized under bilateral agreements.

(12) Information concerning relationships with foreign intelligence organizations or related to foreign collection activities.

APPENDIX 5B: FRAMING COMPONENTS FOR INTELLIGENCE INFORMATION

5B.1. PROCESS.

a. Three components are inherent to the value of all intelligence:

(1) Source.

Where data comes from.

(2) Method.

How data is collected and turned into intelligence.

(3) Mission.

Why intelligence is created.

b. Framing components are intended to help the user identify specific items of information that may warrant protection by classification, pending an evaluation of the damage it may cause and in compliance with the requirements in Paragraph 4.1. As shown in Figures 7 and 8, the framing components are:

(1) Source.

A person or thing from which intelligence information is received that drives the classification of a particular line item.

(2) Method.

How data is collected and turned into intelligence. The tradecraft or methodology used that drives the classification of a particular line item.

(3) Mission.

Why intelligence is created. Aspects about an agency's or DoD Component's mission or a military or operational mission that drives the classification of a particular line item.

Figure 7. Example of Framing Components

Framing Component	Examples
Sources: From where the data comes	• Commercial • Foreign • Academic • Government • Publicly available • Classified
Methods: How data is collected and turned into intelligence	• Tradecraft • Software • Algorithms • Methodologies and Strategies
Missions: Why intelligence is created	• Military support • Situational awareness • Humanitarian • Mapping, Charging, and Geodesy (the science of accurately measuring the Earth's size, shape, orientation, mass distribution and how these vary with time) • National intelligence

Figure 8. Examples of the Use of Framing Components

Source: Unclassified Source. **Method:** Unclassified Method. **Mission:** Support a special operation of a military unit (classified).	The product created will be classified due to the classification of the mission regardless of the unclassified data sources and methods. Classification markings on the product will cite the classification guide of the supported military mission rather than intelligence sources and methods.
Source: Classified by responsible OCA in an SCG. **Method:** Government-created algorithm revealing change over time (unclassified). **Mission:** Unclassified mission.	The classification of the resulting product is driven by the classification of the source. To classify the resulting product accurately, a user will need to identify and consult the applicable SCG, and any request to sanitize or downgrade the information would be referred to the DoD entity for determination.
Source: Unclassified source. **Method:** Aggregation algorithm (unclassified, unless any portion of the script or code reveals a classified source or mission). **Mission:** Repository to satisfy general intelligence community mission requirements (unclassified).	The product is unclassified because the data is unclassified, the algorithm is unclassified, and the resulting database does not reveal a specific intelligence issue.
Source: One source is classified; another source containing the same information is unclassified. **Method:** Method is unclassified. Tools or methods that expose sensitive signatures, activities that serve as key indicators, or a combination of otherwise unclassified sources or observations that provide a unique advantage to decision makers may be classified. **Mission:** Develop an unclassified tool.	The tool is generally unclassified, unless any portion of the code, interface, or metadata reveals a classified mission. If that is the case, it is classified.
Source: Positive identification of an individual as a source to a U.S. intelligence agency. (Classified) **Method:** Information on collection agency human intelligence plans, methods, or accomplishments. (Classified) **Mission:** Specific information on a collection operation. (Classified)	In this case, all three components of source, method, and mission are classified which means that the resulting product would be classified.

c. Creating intelligence without sources of data, methods of analysis, or a mission to support (even if that mission is simple situational awareness) is not possible. Conveying intelligence without revealing sources, methods, or mission supported is possible and is the basis for creating intelligence at a level of classification that enables the widest and most effective dissemination. Building agile and adaptive intelligence requires a deeper understanding of why intelligence is being produced and what interests must be protected. A user who understands the classified components of intelligence can make informed decisions about how to build products for maximum utility.

d. SCGs should be written to enable agile and responsive intelligence to support national security and military missions and operations. The potential for the unauthorized disclosure of protected information is a risk to intelligence. Sources, methods, and missions are the three components at risk. Only a consideration of risk to all three components determines what classification of intelligence is appropriate, acceptable, or essential.

e. The risk to each framing component can be managed or mitigated by any single strategy or combination of strategies. Examples of mitigation strategies are in Figure 9.

Figure 9. Examples of Mitigation Strategies

Strategy	Description	Example
Omit sources and methods completely.	Disseminate what we know but not from where the information came, or how it was collected and turned into intelligence.	"The U.S. Government reports a missile launch."
Omit attribution of sources but report method used.	Disseminate the method, agnostic of source. The method could have come from a variety of data sources.	"The U.S. Government reports imagery confirms a missile launch."
Omit why the information was collected.	Disseminate information without revealing the customer or why the information is needed.	Examples include the maps, charts and intelligence an agency creates for a variety of customers without ever revealing what the products will support.

f. A vast part of USG sources of data, methods of analysis and details of missions can reside on unclassified networks or storage systems. Creating useful intelligence to support many USG missions is possible at an unclassified level. Transferring data to higher classification systems can have value, but producers or analysts should consider analyzing and creating intelligence at the lowest classification possible.

g. The quantity and diversity of unclassified, worldwide, USG information continues to grow exponentially. Not only does this provide more information at the unclassified level but the resulting proliferation of open-source intelligence enables an agency to disguise classified sources more effectively.

h. Armed with sufficient information, analysts can create intelligence products at any classification level to serve the DoD's diverse customer base while protecting sources, methods, and the missions supported.

5B.2. REACHING A DERIVATIVE CLASSIFICATION.

Intelligence producers and consumers must understand the basics of classification authorities to reach accurate derivative classification decisions, which include:

a. If all components fall under a specific agency's authorities, consult that agency's appropriate SCG to determine all line items that apply. The guide may classify different aspects of sources, methods, or missions in separate line items.

b. If the intelligence contains information that does not belong to a specific agency, users must determine whether the responsible agency has issued any security classification guidance. This guidance may take the form of an SCG for a specific mission or effort, a "core" guide for a

broad spectrum of activities, guidance contained in mission planning, or properly marked source documents.

c. If a user cannot find the relevant security classification guidance or is uncertain as to whether their assessment of the information is correct, they will refer the information or product to the appropriate classification management component for further guidance.

SECTION 6: SCG FORMAT

6.1. INTRODUCTION.

a. This section identifies the required sections and information for all SCGs.

b. An SCG template is available on the DTIC Website at https://www.dodtechipedia.mil/dodwiki/pages/viewpage.action?pageId=508330051. It is also available upon request by sending an e-mail to osd.pentagon.rsrcmgmt.list.ousd-intel-infosec-mbx@mail.mil.

6.2. COVER.

SCG statements require:

a. A title. The title should be unclassified and will identify the SCG's subject matter. Place the most significant words of the title first. One-word SCG titles, system nomenclature only, or acronym only SCG titles are not acceptable. SCG titles must, in the fewest words possible, capture and describe the SCG's subject matter. At a minimum, the title must be sufficiently detailed to advise the reader about the subject(s) covered in the SCG. However, if the title is classified, please provide an unclassified title or identification (e.g., number).

b. Date of issuance and date of last review, if applicable. Even if no changes are made to the SCG during the 5-year review, the cover will reflect the date of last review.

c. The applicable distribution statement in accordance with DoDI 5230.24. Because of the requirement to submit SCGs to DTIC, SCGs require a distribution statement. The presence of a distribution statement does not automatically mean the SCG is CUI; it is required for the document to be uploaded to DTIC's repository.

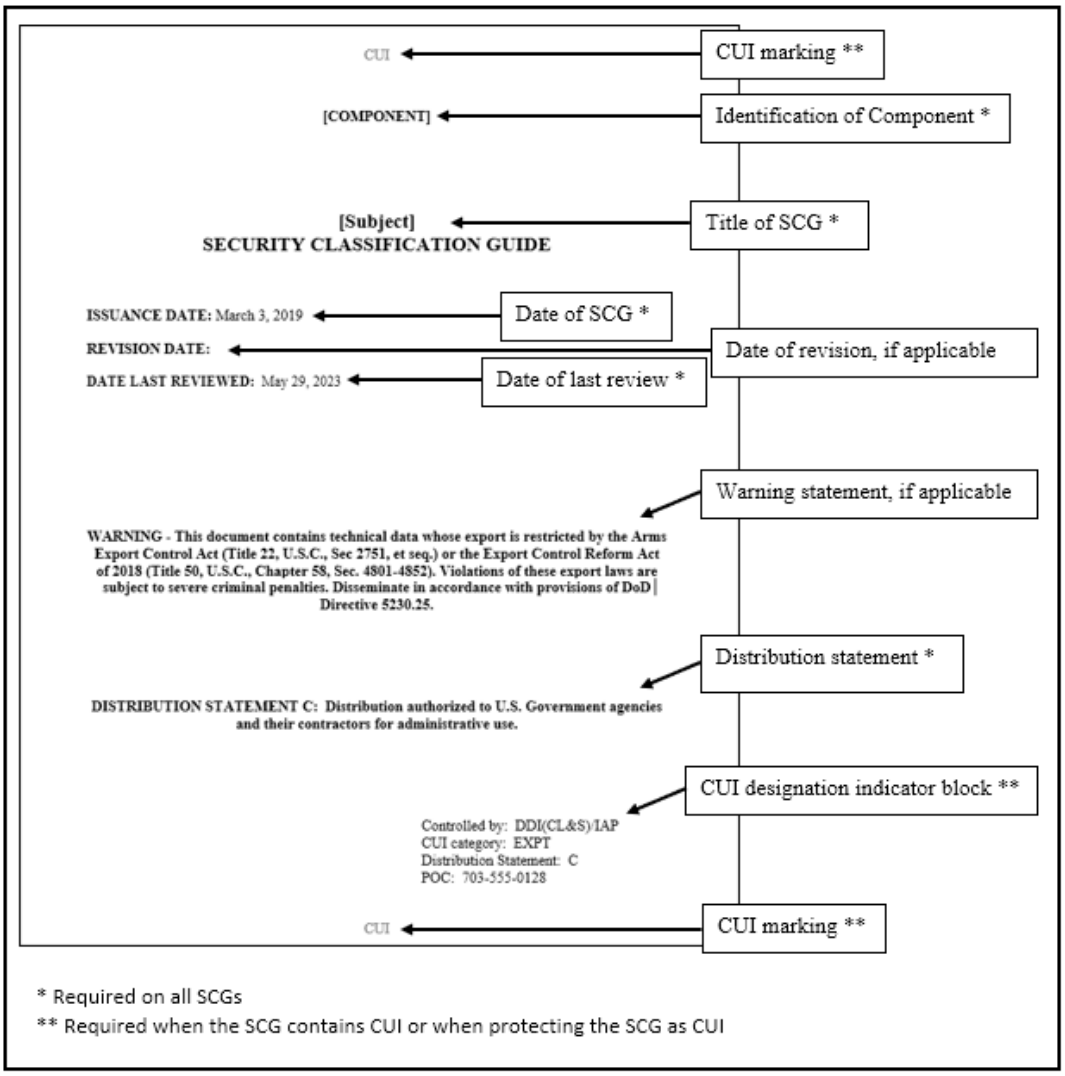
d. Warning statements, if applicable (e.g., the export control warning).

e. Markings.

(1) If the guide is classified, ensure the cover page contains appropriate portion marking, overall classification (of the guide as a whole), applicable dissemination controls or special handling caveats, and a classification authority block in accordance with Volume 2 of DoDM 5200.01. Interior pages must contain portion markings and the overall classification or the classification of each individual page.

(2) Unclassified SCGs may be protected as CUI, shown in Figure 10, as the aggregation of information may identify critical information that meets the criteria of CUI. Follow the CUI marking instructions in DoDI 5200.48.

Figure 10. Example of an SCG Cover Page



6.3. FOREWORD.

a. Description.

Provide a short description of the technology, system, plan, program, project, or mission covered in the guide.

b. Authority.

Explanation of where the authority to classify comes from. See Figure 11 for example authority statement.

Figure 11. Example of Authority Statement

Authority: The [OCA position title] has delegated authority from the [Secretary of Defense or MILDEP, or SAO] to exercise classification level original classification authority (OCA) and issue appropriate classification guidance for the system, plan, program, project, or mission name. This SCG is issued pursuant to Executive Order 13526; Part 2001 of Title 32, Code of Federal Regulations; DoDI 5200.01; DoDM 5200.01 Volumes 1, 2, and 3; and DoDM 5200.45.

c. Interim Changes.

Include an explanation of how interim changes are made and recorded.

d. Supersessions.

State if this is a new SCG or if it supersedes a previous version or other SCG. Include the title and date of the superseded SCG.

e. Effective Date.

Provide the effective date of the SCG.

f. Approved By.

Include the signature block and signature of OCA. If the OCA position title has changed since the previous review due to reorganization or transfer to a different OCA, the SCG must be reviewed and signed by the current OCA.

6.4. SECTION I – GENERAL.

a. Purpose.

State the purpose of the SCG. See Figure 12 for example purpose statements.

Figure 12. Examples of Purpose Statement

PURPOSE: The classification guidance contained herein will be used as derivative classification guidance for classifying [system, plan, program, project, or mission name] information.

PURPOSE: The purpose of the SCG is to provide instructions and guidance on the classification of information and controlled unclassified information safeguarding measures pertaining to [system, plan, program, project, or mission name].

b. Applicability and Scope.

State to whom or what the SCG applies. See Figure 13 for examples of applicability statements.

Figure 13. Examples of Applicability Statement

APPLICABILITY: This classification guidance applies to information or material relating to [program].

APPLICABILITY: This guide will be used as the basis for derivative classification, downgrading, or declassification of information and material associated with [system, plan, program, project, or mission name].

c. Office of Primary Responsibility.

Identify the office responsible for questions regarding the SCG. Include phone number and e-mail address. Organization e-mails are preferred.

d. Classification Challenges.

The classification challenges paragraph must include information on the classification challenge process. See Figure 14 for an example of a classification challenges statement.

Figure 14. Example of Classification Challenges Statement

Classification Challenges: Any authorized holder of national security information who has substantial reason to believe that certain information is improperly or unnecessarily classified is encouraged and expected to challenge that classification and bring about corrective action. The challenge may be initiated either informally or formally. Informal questioning of a classification is encouraged before resorting to a formal challenge. Regardless of form, all challenges will be considered good faith attempts to improve our processes and no retribution will be tolerated against any Government or contractor employee who comes forward with such a request. Questions regarding the challenge process should be referred to [insert office phone number or email].

e. OPSEC.

Include an explanation of what OPSEC is and how it applies to the program. See Figure 15 for an example of an OPSEC statement.

Figure 15. Example of OPSEC Statement

OPSEC. OPSEC countermeasures will be integrated into all activities supporting the planning, development, testing, deployment, transition, and operation of [system, plan, program, project, or mission name]. Users of this SCG shall maintain essential secrecy of information that is useful to adversaries and potential adversaries to plan, prepare, and conduct military and other operations against the United States and shall safeguard such information from unauthorized access and disclosure.

f. Public Release.

Include an explanation of public release process. See Figure 16 for an example of a public release statement.

Figure 16. Example of Public Release Statement

All information (unclassified, controlled unclassified information (CUI), classified) pertaining to the [system, plan, program, project, or mission name] proposed for public release must undergo a formal security classification and policy review and obtain official public release authorization in accordance with DoDIs 5230.09 and 5230.29 before the information is released into the public domain.

g. Foreign Disclosure.

Include an explanation of the foreign disclosure process. See Figure 17 for an example of a foreign disclosure statement.

Figure 17. Example of Foreign Disclosure Statement

Foreign Disclosure. Any disclosure to foreign officials of information classified by this guide will be in accordance with the procedures set forth in the National Disclosure Policy-1, "National Disclosure Policy," and DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations." If a foreign government with which the DoD has entered into a reciprocal procurement memorandum of understanding or offset arrangement expresses an interest in this effort, a foreign disclosure review must be conducted prior to issuance of a solicitation.

h. Using Section II – Classification Tables.

Provide an explanation of the information in each column annotated in Section II.

6.5. SECTION II – CLASSIFICATION TABLES.

a. Each table must provide sufficient information to enable users to fully understand what information is to be protected, at what level, for how long, and with whom it may be shared so

each derivative document can be properly marked and safeguarded. It must also provide information on what is not classified.

b. The tables will provide this information:

(1) Element of Information.

(a) The core of classification is the identification of the specific items or elements of information warranting security protection. The statements and descriptions identifying the elements of information must be clear and specific enough to minimize the probability of error by derivative classifiers. Indicate elements of information which would be unclassified, including CUI, to add clarity and specificity.

(b) If an element of information can be classified at different levels based on additional information included, the element must be listed separately for each level of classification as shown in Figure 19. Do not use ranges of classification (e.g., U-TS).

Figure 18. Examples of Differing Levels of Classification

Element of Information	Classification or Control Level	Reason (1.4)	Declas Date	Dissemination Control	CUI Category	Remarks
2. Fact of U.S. overflights.	Unclassified					
2.1. In Europe	Unclassified					
2.2. In Country X	Secret	1.4(d)	25 years	REL TO USA, CAN		
2.3. In Country Z	Top Secret	1.4(d)	25 years	REL TO USA, CAN		

(c) Do not make the element of information so broad that derivative classifiers are forced to seek classification guidance from the office of primary responsibility. The goal is to provide the user with specific, easy to follow details and instructions, to help reduce the risk of unauthorized disclosure to the classified information.

(d) Consider potential instances of classification by compilation and include those in the guide. See Paragraph 6.6. for information about classification by compilation.

(2) Classification.

(a) Annotate the level of classification or control assigned to each element of information. Only "Top Secret," "TS," "Secret," "S," "Confidential," "C," "Unclassified," "U," or "CUI" will be placed in this block. Be consistent. Either spell out all the classification levels or use only the approved abbreviations. "CUI" will not be spelled out in the banner line.

(b) Ranges of classification levels are not permissible. If referring to another SCG for classification guidance, list the applicable SCG or provide organization contact information in the "Remarks" column as shown in Figure 19.

Figure 19. Example of Referencing Other Source or SCG

Element of Information	Classification or Control Level	Reason (1.4)	Declas Date	Dissemination Control	CUI Category	Remarks
2. Fact of U.S. overflights - Europe.	Unclassified					
3. Fact of U.S. overflights – Country Z.	See Remarks					Refer to [title] SCG for specific guidance.

(3) Reason.

The program, plan, project, etc. must fall under one of the reasons for classification as described in Section 1.4. of E.O. 13526. Multiple reasons within an SCG are possible. Leave blank if referencing another source or SCG for classification instructions or if the element of information reflects unclassified information.

(4) Declassification Date.

This indicates how long the information must remain classified and is not determined by the level of classification.

(a) OCAs can only classify information for a maximum of 25 years, except for information that would clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source (marked as 50X1-HUM) or key design concepts of weapons of mass destruction (marked as 50X2-WMD).

(b) Automatic declassification exemptions (marked as 25X1-25X9) may be incorporated into SCGs only upon approval by the ISCAP pursuant to Part 2003 of Title 32, CFR.

(c) Consider the circumstances under which information may be downgraded. Leave blank when referencing another source or SCG for classification instructions, or if the element of information reflects unclassified information.

(5) Dissemination Control Markings.

List applicable dissemination controls approved for use by the IC.

(6) CUI.

Annotate the CUI category(ies) applicable to the unclassified element of information.

(7) Remarks.

The "Remarks" column is a free text area to document any additional information pertinent to the topic. If referring to another SCG for classification guidance, list the applicable SCG or provide organization contact information in the "Remarks" column.

(8) Enhancement Statements.

This SCG incorporates three statements for each classified line item which appear in three rows immediately under all classified line items. These three statements are labeled "Value," "Damage," and "Unclassified." By better articulating the reason behind classification determinations, the enhancement statements are intended to help users understand why certain portions of information are classified, manage risk, appropriately classify products, and increase product dissemination.

(a) The "Value" statement contains a brief description of why the information in the classified line item is being protected at that level as it relates to mission(s) or function(s) it supports.

(b) The "Damage" statement contains a brief description of the impact to National Security that can be reasonably expected if an unauthorized disclosure of that classified line item occurs.

(c) The "Unclassified" statement contains a brief description of how a user can address the classified line item. Unclassified statements marked "N/A" reflect the classified line item cannot be addressed at the unclassified level."

(d) The enhancement statements are shown in Figure 20.

Figure 20. Example of the Use of Enhancement Statements

Element of Information	Classification or Control Level	Reason (1.4)	Declas Date	Dissemination Control	CUI Category	Remarks
1. Speed of aircraft	Secret	1.4(a)	25 years			
VALUE: Protects mission essential functions. DAMAGE: Compromise would expose information that could be exploited by the adversary. UNCLASSIFIED: The speed of the aircraft ranges from xx to yy.						

c. Figure 21 shows the required information in a standard template format.

Figure 21. Example of Data in Proper SCG Format

Element of Information	Classification or Control Level	Reason (1.4)	Declas Date	Dissemination Control	CUI Category	Remarks
1. Speed of aircraft	Secret	1.4(a)	25 years			
VALUE: Protects mission essential functions. DAMAGE: Compromise would expose information that could be exploited by the adversary. UNCLASSIFIED: The speed of the aircraft ranges from xx to yy.						
2. Fact of U.S. overflights in Europe.	Unclassified					
3. Personnel information.	CUI				PRVCY	

6.6. CLASSIFICATION BY COMPILATION.

a. Classification by compilation will be determined by the appropriate OCA and annotated in the SCG. Guidance on compilation will be specific and clear to the user of the SCG so derivative classifiers understand what is classified, at what level, and for what duration.

b. Classification by compilation occurs when portions of unclassified information are combined in a way that discloses classified information. Similarly, items of information that are classified at a specified level may become classified at a higher level when combined.

c. As part of the classification decision process, OCAs should determine whether the compilation has been previously classified by another OCA.

d. OCAs will avoid using classification to protect information merely because the compiled data represents a significant amount of information available in one place unless damage to the national security can be communicated as detailed in Section 4. When information qualifies for classification by compilation, it is because the whole is greater than the sum of the parts (i.e., something new is revealed by putting all the portions together that is not revealed by the individual parts).

e. Guidance on how to mark a document classified by compilation is in Volume 2 of DoDM 5200.01.

f. The examples in Figure 22 demonstrate circumstances for classification by compilation.

Figure 22. Examples of Classification by Compilation in an SCG

Element of Information	Classification or Control Level	Reason (1.4)	Declas Date	Dissemination Control	CUI Category	Remarks
201.1. Theater-wide operation failure report, outage report, or problem.	Unclassified					
201.2. Two or more theater-wide operation failure reports, outage reports, or problem reports.	Secret	1.4(a)	10 years			
301.1. Mission	Secret	1.4(a)	Upon completion of mission, not to exceed 25 years.			
301.2. Geographic location.	Secret	1.4(a)	25 years			
301.3. Mission and geographic location together.	Top Secret	1.4(a)	25 years			

6.7. INTERIM CLASSIFICATION GUIDANCE.

a. Interim classification guidance may be issued when classification decisions must be communicated quickly and there is insufficient time to communicate the decision(s) through an update to, or development of, an SCG. Interim guidance can be annotated in a memorandum, but the required elements of information must be placed in the same table format as in an SCG as shown in Figure 23. Interim guidance will be incorporated into an SCG as soon as practical but not later than 1 year from date of the decision.

b. Interim classification guidance will:

(1) Go through the same horizontal coordination process in accordance with Paragraph 5.11.l.

(2) Be signed by the OCA.

(3) Be submitted to DTIC in accordance with the procedures in Paragraph 5.6.

Figure 23. Recommended Format for Interim Classification Guidance

MEMORANDUM FOR [applicable organizations]
DIRECTOR FOR DEFENSE INTELLIGENCE (COUNTERINTELLIGENCE, LAW ENFORCEMENT, AND SECURITY)

SUBJECT: Interim Security Classification Guidance

1. To ensure the security and protection of [program name, plan, etc.] related information, I am issuing the following classification guidance. This guidance will be in effect for one year, at which time it will be incorporated into a formal security classification guide.

Element of Information	Classification or Control Level	Reason (1.4)	Declas Date	Dissemination Control	CUI Category	Remarks

2. My point of contact for this action is

Signature block of OCA

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
AD	accession document
CFR	Code of Federal Regulations
CNSI	classified national security information
CUI	controlled unclassified information
DDI(CL&S)	Director for Defense Intelligence (Counterintelligence, Law Enforcement, and Security)
DoDD	DoD directive
DoDI	DoD instruction
DoDM	DoD manual
DTIC	Defense Technical Information Center
E.O.	Executive order
FCGR	Fundamental Classification Guidance Review
IC	Intelligence Community
ISCAP	Interagency Security Classification Appeals Panel
MILDEP	Military Department
NIPRNET	Non-classified Internet Protocol Router Network
OCA	original classification authority
OPSEC	operations security
SAO	senior agency official
SAP	special access program
SCG	security classification guide
SCI	sensitive compartmented information
SIPRNET	SECRET Internet Protocol Router Network
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USG	U.S. Government

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
alternative compensatory control measures	Additional controls to protect information when standard security measures are insufficient to enforce need-to-know for classified information but for which neither SCI nor SAP protections are warranted.
classification	Defined in E.O. 13526.
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 pursuant to E.O. 13526. Also applies to information classified at a lower level that, when combined with other information, could become classified at a higher level.
CNSI	Defined in E.O. 13526.
confidential source	Defined in E.O. 13526.
critical program information	Defined in DoDI 5200.39
CUI	Defined in DoDI 5200.48.
damage to the national security	Defined in E.O. 13526.
declassification	Defined in E.O. 13526.
Defense Security Enterprise	Defined in DoDD 5143.01.
derivative classification	Defined in E.O. 13526.
disclosure	The coordinated and approved oral and visual transfer of CNSI or CUI through approved channels to an authorized representative of a foreign government or international organization. "Disclosure" is oral and visual transfer of information. "Release" is physical transfer of documents or materiel.

TERM	DEFINITION
downgrading	Defined in E.O. 13526.
FCGR	A comprehensive review of the agency's classification guidance, particularly classification guides, to ensure the guidance reflects current circumstances and to identify classified information that no longer requires protection and can be declassified.
foreign government information	Defined in E.O. 13526.
formerly restricted data	Defined in Section 1045.30 of Title 10, CFR.
horizontal coordination	The process of conducting research to identify SCGs covering similar systems, plans, programs, projects, or missions to ensure consistent classification of information across multiple agencies, components, and organizations.
human-readable	Product output that is in a structured format which can be consumed (read) directly by a person.
IC	Defined in DoDM 5240.01.
Information Security Oversight Office	Established within the National Archives and Records Administration, acting in consultation with the National Security Advisor to implement and oversee agency actions to ensure compliance with E.O. 13526.
machine-readable	Product output that is in a structured format, typically XML, which can be consumed by another program using consistent processing logic.
national security	Defined in E.O. 13526.
OCA	Defined in E.O. 13526.
OPSEC	Defined in DoDD 5205.02E.
original classification	Defined in E.O. 13526.
restricted data	Defined in Section 1045.30 of Title 10, CFR.
SAO	Defined in E.O. 13526.

TERM	DEFINITION
SCG	A record of original classification decisions as determined and approved by the appropriate OCA used for derivative classification.
secondary distribution	Release of documents provided after primary distribution by the originator or controlling office.
unauthorized disclosure	A communication or physical transfer of classified information to an unauthorized recipient.
unclassified information	Information not meeting the criteria for classification set forth in E.O.13526.
uniqueness	The quality of being the only one of its kind or particularly remarkable, special, or unusual.

REFERENCES

Code of Federal Regulations, Title 10, Section 1045.30

Code of Federal Regulations, Title 32

DoD Directive 5143.01, "Under Secretary of Defense for Intelligence and Security (USD(I&S))," October 24, 2014, as amended

DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012, as amended

DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, as amended

DoD Instruction 5025.13, "DoD Plain Language Program," January 23, 2020, as amended

DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)," April 21, 2016, as amended

DoD Instruction 5200.39, "Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)," May 28, 2015, as amended

DoD Instruction 5200.48, "Controlled Unclassified Information (CUI)," March 6, 2020

DoD Instruction 5230.09, "Clearance of DoD Information for Public Release," January 25, 2019, as amended

DoD Instruction 5230.24, "Distribution Statements on DoD Technical Documents," January 10, 2023

DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 13, 2014, as amended

DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012, as amended

DoD Manual 5200.01, Volume 2, "DoD Information Security Program: Marking of Information," February 24, 2012, as amended

DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended

DoD Manual 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities," August 8, 2016

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

Order of December 29, 2009, "Original Classification Authority"

United States Code, Title 5, Section 552

United States Code, Title 42 (also known as the "Atomic Energy Act of 1954, as amended"

United States Code, Title 44, Section 3303