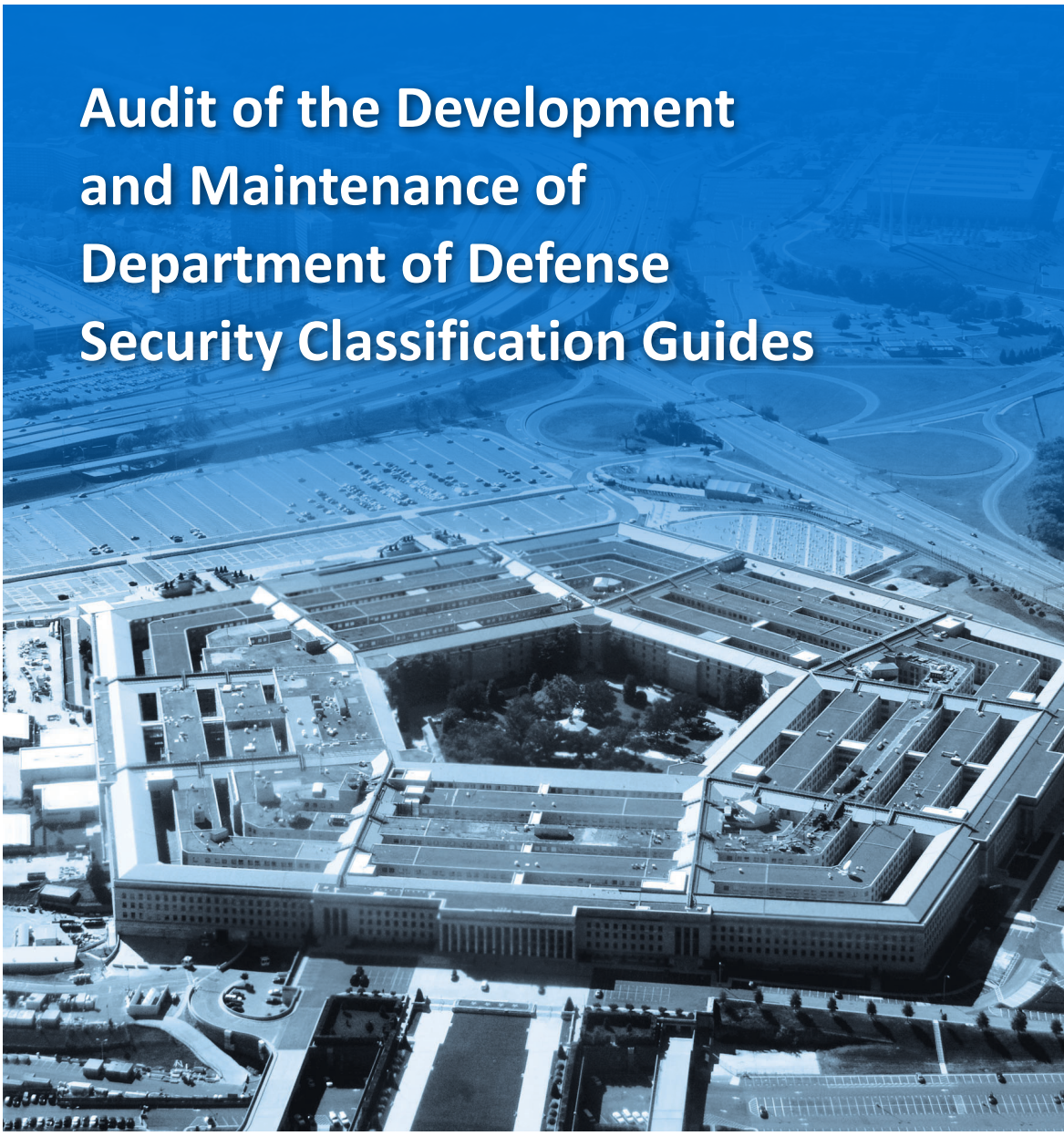
Report No. DODIG-2022-107

INSPECTOR GENERAL

U.S. Department of Defense

JUNE 21, 2022

Audit of the Development and Maintenance of Department of Defense Security Classification Guides



INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Results in Brief

Audit of the Development and Maintenance of Department of Defense Security Classification Guides

June 21, 2022

Objective

The objective of this audit was to determine whether DoD Components developed and maintained security classification guides (SCGs) in accordance with Federal and DoD guidance.

Background

The DoD uses SCGs to communicate the requirements for classifying and protecting sensitive DoD information. The SCGs identify the classification of a system, plan, program, project, or mission, including the level and duration of classification for protecting information critical to national security. An original classification authority (OCA) is an individual, authorized in writing, either by the President, Vice President, or an agency head, to classify sensitive information in the first instance and is responsible for developing and maintaining the accuracy of SCGs. Once an OCA issues an SCG, derivative classifiers use the SCGs to facilitate the proper and uniform classification of information. Derivative classification is the process of incorporating, paraphrasing, restating, or generating in a new form information that is already classified and marking the newly developed material consistent with classification guidance, which includes any applicable SCGs.

The DoD requires OCAs to follow seven steps when developing SCGs, provide a copy of each approved SCG to the Defense Technical Information Center (DTIC) index of SCGs, and review and update SCGs at least every 5 years to promote uniformity and consistency and to avoid classification conflicts between SCGs.

Background (cont'd)

We reviewed 50 SCGs during the audit. Of those 50 SCGs, we statistically selected 43 to review from a universe of 1,501 SCGs and nonstatistically selected an additional seven SCGs to review that we had used in previous audits or that had known problems.

Finding

DoD Component OCAs did not develop or maintain SCGs in accordance with Federal and DoD guidance. Of the 50 SCGs that we selected for review, the OCAs could not locate 3 of the SCGs and did not properly cancel another 4 SCGs that were no longer needed. For the remaining 43 SCGs, the OCAs did not:

- identify and review existing classification guidance to avoid classification conflicts between similar information for 38 SCGs;
- identify the items of information requiring protection for one SCG;
- identify how long the classification should remain in effect for 16 SCGs;
- identify the reasons for classifying information for 23 SCGs;
- identify the classification level of information for 34 SCGs;
- identify the SCG approval authority with program and supervisory responsibility over the information addressed for seven SCGs;
- provide a copy of the SCG to the DTIC for 15 SCGs;
- conduct a 5-year review and update 20 SCGs; or
- complete mandatory classification training before exercising their authority for 34 SCGs.

The DoD Components did not develop and maintain SCGs in accordance with Federal and DoD guidance because:

- the Under Secretary of Defense for Intelligence and Security did not direct, administer, and oversee the DoD process for developing and maintaining SCGs, as required by DoD Manual 5200.01, Volume 1, and DoD Manual 5200.45; and

Results in Brief

Audit of the Development and Maintenance of Department of Defense Security Classification Guides

Finding (cont'd)

- the DTIC did not establish business rules for the SCG index to ensure that OCAs could identify existing classification guidance relevant to the development of new SCGs. The DTIC also did not issue reminders to the OCAs concerning the required SCG 5-year review.

Based on the universe of 1,501 SCGs, we project that OCAs did not develop or maintain 1,257 SCGs (83.7 percent) in accordance with DoD guidance. Furthermore, we project that the OCAs would not be able to locate or had improperly canceled 244 SCGs (16.3 percent). Notably, we project at least one type of error in each of the 1,501 SCGs in the universe.

Inaccurate and incomplete SCGs increase the risk that derivative classifiers will incorrectly interpret or apply the guidance and; therefore, over- or under-classify information, classify similar information inconsistently across programs, or not declassify information in a timely manner. Over-classification can result in a lack of insight and transparency concerning DoD programs. Under-classification can result in unauthorized disclosure of classified information that can inform threat actors about critical DoD programs and systems. If immediate actions are not taken to address issues identified in this report, the DoD increases the risk of unauthorized disclosure of classified information and the potential for threat actors to gain unauthorized access to information about critical programs and systems.

Recommendations

We recommend that the Under Secretary of Defense for Intelligence and Security:

- Direct all DoD Component Heads to account for all SCGs under their purview.
- Direct all DoD Component Heads to immediately review all SCGs under their purview, and at least once every 5 years thereafter, and take action to update the SCGs as needed.
- Establish a process to ensure that the DoD Components, the OCAs, and the DTIC comply with the requirements in DoD Manual 5200.01, Volume 1, and DoD Manual 5200.45.
- In coordination with the Under Secretary of Defense for Research and Engineering, direct the DTIC to re-establish the 5-year reminder process to ensure that OCAs review and update SCGs as required.

In addition, we recommend that the DTIC Administrator, in coordination with the Under Secretary of Defense for Intelligence and Security, establish business rules for the SCG index, including an SCG naming, numbering, and formatting convention that will facilitate OCA searches of existing classification guidance to enable consistent classification of similar information throughout the DoD.

Management Comments and Our Response

The Deputy Director for Defense Intelligence, Counterintelligence, Law Enforcement, and Security, responding for the Under Secretary of Defense for Intelligence and Security, did not agree or disagree with the recommendations. Therefore, the Deputy Director should provide additional comments to the final report describing the steps that will be taken to direct DoD Component Heads to account for all SCGs under their purview and to establish a process to ensure compliance with DoD Manual 5200.01, Volume 1, and DoD Manual 5200.45.

The Deputy Director stated that an SCG review was underway in accordance with a 5-year review requirement in Executive Order 13526. Therefore, the recommendation to direct DoD Component Heads to conduct an SCG review is closed and no further action is required.

Comments (cont'd)

The DTIC Administrator disagreed with the recommendation to establish business rules for the SCG index, stating that "complex" rules would not guarantee a complete, accurate, and easily searchable SCG index, but would instead increase opportunities for error, making SCG retrieval more difficult. We do not consider a naming, numbering, and formatting convention as a set of "complex business rules," but instead necessary action to reduce classification conflicts and eliminate duplicate SCG index entries. Therefore, the DTIC Administrator should provide additional comments to the final report on the establishment of business rules to facilitate OCA searches of existing classification guidance.

Please see the Recommendations Table on the next page for the status of the recommendations.

Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Under Secretary of Defense for Intelligence and Security	1.a, 1.c	3	1.b
Administrator, Defense Technical Information Center	2	None	None

Please provide Management Comments by July 21, 2022.

Note: The following categories are used to describe agency management's comments to individual recommendations.

- **Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **Closed** – DoD OIG verified that the agreed upon corrective actions were implemented.

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

June 21, 2022

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY
ADMINISTRATOR, DEFENSE TECHNICAL INFORMATION CENTER

SUBJECT: Audit of the Development and Maintenance of Department of Defense Security Classification Guides (Report No. DODIG-2022-107)

This final report provides the results of the DoD Office of Inspector General's audit. We previously provided copies of the draft report and requested written comments on the recommendations. We considered management's comments on the draft report when preparing the final report. Those comments are included in the report.

This report contains three recommendations that are considered unresolved because management officials did not fully address the recommendations. Therefore, as discussed in the Recommendations, Management Comments, and Our Response section of this report, the recommendations will remain unresolved until an agreement is reached on the actions to be taken to address the recommendations. Once an agreement is reached, the recommendations will be considered resolved but will remain open until documentation is submitted showing that the agreed-upon actions are complete. Once we verify that the actions are complete, the recommendations will be closed.

This report contains one recommendation that is considered resolved. Therefore, as discussed in the Recommendations, Management Comments, and Our Response section of this report, the recommendation will remain open until documentation is submitted showing that the agreed-upon actions are complete. Once we verify that the actions are complete, the recommendation will be closed.

This report contains one recommendation that is considered closed as discussed in the Recommendations, Management Comments, and Our Response section of this report. That recommendation does not require further action.

DoD Instruction 7650.03 requires that recommendations be resolved promptly. For the unresolved recommendations, please provide us within 30 days your response concerning specific actions in process or alternative corrective actions proposed on the recommendations. For the resolved recommendations, please provide us within 90 days documentation showing

that the agreed-upon action has been completed. Your response should be sent as a PDF file to audcso@dodig.mil if unclassified or [redacted] if classified SECRET. Responses must have the actual signature of the authorizing official for your organization.

We appreciate the cooperation and assistance received during the audit. If you have any questions, please contact me at [redacted].

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations & Acquisition,
Contracting, and Sustainment

Contents

Introduction

Objective 1

Background 1

Review of Internal Controls 5

Finding. DoD Component OCAs Did Not Develop or Maintain SCGs in Accordance With Federal and DoD Guidance 6

DoD Component OCAs Could Not Locate or Did Not Properly Cancel SCGs 7

DoD Component OCAs Did Not Properly Develop or Maintain SCGs 8

The USD(I&S) Did Not Direct, Administer, or Oversee the DoD Process for Developing and Maintaining SCGs 16

The DTIC Did Not Establish Business Rules for the SCG Index or Issue Review Reminders to OCAs 16

Inaccurate and Incomplete SCGs Reduce the DoD's Ability to Protect National Security Information 17

Management Comments on the Finding and Our Response 18

Recommendations, Management Comments, and Our Response 19

Appendixes

Appendix A. Scope and Methodology 24

Internal Control Assessment and Compliance 25

Use of Computer-Processed Data 26

Use of Technical Assistance 26

Prior Coverage 26

Appendix B. SCGs Reviewed 28

Appendix C. Statistical Sample 30

Management Comments

USD(I&S) 32

DTIC 34

Acronyms and Abbreviations 36

Glossary 37


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Introduction

Objective

The objective of this audit was to determine whether DoD Components developed and maintained security classification guides (SCGs) in accordance with Federal and DoD guidance. See Appendix A for a discussion of the scope and methodology and prior coverage related to the audit objective. See the Glossary for definitions of technical terms.

Background

The DoD uses SCGs to communicate the requirements for classifying and protecting sensitive DoD information. The SCGs identify the classification of a system, plan, program, project, or mission, including the level and duration of classification for protecting information critical to national security. The level of classification identifies whether the information is TOP SECRET, SECRET, or CONFIDENTIAL. If inappropriately released, TOP SECRET information could cause exceptionally grave damage to national security; SECRET information could cause serious damage to national security; and CONFIDENTIAL information could cause damage to national security. The duration of classification identifies the specific date or events for downgrading or declassifying information included in an SCG.

An original classification authority (OCA) is an individual, authorized in writing, either by the President, Vice President, or an agency head, to classify sensitive information in the first instance and is responsible for developing and maintaining the accuracy of SCGs. Once an OCA issues an SCG, derivative classifiers use the SCGs to facilitate the proper and uniform classification of information. Derivative classification is the process of incorporating, paraphrasing, restating, or generating in a new form information that is already classified and marking the newly developed material consistent with classification guidance, which includes any applicable SCGs.

Executive Order 13526 and Title 32 Code of Federal Regulations section 2001 prescribe a uniform system for classifying, safeguarding, and declassifying national security information.[1] Executive Order 13526 and Title 32 Code of Federal Regulations section 2001 require Federal agencies with an OCA to:

- develop SCGs;
- provide OCAs annual mandatory training on the proper application of classification principles;

[1] Executive Order 13526, "Classified National Security Information," December 29, 2009; and Title 32 Code of Federal Regulations, section 2001, "Classified National Security Information."

- conduct a comprehensive review of SCGs to ensure that the guides reflect up-to-date requirements; and
- identify classified information that no longer requires protection and can be declassified.

DoD Manual 5200.45 requires DoD Components to issue SCGs for weapon systems, military plans, and operations (among other categories); review security classification guidance every 5 years for currency and accuracy; and update or cancel SCGs as required.[2]

Roles and Responsibilities

DoD Manual 5200.01, Volume 1, and DoD Manual 5200.45 assign roles and responsibilities for implementing a standard SCG management process.[3] Specifically, the Under Secretary of Defense for Intelligence and Security (USD[I&S]) is required to:

- direct, administer, and oversee the development, distribution, maintenance, revision, and cancellation of SCGs; and
- establish and enforce policies and procedures for developing and classifying SCGs.

DoD Manual 5200.01, Volume 1 also requires heads of DoD Components to direct the head of each activity within the DoD Component that creates classified information to properly manage and oversee the activity's development, distribution, maintenance, revision, and cancellation of SCGs.

OCAs are required to:

- develop and approve SCGs to facilitate the proper and uniform derivative classification of information;
- review SCGs as necessary and at least once every 5 years; and
- submit changes to an SCG to the Defense Technical Information Center (DTIC) using DD Form 2024.[4]

[2] DoD Manual 5200.45, "Instructions for Developing Security Classification Guides," April 2, 2013, Incorporating Change 1, April 6, 2018, and Incorporating Change 2, September 15, 2020.

[3] DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification and Declassification, February 24, 2012, Incorporating Change 1, May 4, 2018, and Incorporating Change 2, July 28, 2020.

[4] OCAs use DD Form 2024, "DoD Security Classification Guide Certified Data Elements," to submit changes to an SCG.

Furthermore, the DTIC, under the authority, direction, and control of the Under Secretary of Defense for Research and Engineering, is responsible for maintaining an index of SCGs in an online database accessible through www.dodtechipedia.mil.[5] The DTIC is also responsible for sending reminders to DoD Components to conduct the required 5-year SCG review and submit any changes using DD Form 2024.

Requirements for Developing and Maintaining SCGs

DoD Manual 5200.45 requires OCAs to follow seven steps when developing SCGs.

Step 1: Consider Related Current Guidance. Identify and review existing classification guidance to avoid conflicts between SCGs. When existing classification guidance is similar but not the same, include an explanation of the classification differences in the SCG.

Step 2: Determine the State-of-the-Art Status. Determine whether the information is known or published domestically or in foreign countries. To make that determination for scientific or technical information, the OCA should consult technical and intelligence specialists.

Step 3: Identify the National Advantage. Review the information and decide what the system, plan, program, project, or mission does or seeks to accomplish that will result in a net advantage to the United States.[6]

Step 4: Make the Initial Classification Determination. Conduct an analysis to identify the information that should be classified to protect the national advantage, with emphasis on some of the more specific information or data that covers performance capabilities, vulnerabilities, and weaknesses.

Step 5: Identify Specific Items of Information That Require Classification. Determine what information must be protected to prevent access by hostile forces, and develop or apply timely and effective countermeasures. Examples of information that require classification include information about military plans, weapons systems, and vulnerabilities to national security.

Step 6: Determine the Duration of Classification. Determine how long the classification should remain in effect, determine the appropriate declassification instructions for each item of classified information, and evaluate the possibility of downgrading the classification.

[5] Only SCGs that are classified up to the SECRET level are required to be submitted to the DTIC. SCGs that are classified at the TOP SECRET, Sensitive Compartmented Information, or Special Access Program level and any SCGs deemed by the OCA to be too sensitive for automatic secondary distribution are not required to be submitted to the DTIC. For the purpose of this report, we only reviewed SCGs that are classified up to the SECRET level.

[6] National advantage refers to the benefits, direct or indirect, that the United States can accrue or be expected to accrue based on classifying information.

Step 7: Write the SCG. The OCA who has program or supervisory responsibility over the information addressed in the SCG should be identified in the SCG, as well as the office of primary responsibility that can be contacted for clarification or additional information. The SCG should state the specific information elements that require protection and include the classification levels, reasons of classification, duration of classification, and any required downgrading actions for the information.

In addition, DoD Manuals 5200.01, Volume 1, and 5200.45 require OCAs to:

- provide a copy of each approved SCG to the DTIC upon issuance; and
- review and update the issued SCGs at least once every 5 years to promote uniformity and consistency and to avoid classification conflicts between SCGs.

OCAs are required to complete mandatory classification training before exercising their authority as OCAs and annually thereafter.

SCGs Selected for Review

We selected 50 SCGs to review. We selected a statistical sample of 43 SCGs to review from a universe of 1,501 SCGs.[7] The SCGs we selected were classified at either the UNCLASSIFIED, CONFIDENTIAL, or SECRET levels. We also nonstatistically selected for review an additional seven SCGs that we had used in prior audits or that had known problems, such as incorrect classification of ordnance-related information and conflicts with other ordnance-related SCGs. Table 1 lists the number of SCGs reviewed by DoD Component. See Appendix B for a list of the SCGs that we reviewed.[8]

Table 1. DoD Component SCGs Selected for Review

DoD Component	SCGs Statistically Selected	SCGs Nonstatistically Selected
Army	13	0
Navy	12	3
Air Force	6	0
USD(I&S)	0	1
USD(A&S)	1	0
USSOCOM	2	1
USCYBERCOM	0	1

[7] The Office of the USD(I&S) provided the universe of 1,501 SCGs on August 28, 2020.

[8] As shown in Appendix B, we numbered the SCGs 1-50 for ease of reference.

Table 1. DoD Component SCGs Selected for Review (cont'd)

DoD Component	SCGs Statistically Selected	SCGs Nonstatistically Selected
USINDOPACOM	0	1
USEUCOM	1	0
DARPA	4	0
SCO	2	0
MDA	1	0
TRMC	1	0
Total	**43**	**7**

Legend

DARPA	Defense Advanced Research Projects Agency
MDA	Missile Defense Agency
SCO	Strategic Capabilities Office
TRMC	Test Resource Management Center
USCYBERCOM	U.S. Cyber Command
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USEUCOM	U.S. European Command
USINDOPACOM	U.S. Indo-Pacific Command
USSOCOM	U.S. Special Operations Command

Source: The DoD OIG.

Review of Internal Controls

DoD Instruction 5010.40 requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls.[9] We identified internal control weaknesses related to SCG development, maintenance, and accountability. We will provide a copy of the final report to the senior officials responsible for internal controls at the Military Services, combatant commands, Office of the Secretary of Defense, and Defense agencies.

[9] DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

Finding

DoD Component OCAs Did Not Develop or Maintain SCGs in Accordance With Federal and DoD Guidance

DoD Component OCAs did not develop or maintain SCGs in accordance with Federal and DoD guidance. Of the 50 SCGs that we selected for review, the OCAs could not locate 3 of the SCGs and did not properly cancel another 4 SCGs that were no longer needed. For the remaining 43 SCGs, the OCAs did not:

- identify and review existing classification guidance to avoid classification conflicts between similar information for 38 SCGs;
- identify the items of information requiring protection for one SCG;
- identify how long the classification should remain in effect for 16 SCGs;
- identify the reasons for classifying information for 23 SCGs;
- identify the classification level of information for 34 SCGs;
- identify the SCG approval authority with program and supervisory responsibility over the information addressed for seven SCGs;
- provide a copy of the SCG to the DTIC for 15 SCGs;
- conduct a 5-year review and update for 20 SCGs; or
- complete mandatory classification training before exercising their authority for 34 SCGs.

The DoD Component OCAs did not develop or maintain SCGs in accordance with Federal and DoD guidance because the USD(I&S) did not direct, administer, or oversee the DoD process for developing and maintaining SCGs, as required by DoD Manual 5200.01, Volume 1 and DoD Manual 5200.45. In addition, the DTIC did not establish business rules for the SCG index to ensure that the OCAs could identify existing classification guidance relevant to the development of new SCGs. The DTIC also did not issue reminders to the OCAs concerning the required SCG 5-year review.

Based on the universe of 1,501 SCGs, we project that the OCAs did not develop or maintain 1,257 SCGs (83.7 percent) in accordance with DoD guidance. Furthermore, we project that the OCAs would not be able to locate or had improperly canceled 244 SCGs (16.3 percent). Notably, we project at least one type of error in each of the 1,501 SCGs in the universe. Inaccurate and incomplete SCGs increase the risk that derivative classifiers will incorrectly interpret or apply the guidance and; therefore, over- or under-classify information, classify similar

information inconsistently across programs, or not declassify information in a timely manner. Over-classification can result in a lack of insight and transparency concerning DoD programs. Under-classification can result in unauthorized disclosure of classified information that can inform threat actors about critical DoD programs and systems. If immediate actions are not taken to address issues identified in this report, the DoD increases the risk of unauthorized disclosure of classified information and the potential for threat actors to gain unauthorized access to information about critical programs and systems.

DoD Component OCAs Could Not Locate or Did Not Properly Cancel SCGs

DoD Component OCAs could not locate three SCGs or did not properly cancel another four SCGs.

DoD Component OCAs could not locate three SCGs or did not properly cancel another four SCGs, as required by DoD Manual 5200.01, Volume 1. Specifically, the OCAs for the Navy could not locate a copy of "CG-RN-1 Rev 3 DOE-DoD Classification Guide for the Naval Nuclear Propulsion Program" SCG (SCG #20) or "Supercavitating High Speed Bodies Technology" SCG (SCG #22), and the OCA for the USD(A&S) could not locate a copy of "USD(A&S)" SCG (SCG #41). In addition, the OCAs for the Army, Navy, and the Air Force did not properly cancel the "Cerberus-Lite Scout Portable Surveillance System" SCG (SCG #1), "Contingency Expeditionary Force" SCG (SCG #12), on each end of the "Landing Craft, Air Cushion" SCG (SCG #17), or "Neptune Eagle" SCG (SCG #34).

To obtain copies of the SCGs, we requested the SCGs from the Office of the USD(I&S), applicable DoD Components, or the DTIC. For the three SCGs that the OCAs could not locate, we requested copies from DTIC officials, who also were unable to provide a copy of the SCGs, although the SCG titles were on the DTIC index for two of the SCGs. While DoD guidance does not specifically address SCG accountability or the need to conduct an inventory of SCGs, DoD Manuals 5200.01, Volume 1, and 5200.45 require that OCAs maintain a copy of SCGs and provide a copy to the DTIC once an SCG is issued.

For the four improperly canceled SCGs, DoD Manual 5200.01, Volume 1, states that SCGs should be canceled when all information the SCG specifies as classified has been declassified, or if a new SCG incorporates the classified information covered by the old SCG and there is no reasonable likelihood that any information not included in the new SCG would be the subject of derivative classification. DoD Manual 5200.01, Volume 1, also states that upon canceling an SCG, the OCA

should maintain a copy of the canceled SCG and submit a DD Form 2024 to the DTIC. However, the OCAs for the four improperly canceled SCGs did not send the required form to the DTIC.

On February 2, 2022, Navy officials stated that they had SCG #20 and provided us a copy of the front cover. However, the officials stated that the Navy could not provide a copy of the SCG to the DTIC because the Department of Energy deemed the SCG to be too sensitive and limited its distribution. In addition, Navy officials stated that they could not initially locate SCG #22 because the title and the internal Navy identification number for the SCG changed. However, the Navy did not provide a copy of a DD Form 2024 to verify the change.

DoD Component OCAs Did Not Properly Develop or Maintain SCGs

DoD Component OCAs did not develop and maintain 43 SCGs in accordance with Executive Order 13526 and DoD Manuals 5200.01, Volume 1, and 5200.45.

DoD Component OCAs did not develop and maintain 43 SCGs in accordance with Executive Order 13526 and DoD Manuals 5200.01, Volume 1, and 5200.45. To determine whether the DoD Component OCAs properly developed and maintained the SCGs, we obtained, reviewed, and analyzed the SCGs to verify whether the OCAs followed the seven steps for developing the SCGs and other requirements for maintaining the SCGs. The deficiencies we identified are summarized by DoD Component in Table 2.

Table 2. SCG Deficiencies Identified by DoD Component

SCG Deficiencies Identified	Army	Navy	Air Force	USD(I&S)	USSOCOM	USEUCOM	USCYBERCOM	USINDOPACOM	DARPA	SCO	MDA	TRMC
Existing Classification Guidance Was Not Identified and Reviewed to Avoid Conflicts	8	11	4	1	3	1	1	1	4	2	1	1
Information Requiring Protection Was Not Identified	0	0	1	0	0	0	0	0	0	0	0	0
Duration for Classifying Information Was Not Identified	3	1	3	1	1	1	1	1	2	2	0	0
Reasons for Classifying Information Were Not Identified	6	5	3	1	1	0	1	1	2	2	1	0
Classification Level for Information Was Not Identified	6	10	5	0	3	1	1	1	3	2	1	1
OCA Not Identified	0	7	0	0	0	0	0	0	0	0	0	0
Copy Not Provided to the DTIC	2	0	2	1	3	1	0	1	1	2	1	1
Not Reviewed and Updated Every 5 Years	2	7	4	0	2	0	0	1	3	0	0	1

Source: The DoD OIG.

OCAs Did Not Avoid Classification Conflicts

The OCAs for the Army, Navy, Air Force, USD(I&S), USSOCOM, USEUCOM, USCYBERCOM, USINDOPACOM, DARPA, SCO, MDA, and TRMC did not identify or review existing classification guidance to avoid conflicts between similar information for 38 SCGs as required by Step 1 of the SCG development process. A classification conflict occurs when two SCGs contradict each other in terms of the classification markings. We identified classification conflicts related to space systems, biometrics, weapon systems, financial information, military exercises, cyberspace systems, sensors, ordnance activities, combat vehicles, and directed energy. For example, the Air Force "Operationally Responsive Space-2" SCG (SCG #29) and DARPA "Lorentz Force Orbitology Study" SCG (SCG #43) identified the space program's mission information as UNCLASSIFIED, while the Air Force "Automated Navigation and Guidance Experiment for Local Space" SCG (SCG #30) identified similar information as TOP SECRET. Table 3 identifies the conflicting guidance by SCG.

Table 3. SCGs With Conflicting DoD Security Classification Guidance

SCG #	DoD Program	Information With Classification Conflicts	Classification Level				
			UNCLASSIFIED	FOUO	CONFIDENTIAL	SECRET	TOP SECRET
29, 30, 33, 43	Space	Mission	Air Force, DARPA	Air Force	Air Force	Air Force	Air Force
27, 29, 30, 31, 33, 43		Spacecraft Drawings and Specification	Air Force, Navy, DARPA	Air Force	n/a	n/a	n/a
27, 29, 30, 31, 43		Performance and Capability	Air Force	Air Force	Air Force, Navy	Air Force, DARPA	Air Force
6, 8	Biometric	Funding and Budget	Army	Army	n/a	n/a	n/a
6, 8		Work Force	Army	Army	n/a	n/a	n/a
6, 8		Technical Details	Army	Army	n/a	n/a	n/a
6, 8		Training Requirement	n/a	Army	n/a	Army	n/a

Table 3. SCGs With Conflicting DoD Security Classification Guidance (cont'd)

SCG #	DoD Program	Information With Classification Conflicts	Classification Level				
			UNCLASSIFIED	FOUO	CONFIDENTIAL	SECRET	TOP SECRET
2, 13, 23, 32, 44	Weapon System	Countermeasure Vulnerabilities	n/a	n/a	Navy	Army, Air Force, DARPA	Air Force
2, 13, 23, 32, 44		Reliability of Weapon System	Army	n/a	Navy	Army, Air Force, DARPA	n/a
2, 11, 13, 23, 44		Performance Range	n/a	n/a	Navy	Army, DARPA	n/a
2, 13, 23, 32		System Accuracy	Army	n/a	Navy	Army, Air Force	n/a
2, 13, 23, 32, 44		Effectiveness of Weapon Systems	DARPA	DARPA	Navy, DARPA	Army, DARPA	Air Force
2, 23, 24, 32		Nose and Warhead Hardware	Army, Navy, Air Force	n/a	Navy	n/a	n/a
38, 42	Financial Information	Financial Code	USD(I&S)	USD (I&S)	USD (I&S)	USD(I&S), USSOCOM	USD(I&S), USSOCOM
38, 42		Customer Record	USD(I&S)	USSOCOM	n/a	n/a	n/a
36, 37	Military Exercises	Personnel	n/a	USEUCOM	n/a	USINDOPACOM	n/a
36, 37		Exercise Dates	USEUCOM	n/a	USINDOPACOM	n/a	n/a
35, 48, 50	Cyberspace Systems	Performance and Effectiveness	n/a	SCO	SCO	TRMC, USCYBERCOM, SCO	n/a
35, 48, 50		Test Results	TRMC	SCO, TRMC	SCO, TRMC	USCYBERCOM, SCO, TRMC	TRMC
35, 50		Advanced Technology	n/a	n/a	n/a	TRMC	USCYBERCOM

Table 3. SCGs With Conflicting DoD Security Classification Guidance (cont'd)

SCG #	DoD Program	Information With Classification Conflicts	Classification Level				
			UNCLASSIFIED	FOUO	CONFIDENTIAL	SECRET	TOP SECRET
19, 21, 26, 29, 47, 49	Sensor	Initial Operational Capability	Navy, MDA	Navy, MDA, SCO	Navy, MDA, SCO	MDA, SCO	n/a
4, 19, 21, 26, 28, 47, 49		Algorithms	Navy, MDA	MDA	MDA	Army, Navy, MDA, SCO	n/a
15, 16	Ordnance	Budget Submission	n/a	Navy	Navy	n/a	n/a
14, 15		Milestone	Navy	Navy	Navy	n/a	n/a
14, 15		Technical Detail	n/a	Navy	Navy	Navy	n/a
17, 25	Combat Vehicles	Deficiencies	Navy	n/a	n/a	Navy	n/a
17, 18, 25		Funding	n/a	Navy	Navy	Navy	n/a
45, 46	Directed Energy	External Views, Photographs, and Drawings	DARPA	DARPA	DARPA	DARPA	DARPA
45, 46		Military Applications	DARPA	DARPA	DARPA	DARPA	n/a
45, 46		Laser Pulse Interaction	DARPA	DARPA	DARPA	DARPA	DARPA

SCG # = Corresponds with SCG Title as documented in Appendix B.

*n/a = not applicable

Source: The DoD OIG.

An Air Force OCA Did Not Identify Information Requiring Protection

An OCA for the Air Force did not identify all the specific information requiring protection on each side of "Operationally Responsive Space-2" SCG (SCG #29) as required by Step 5 of the SCG development process. To determine whether OCAs identified information that must be protected, we reviewed SCGs and interviewed DoD officials from the DoD Components responsible for the SCG to identify the process they followed for identifying information that must be protected.

Instead of identifying information requiring protection in SCG #29, the OCA included blank sections in the SCG with the heading "reserved." We requested additional information about the meaning of the "reserved" sections, but Air Force officials stated that they did not have historical knowledge of the development of SCG #29. After we informed Air Force officials of this deficiency, they provided documentation verifying that the SCG was canceled in August 2014.

OCAs Did Not Identify Classification or Declassification Instructions for All SCGs

OCAs did not identify classification or declassification instructions as required by Step 6 of the SCG development process. Specifically,

- OCAs for the Army, Navy, Air Force, USD(I&S), USSOCOM, USCYBERCOM, USEUCOM, USINDOPACOM, DARPA, and SCO did not identify how long the classification should remain in effect for 16 SCGs. For example, the OCA for the "Army Joint Air-to-Ground Missile" SCG (SCG #13) did not identify the duration for classifying information, including performance requirements and non-armor targets, in 45 instances throughout the SCG.
- OCAs for the Army, Navy, Air Force, USD(I&S), USSOCOM, USCYBERCOM, USINDOPACOM, DARPA, SCO, and MDA did not identify the reasons for classifying specific information in 23 SCGs. For example, the OCA for the "Navy Explosive Ordnance Disposal Non-Nuclear" SCG (SCG #15) did not identify the reasons for classifying information, including ordnance items under development and area denial munitions, in 38 instances throughout the SCG.
- OCAs for the Army, Navy, Air Force, USSOCOM, USEUCOM, USCYBERCOM, USINDOPACOM, DARPA, SCO, MDA, and TRMC did not identify the classification level for specific information in 34 SCGs. For example, the OCA for the "Army Small Satellite" SCG (SCG #9) did not specify the classification level for satellite operational information and technical data, in 35 instances throughout the SCG.

Navy OCAs Did Not Identify the SCG Approval Authority

Navy OCAs did not identify themselves as the SCG approval authority as required by Step 7 of the SCG development process for seven SCGs. An SCG is the written record of an OCA's original classification decision, and accordingly the OCA should be identified in the SCG. If the OCA is not identified, there is no assurance that the SCG contains valid and verifiable information and users of the SCG do not have the OCA's contact information for questions or comments.

OCAs Did Not Provide SCGs to the DTIC

OCAs for the Army, Air Force, USD(I&S), USSOCOM, USEUCOM, USINDOPACOM, DARPA, SCO, MDA, and TRMC did not provide 15 SCGs to the DTIC. DoD Manual 5200.01, Volume 1, requires OCAs to provide a copy of each approved SCG to the DTIC, in part to facilitate Step 1 of the SCG development process.
Table 4 identifies the SCGs that were not provided to the DTIC.

Table 4. SCGs Not Provided to the DTIC

SCG #	DoD Component	SCG Title
7	Army	Foreign Material Program
10	Army	Rhino Explosive Hazard Pre-Detonation System
31	Air Force	Aerospace Vehicle Equipment Increment 1 Program
34	Air Force	Neptune Eagle*
36	USEUCOM	Supplemental SCG for Austere Challenge
37	USINDOPACOM	United States Forces Korea SCG*
38	USSOCOM	Sensitive Financial Operations*
39	USSOCOM	Identity Management
40	USSOCOM	Army Special Operations Aviation Rotary Wing Modernization Program
42	USD(I&S)	Financial Management for Sensitive Activities*
45	DARPA	Siren Study Project
47	MDA	Combined Optical Measurements Experimentation Test
48	SCO	Program Specific Protection Plan for LiTE Saber
49	SCO	Program Specific Protection Plan for Vanguard
50	TRMC	National Cyber Range

SCG # = Corresponds with SCG Title as documented in Appendix B.
* = SCGs that were nonstatistically selected for review.
Source: The DoD OIG.

OCAs Did Not Review or Update SCGs Every 5 Years

The OCAs for the Army, Navy, Air Force, USSOCOM, USINDOPACOM, DARPA, and TRMC did not conduct 5-year reviews for 20 SCGs. DoD Manual 5200.45 requires OCAs to review and update SCGs at least once every 5 years to promote uniformity and consistency and avoid classification conflicts between SCGs. According to DoD officials, the OCAs did not review and update the SCGs because of personnel constraints and because they did not receive reminders from the DTIC when the SCGs were approaching their 5-year review requirement.

Some OCAs had not reviewed or updated their SCGs since the SCGs were issued. For example, an OCA for DARPA did not review or update the "Lorentz Force Orbitology Study" SCG (SCG #43) since the issuance of the SCG in February 2007, more than 14 years ago. An OCA for the Air Force did not review or update the "Single Channel Transponder System" SCG (SCG #33) since February 2012, more than 9 years ago. In addition, an OCA for USINDOPACOM did not review or update the "U.S. Forces Korea" SCG (SCG #37) since 2005, more than 16 years ago.

OCAs Did Not Consistently Complete Mandatory Classification Training

The OCAs for the Army, Navy, Air Force, USD(A&S), USSOCOM, USINDOPACOM, SCO, and TRMC did not consistently complete the mandatory classification training before exercising their authority for 34 SCGs. To determine whether the OCAs completed the training, we requested that the OCAs provide documentation to support completion of classification training from FY 2016 through FY 2020. Table 5 identifies the results by DoD Component.

Table 5. Number of SCGs for Which OCAs Did Not Complete Classification Training, by DoD Component

DoD Component	FY 2016 Through FY 2020
Army	11
Navy	11
Air Force	4
USD(A&S)	1
USSOCOM	3
USINDOPACOM	1
SCO	2
TRMC	1
Total	**34**

Source: The DoD OIG.

The USD(I&S) Did Not Direct, Administer, or Oversee the DoD Process for Developing and Maintaining SCGs

USD(I&S) did not direct, administer, or oversee the DoD process for developing and maintaining SCGs, as required by DoD Manual 5200.01, Volume 1, and DoD Manual 5200.45. We identified recurring, systemic, and unaddressed problems at every level throughout the SCG development and maintenance process. Based on the universe of 1,501 SCGs, we project that the OCAs did not develop or maintain 1,257 SCGs (83.7 percent) in accordance with DoD guidance. Furthermore, we project that the OCAs would not be able to locate or had improperly canceled 244 SCGs (16.3 percent). Notably, we project at least one type of error in each of the 1,501 SCGs in the universe. As the DoD official with primary oversight responsibility for the DoD's information security program, it is incumbent on the USD(I&S) to ensure that DoD Components effectively and efficiently implement the SCG process.

As the DoD official with primary oversight responsibility for the DoD's information security program, it is incumbent on the USD(I&S) to ensure that DoD Components effectively and efficiently implement the SCG process.

We initially identified this audit as a priority because of findings and recommendations made in prior DoD OIG reports that indicated problems with SCGs existed. For example, in Report No. DODIG-2020-101, we reported that the Department of the Navy did not consistently classify and protect ordnance-related information in accordance with DoD Manuals 5200.01, Volumes 1 and 2, and Naval Supply Systems Command-Navy Ammunition Logistics Command P-724. We also reported that the Department of the Navy did not avoid conflicts between the "Navy Inventory Management" SCG and other ordnance-related SCGs. In that report, we recommended that the USD(I&S) develop a policy to ensure that SCGs are coordinated across the Department and the Military Services to avoid classification conflicts before finalizing SCGs.[10] That recommendation remained open as of January 2, 2022, 18 months after the report was issued.

The DTIC Did Not Establish Business Rules for the SCG Index or Issue Review Reminders to OCAs

The DTIC did not establish business rules for the SCG index or issue reminders to OCAs to conduct the required 5-year SCG reviews. The SCG index was designed to be the authoritative source for OCAs and derivative classifiers and the review of the SCG index is a critical part of Step 1 of the SCG development process. During

[10] Report No. DODIG-2020-101, "Naval Ordnance Data Classification Issues Identified During the Oversight of the U.S. Navy General Fund Financial Statement Audit for FY 2020," July 2, 2020.

the audit, we requested access to the index so we could identify a sample of SCGs to review; however, we identified so many discrepancies that we were unable to rely on the index to determine our sample. For example, we identified 62 duplicate SCGs when we first accessed the index and as of December 2, 2021, 31 of those duplicates remained. In addition, we compared SCG inventories provided by the DoD Components to the index and identified 1,618 SCGs that were not included in DTIC's SCG index but should have been. Furthermore, we determined that because the index did not have a standard naming convention, many of the SCG names in the index did not match the actual name of the SCG, which made it difficult for OCAs to identify and review existing SCGs to avoid conflicts between SCGs.

We identified 1,618 SCGs that were not included in DTIC's SCG index but should have been.

An accurate and complete SCG index will also help DTIC officials identify SCGs that are due for the required 5-year review and send a reminder to the responsible OCAs. DTIC officials stated that they were not sending the reminders because the DTIC and the USD(I&S) had a "verbal agreement exempting the DTIC from this responsibility." However, officials in the Office of the USD(I&S) stated that no such agreement existed and that the DTIC should have been sending the reminders.

Inaccurate and Incomplete SCGs Reduce the DoD's Ability to Protect National Security Information

Inaccurate and incomplete SCGs increase the risk that derivative classifiers will incorrectly interpret or apply the classification guidance and therefore, over- or under-classify critical national security information, classify similar information inconsistently across programs, or not declassify information in a timely manner. Over-classification can result in unnecessarily restricted information sharing and a lack of insight and transparency concerning DoD programs. Under-classification can result in unauthorized disclosure of classified information that can inform threat actors about critical DoD programs and systems. For example, officials in the Office of the USD(I&S) stated that in 2021, a derivative classifier applied classification markings to a document based on an SCG that should have been updated but was not. Those actions resulted in spillage of classified information through multiple media outlets, allowing threat actors easy access to that information. As stated previously, the projection of our statistically sampled results indicates that there is at least one type of error in each of

The projection of our statistically sampled results indicates that there is at least one type of error in each of the 1,501 SCGs in the universe.

the 1,501 SCGs in the universe. This projection and the findings of our report are significant and necessitate immediate action to address the recommendations and reduce the risk of unauthorized disclosure of national security information.

Management Comments on the Finding and Our Response

Undersecretary of Defense for Intelligence and Security Comments

The Deputy Director for Defense Intelligence, Counterintelligence, Law Enforcement, and Security, responding for the USD(I&S), stated that this report offers a revealing look at a priority item for the Defense Security Enterprise. The Deputy Director added that it would be instructive and supportive of the Defense Security Enterprise's strategy if the DoD OIG would recommend that the:

- DoD Components elevate security within their funding priorities; and
- Director, Cost Assessment and Program Evaluation independently assess how effectively the DoD Components are integrating security into their programming requests.

The Deputy Director stated that if the DoD OIG's intent was to report that the USD(I&S) did not "sufficiently" direct, administer, or oversee the DoD process for developing and maintaining SCGs in accordance with DoD guidance, then the DoD OIG should also acknowledge the responsibilities of the DoD Components to execute and sufficiently resource requirements. The Deputy Director further stated that when the DoD's challenges are attributed to Component-level under-resourcing, competing priorities, or inattentiveness, the primary challenge is not a policy gap, but a compliance gap.

The Deputy Director also stated that while the projected error rate was concerning, the underlying assumption is that the error rate in the SCG population remains constant with the 3-percent sample size selected by the audit team. The Deputy Director added that it would be instructive to know the statistical significance of the sample, as well as any other mathematical formulas used by the OIG to arrive at the error rate.

Our Response

We agree that SCGs are an important priority for the Defense Security Enterprise because incorrect and incomplete SCGs increase the risk of unauthorized access and disclosure of classified information. We also agree that the primary challenges identified in this report are attributable to non-compliance with Federal and

DoD guidance, and we directly make that attribution in the first sentence of the Finding and throughout the report. The report recommendations were directed to the USD(I&S), as the USD(I&S) has responsibility pursuant to DoD Manuals 5200.01, Volume 1 and DoD Manual 5200.45, to oversee the development, distribution, maintenance, revision, and cancellation of SCGs and enforce policies and procedures for developing SCGs.

We acknowledge the roles and responsibilities of the DoD Component Heads in the Background section of this report; however, we made recommendations to the USD(I&S) because our findings were systemic and pervasive across all DoD Component SCGs reviewed, and therefore require USD(I&S) attention and action. With respect to making recommendations to the DoD Components to elevate security in their funding priorities, the establishment of funding priorities is a management decision and while management could use the findings in this report to help inform those priorities, such decisions include factors outside the scope of this audit.

With regards to the Deputy Director's concerns on the projected error rate and the sample size, Appendix C of this report, which was provided to the USD(I&S) as part of the draft report, contains a detailed discussion on the universe, sample, and projections. We developed our sample using an attribute design for a simple random sampling without replacement, which allows error rates to be projected onto a population. Based on our sample size of 43 SCGs, using a 90-percent confidence level for the detection of errors, we calculated the SCG error rate to be 83.7 percent of the SCG population. In addition, we calculated that the OCAs would not be able to locate 7 percent of the SCGs and that 9.3 percent were improperly canceled. Using these reliable estimates, as previously stated in this report, we project at least one type of error in each of the 1,501 SCGs in the universe. See Appendix C for additional information on the sample and projected error rates.

Recommendations, Management Comments, and Our Response

Recommendation 1

We recommend that the Under Secretary of Defense for Intelligence and Security:

a. Direct all DoD Component Heads to account for all security classification guides under their purview.

b. Direct all DoD Component Heads to immediately review all security classification guides under their purview, and at least once every 5 years thereafter, and take action to update security classification guides as needed.

c. Establish a process to ensure that DoD Components, the original classification authorities, and the Defense Technical Information Center comply with the requirements in DoD Manual 5200.01, Volume 1, and DoD Manual 5200.45.

Undersecretary of Defense for Intelligence and Security Comments

The Deputy Director for Defense Intelligence, Counterintelligence, Law Enforcement, and Security, responding for the USD(I&S), did not agree or disagree with the recommendations. However, the Deputy Director stated that the Defense Security Executive issued a memorandum on July 26, 2021, that requested DoD Components assist the USD(I&S) in reemphasizing and reinforcing existing SCG policy requirements based on preliminary feedback from the DoD OIG audit and USD(I&S) staff research.[11] The Defense Security Executive memorandum states that DoD Component Heads are responsible for the overall management, functioning, and effectiveness of their information security programs, including overseeing OCAs to ensure they personally approve, issue, and provide copies of their SCGs to the DTIC, or provide a justification to the USD(I&S) for any omissions. In the memorandum, the Defense Security Executive directs the Component Heads to ensure that all DoD personnel who participate in developing SCGs complete OCA classification training and that DoD Component security managers maintain the classification training documentation and make it available for inspection. The Defense Security Executive also directs the DoD Component Heads to ensure that DoD personnel who prepare draft classification guidance conduct adequate research on existing guidance before submitting new SCGs for OCA approval. The memorandum states that any OCA who is notified of possible conflicts in classification guidance should take prompt corrective action, report such action, and provide all documentation pertaining to the conflicts to their security manager. The prompt reporting of classification conflicts will enable DoD Component security managers to discuss those conflicts with the Office of the USD(I&S) as part of their annual self-inspection.

Our Response

Comments from the Deputy Director did not address the specifics of Recommendations 1.a. and 1.c.; therefore, those recommendations are unresolved. During the audit, the USD(I&S) provided the audit team with a copy of the Defense Security Executive's memorandum, and while it addressed SCG development

[11] USD(I&S) Memorandum, "Security Classification Policy And Enhanced Oversight Requirements," July 26, 2021. The Director for Defense Intelligence, Counterintelligence, Law Enforcement, and Security serves as the Defense Security Executive.

and maintenance, the memorandum generally reiterated existing guidance in DoD Manual 5200.01, Volume 1, and DoD Manual 5200.45. The memorandum did not include a requirement for the DoD Component Heads to account for all SCGs under their purview (Recommendation 1.a.) to ensure that any SCGs missing from the SCG index are identified and forwarded to the DTIC. The memorandum also did not establish a process to ensure that the DoD Components, OCAs, and the DTIC comply with the existing guidance now and in the future (Recommendation 1.c.). Therefore, we request that the Deputy Director provide additional comments to the final report stating how she will ensure that all SCGs are accounted for and that a process is established to ensure compliance with the DoD Manual 5200.01, Volume 1, and DoD Manual 5200.45.

Although the Deputy Director did not agree or disagree with Recommendation 1.b., USD(I&S) actions taken and planned in response to Recommendation 3 to ensure that all SCGs are reviewed and updated as necessary by September 2, 2022, and every 5 years afterwards meets the intent of the recommendation. Therefore, we consider Recommendation 1.b. closed and no further action is required.

Recommendation 2

We recommend that the Defense Technical Information Center Administrator, in coordination with the Under Secretary of Defense for Intelligence and Security, establish business rules for the security classification guide index, including a security classification guide naming, numbering, and formatting convention that will facilitate original classification authority searches of existing classification guidance to enable consistent classification of similar information throughout the DoD.

Defense Technical Information Center Comments

The DTIC Administrator disagreed with the recommendation, stating that the proposed solution fails to address the issues identified in the report, which were inconsistent SCG titles, and duplicate and missing SCGs. The Administrator stated that establishing complex business rules would not guarantee a complete, accurate, and easily searchable SCG index, but would instead increase opportunities for error, making SCG retrieval more difficult. The Administrator added that the DTIC modified its SCG standard operating procedures to include quality control measures to ensure that the SCG index titles mirror, verbatim, the actual SCG titles, and removed and resolved all duplicate SCGs.

Our Response

Comments from the Administrator did not address the specifics of the recommendation; therefore, the recommendation is unresolved. Step 1 of the SCG development process requires OCAs to identify and review existing classification guidance to avoid conflicts between SCGs. A naming, numbering, and formatting convention for SCGs will facilitate OCA searches of the index and improve the OCAs' ability to complete Step 1. We do not consider a naming, numbering, and formatting convention as a set of "complex business rules," but instead necessary action to reduce classification conflicts, eliminate duplicate SCG index entries, and promote SCG update notification. Furthermore, this recommendation was not intended to address the SCGs missing from the index, because DoD Manual 5200.01, Volume 1 and DoD Manual 5200.45 clearly state that the OCAs are responsible for providing a copy of each approved SCG to the DTIC upon issuance. Recommendation 1.a., addresses OCA compliance with that guidance.

Modifying DTIC internal procedures to require that SCG index titles match the actual SCG title is a good first step, but it does not ensure that the SCG title fully reflects the contents of the SCG and that the OCA can identify related guidance. We recommended that the DTIC Administrator establish the business rules **in coordination with the USD(I&S)** [emphasis added] to ensure an enterprise solution for naming, numbering, and formatting SCGs throughout the DoD. Therefore, we request that the DTIC Administrator provide comments to the final report stating how he will coordinate with the USD(I&S) to establish business rules for the security classification guide index, including a security classification guide naming, numbering, and formatting convention that will facilitate OCA searches of existing classification guidance.

Recommendation 3

We recommend that the Under Secretary of Defense for Intelligence and Security, in coordination with the Under Secretary of Defense for Research and Engineering, direct the Defense Technical Information Center to re-establish the 5-year reminder process to ensure that original classification authorities review and update security classification guides as required.

Undersecretary of Defense for Intelligence and Security Comments

The Deputy Director for Defense Intelligence, Counterintelligence, Law Enforcement, and Security, responding for the USD(I&S), did not agree or disagree with the recommendation, stating that USD(I&S) guidance aligns with the Fundamental Classification Guidance Review (FCGR) in Executive Order 13526, which requires that SCGs be reviewed and updated every 5 years. The Deputy Director stated

that DoD Components were tasked to initiate an FCGR on February 1, 2022; submit status reports to the USD(I&S) on April 29, 2022, and July 29, 2022; and submit a final report, including an updated listing of SCGs, by September 2, 2022. The Deputy Director added that because the FCGR review is required every 5 years, the DTIC 5-year reminder process might be duplicative.

Defense Technical Information Center Comments

Although not required to comment, the DTIC Administrator agreed with the recommendation, stating that the DTIC developed a standard operating procedure to remind OCAs of their 5-year SCG review and update requirement.

Our Response

Although the Deputy Director did not agree or disagree with the recommendation, DoD Component actions taken in conjunction with the FCGR meet the intent of the recommendation. However, the Deputy Director, in coordination with the Under Secretary of Defense for Research and Engineering, should determine whether DoD guidance should be revised to acknowledge the FCGR requirement and whether that requirement makes the DTIC reminder process unnecessary. Because DoD actions to meet the FCGR address the specifics of the recommendation, the recommendation is resolved but will remain open. We will close the recommendation once the USD(I&S) provides documentation verifying the FCGR is complete and indicating that DoD guidance was revised, if necessary, to adjust the DTIC's role in the reminder process.

Appendix A

Scope and Methodology

We conducted this performance audit from August 2020 through February 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We obtained a list of SCGs from the DTIC and a list from the Office of the USD(I&S). In addition, we requested that DoD Components provide a universe of their SCGs. We compared the list provided by the DTIC against the individual SCGs provided by DoD Components to identify inconsistencies and develop a universe of SCGs. To conduct the audit, we used the USD(I&S) list, which as of August 28, 2020, included 1,501 SCGs. We did not use the list provided by the DTIC because, as stated in this report, we determined that the DTIC list was inaccurate and incomplete.

In coordination with the DoD OIG Quantitative Methods Division, we selected a statistical sample of 43 SCGs to review from the universe of 1,501 SCGs. We used the statistical sample to project the number of SCGs containing errors as well as the number of missing SCGs. We also nonstatistically selected for review an additional seven SCGs that we had used in prior audits or that had known problems, such as incorrect classification of ordnance-related information and conflicts with other ordnance-related SCGs.

To understand the process used to develop, maintain, and cancel SCGs, we interviewed DoD officials from the following organizations.

- Office of the USD(I&S), Counterintelligence, Law Enforcement, and Security
- DTIC
- Department of the Air Force Policy and Oversight Division
- Department of the Army Information Security and Policy Division
- Department of the Navy Program Protection Branch
- Air Force Materiel Command
- Air Force Life Cyber Management Center
- Air Force Military Satellite Communications Directorate
- Air Force Nuclear Weapons Center
- Navy Sea Systems Command

- Defense Office of Prepublication and Security Review
- Information Security Oversight Office
- USEUCOM Information Security Branch
- USCYBERCOM Information Management Defense Office
- DARPA
- SCO Security and Program Protection
- MDA Information Security Information Safeguards
- TRMC
- USINDOPACOM
- Joint Staff Information Security Branch

In addition, we reviewed Federal laws and DoD policies, including Army, Navy, and Air Force guidance, to identify specific requirements for developing, maintaining, and canceling SCGs.

To determine whether DoD Components developed, maintained, and canceled SCGs in accordance with Federal and DoD guidance, we:

- determined whether OCAs followed the steps when developing the SCGs;
- reviewed SCGs to identify the process DoD officials followed when identifying information that must be protected;
- determined whether OCAs reviewed and updated SCGs at least once every 5 years to promote uniformity and consistency and avoid classification conflicts between SCGs; and
- determined whether the OCAs completed the classification training from FY 2016 through FY 2020.

Internal Control Assessment and Compliance

We assessed internal controls and compliance with laws and regulations necessary to satisfy the audit objective. In particular, we reviewed and assessed internal controls related to DoD processes at the Office of the USD(I&S) level and below for SCGs. This includes policy and procedures in place, oversight, and accountability for SCGs. However, because our review was limited to those internal controls and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

Use of Computer-Processed Data

We obtained a list of SCGs from the Office of the USD(I&S) and the DTIC to determine the total number of SCGs across the DoD. We compared those lists and determined that the DTIC list was inaccurate and incomplete because it contained duplicates and was missing SCGs included on the USD(I&S) list. We also discussed both lists with officials from the Office of the USD(I&S) and the DTIC and further assessed the reliability of the USD(I&S) list through discussions with DoD Component officials. We determined that the USD(I&S) list of SCGs was reliable to select a statistical sample of SCGs to review during the audit.

Use of Technical Assistance

The DoD OIG Quantitative Methods Division provided assistance in developing a statistical simple random sampling methodology that we used to select 43 SCGs from a universe of 1,501 SCGs for inclusion in the audit scope. We used a 90-percent confidence level and 7.5 percent precision to determine the sample size. We used the sample to project the number of SCGs containing errors within the 1,501 SCG universe. See Appendix C for the statistical sample plan and projections.

Prior Coverage

During the last 5 years, the DoD OIG issued three reports that included discussion on SCGs and classification problems associated with those SCGs. Unrestricted DoD OIG reports can be accessed at http://www.dodig.mil/reports.html/.

DoD OIG

Report No. DODIG-2020-101, "Naval Ordnance Data Classification Issues Identified During the Oversight of the U.S. Navy General Fund Financial Statement Audit for FY 2020," July 2, 2020

> During the FY 2018, 2019, and 2020 Financial Statement Audits of the Navy General Fund, the DoD OIG determined that the Navy and Marine Corps classified and handled ordnance information inconsistently. In addition, the Navy and Marine Corps did not properly classify and mark ordnance documents in accordance with DoD policy. Furthermore, the Navy did not prevent conflicts between the "Navy Inventory Management" SCG and specific ordnance SCG requirements.

Report No. DODIG-2020-098, "Audit of Governance and Protection of Department of Defense Artificial Intelligence Data and Technology," June 29, 2020

The DoD OIG determined that the Joint Artificial Intelligence Center needed to develop an SCG to help DoD Components identify sensitive and classified information, and apply the appropriate security markings to ensure that information used to support artificial intelligence projects was properly protected.

Report No. DODIG-2017-028, "Follow up to DoD Evaluation of Over-Classification of National Security Information," December 1, 2016

The DoD OIG determined that the agreed-upon recommendations made in Report No. DODIG-2013-142, "DoD Evaluation of Over-Classification of National Security Information," September 30, 2013, were implemented. In response to the DoD OIG recommendations, the Defense Security Service Center for Development of Security Excellence increased delivery methods for security training courses and additional course offerings tailored to original and derivative classifiers.

In addition, the USD(I&S) directed Component reviews of OCA positions to ensure that those positions were needed. Furthermore, the USD(I&S) required DoD officials to review and submit SCGs to the DTIC in a timely manner along with a completed DD Form 2024 signed by an OCA, to improve accountability over the process.

Appendix B

SCGs Reviewed

Table 6 lists the 50 SCGs we reviewed. We assigned each SCG a number for ease of reference throughout the report.

Table 6. SCGs Reviewed by DoD Component

SCG #	DoD Component	SCG Title
1	Army	Cerberus-Lite Scout Portable Surveillance System
2	Army	Cartridge, 140-mm: High Explosive, Multipurpose with Tracer, XM 965
3	Army	Armored Multi-Purpose Vehicle
4	Army	Hostile Fire Indication and Visual Acquisition Disruption
5	Army	Joint Service Transportable Decontamination System Small Scale, Phase II
6	Army	Biometrics Collection Capability
7	Army	Foreign Material Program
8	Army	Voice Identity Biometric Exploitation Services
9	Army	Small Satellite
10	Army	Rhino Explosive Hazard Pre-Detonation System
11	Army	Joint Multi-Platform Advanced Combat Identification
12	Army	Contingency Expeditionary Force
13	Army	Joint Air-to-Ground Missile
14	Navy	Decoy, Shipboard Ordnance Infrared
15	Navy	Explosive Ordnance Disposal, NonNuclear
16	Navy	Inventory Management Data, Conventional Naval Ordnance (Except Chemical/Biological) and Research, Development, Training & Evaluation (RDT&E) Dollar Amounts
17	Navy	Landing Craft, Air Cushion
18	Navy	Dry Deck Shelter
19	Navy	Navy Airborne Electronic Jammer Technique Optimization
20	Navy	Department of Energy-DoD Classification Guide for the Naval Nuclear Propulsion Program
21	Navy	Acoustic Vector Sensor & Array Technology and Systems
22	Navy	Supercavitating High Speed Bodies Technology
23	Navy	Torpedoes (MK 37, 44, 45, and Freedom)
24	Navy	Non-Nuclear Warhead Development, Advanced

Table 6. SCGs Reviewed by DoD Component (cont'd)

SCG #	DoD Component	SCG Title
25	Navy	Fleet Combat Support Helicopter MH-60S
26	Navy	AN/AQS-20A Sonar, Mine Detecting Set
27	Navy	Rocket Propulsion Technology
28	Navy	Multi-Function Mast (OE-538) Antenna System
29	Air Force	Operationally Responsive Space-2
30	Air Force	Automated Navigation and Guidance Experiment for Local Space
31	Air Force	Aerospace Vehicle Equipment Increment 1 Program
32	Air Force	Intercontinental Ballistic Missile
33	Air Force	Single Channel Transponder System
34	Air Force	Neptune Eagle
35	USCYBERCOM	United States Cyber Command Instruction 5200-03
36	USEUCOM	Austere Challenge 2021
37	USINDOPACOM	United States Forces Korea SCG
38	USSOCOM	Sensitive Financial Operations
39	USSOCOM	Identity Management
40	USSOCOM	Army Special Operations Aviation Rotary Wing Program
41	USD(A&S)	Acquisition and Sustainment SCG
42	USD(I&S)	Financial Management for Sensitive Activities
43	DARPA	Lorentz Force Orbitology Study
44	DARPA	Upward Falling Payloads
45	DARPA	Siren Study Project
46	DARPA	Ultrashort Pulse Laser
47	MDA	Combined Optical Measurements Experimentation Test
48	SCO	Program Specific Protection Plan for LiTE Saber
49	SCO	Program Specific Protection Plan for Vanguard
50	TRMC	National Cyber Range

Source: The DoD OIG.

Appendix C

Statistical Sample

Population:
The population consisted of 1,501 SCGs obtained from the Office of the USD(I&S).

Parameters:
We used a 90-percent confidence level and 7.5-percent precision to calculate a sample size of 43 for a simple random sample.

Sample Plan:
We used the RAND() function in Microsoft Excel to randomize the population, from which the sample of 43 SCGs were selected without replacement.

ANALYSIS AND INTERPRETATION

Fieldwork Results:
We analyzed the 43 SCGs in the sample and found that 36 of them were not developed and maintained in accordance with Federal and DoD guidance. Furthermore, there were three SCGs in the sample that OCAs were unable to locate and four that were not properly canceled.

Statistical Projection and Interpretation:
We calculated the following statistical projections to the overall universe with a 90-percent confidence level.

Table 7. SCGs Not Developed and Maintained in Accordance With Federal and DoD guidance

SCGS Not Developed and Maintained in Accordance With DoD Guidance	Lower Bound	Point Estimate	Upper Bound
Rate (Percent)	73.3	83.7	94.1
Number	1,101	1,257	1,413

Source: The DoD OIG.

We project with a 90-percent confidence level that the percentage of SCGs that were not developed and maintained in accordance with Federal and DoD guidance is between 73.3 percent and 94.1 percent, with a point estimate of 83.7 percent. The corresponding number of SCGs that were not developed and maintained in accordance with DoD guidance is between 1,101 and 1,413, with a point estimate of 1,257.

Table 8. SCGs That OCAs Were Not Able To Locate

SCGs That OCAs Were Not Able To Locate	Lower Bound	Point Estimate	Upper Bound
Rate (Percent)	0.0	7.0	14.5
Number	3	105	218

Source: The DoD OIG.

We project with a 90-percent confidence level that the percentage of SCGs that OCAs were not able to locate is between 0.0 percent and 14.5 percent, with a point estimate of 7.0 percent. The corresponding number of SCGs that OCAs were not able to locate is between 3 and 218, with a point estimate of 105.

Table 9. SCGs Not Properly Canceled

SCGS Not Properly Canceled	Lower Bound	Point Estimate	Upper Bound
Rate (Percent)	0.9	9.3	17.7
Number	13	139	266

Source: The DoD OIG.

We project with a 90-percent confidence level that the percentage of SCGs that were not properly canceled is between 0.9 percent and 17.7 percent, with a point estimate of 9.3 percent. The corresponding number of SCGs that were not properly canceled is between 13 and 266, with a point estimate of 139.

Management Comments

USD(I&S)

INTELLIGENCE
AND SECURITY

OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

April 25, 2022

MEMORANDUM FOR OFFICE OF THE DOD INSPECTOR GENERAL

SUBJECT: DoD OIG Draft Report, "Audit of the Development and Maintenance of Department of Defense Security Classification Guides," Project No. D2020-D000CX-166.000 (February 28, 2022).

References: (a) DoDM 5200.01 Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," incorporating Change 2, July 28, 2020.
(b) DoDM 5200.45, "Instructions for Developing Security Classification Guides," incorporating Change 2, September 15, 2020.

Thank you for the opportunity to review and provide comments on the subject draft report. Security Classification Guides (SCG) are the primary tool to establish and convey Original Classification Authority (OCA) direction and assist personnel regarding consistent derivative classification. I am responding on behalf of the Under Secretary of Defense for Intelligence and Security (USD(I&S)).

The subject report offers a revealing look at a priority item for the Defense Security Enterprise (DSE). The FY2021-2025 DSE Strategy includes a call for Components to support appropriate investment of Defense spending, informed by risk and credible research. Given OIG's research, it would be both instructive and supportive of the DSE Strategy for DoD OIG to recommend Components elevate security within their funding prioritization and that the Director, Cost Assessment and Program Evaluation provide an independent assessment of how effectively Components are integrating security into their programming requests.

The subject draft report claims DoD Components did not develop and maintain SCGs in accordance with Federal and DoD guidance because the Under Secretary of Defense for Intelligence and Security did not direct, administer, and oversee the DoD process for developing and maintaining SCGs, as required by References (a) and (b). If OIG intended to assess that the USD(I&S) did not *sufficiently* direct, administer, and oversee this responsibility, I would again point to the responsibilities of Components to execute and sufficiently resource requirements. As it relates to the continual balancing between oversight and management, the DSE strives to balance centralized policy frameworks with de-centralized implementation. Whether the Department's challenges are attributed to Component-level under-resourcing, competing priorities, or inattentiveness, our primary challenge is not a policy gap, but a compliance gap.

While the possibility of the DoD OIG-predicated population error rate of 84 percent concerns me, this assumes the error rate in the SCG population remains constant with the three percent sample size selected by the audit team. Acknowledging the possibility an appropriate size would be substantially larger given the population number, it would be very instructive to know the statistical significance of the current sample, as well as any other mathematical formulas used by the OIG to arrive at this considerable judgement.

USD(I&S) (cont'd)

I&S-issued policy requires SCGs to be updated every five years, which is consistent with FCGR guidance in Executive Order 13526. The FCGR ensures all SCGs are reviewed, updated, and cancelled as necessary and appropriate. This process is initiated across the Executive Branch by the Information Security Oversight Office (ISOO) and the Department is executing that review at the request of my office. Given that ISOO tasks the FCGR to the Agencies every five years, Defense Information Technical Center reminders may be duplicative. Of note, DoD Components were directed to complete the Fundamental Classification Guidance Review (FCGR) issued on February 1, 2022, and documentation is attached for reference.

Omitted because of length. Copies provided upon request.

On July 26, 2021, the Defense Security Executive issued the attached "Security Classification Policy and Enhanced Oversight Requirements" memorandum, a copy of which was forwarded to your office on July 27, 2021. We believe this is relevant to your research and the findings of this report, and request it be included.

Omitted because of length. Copies provided upon request.

Please consider the comments and suggested edits from my office and OGC included in the attached version of the draft report. My point of contact for information security policy matters is [redacted]

Tara L. Jones
Deputy Director for Defense Intelligence
Counterintelligence, Law Enforcement,
& Security

Attachments:
As stated

DTIC

DEFENSE TECHNICAL INFORMATION CENTER
8725 JOHN J. KINGMAN ROAD
FORT BELVOIR, VIRGINIA 22060-6218

IN REPLY REFER TO: DTIC-D

MEMORANDUM FOR Inspector General, Department of Defense, 4800 Mark Center Drive, Alexandria, Virginia 22350-1500

Subject: DTIC Response to "Audit of the Development and Maintenance of Department of Defense Security Classification Guides (Project No. D2020-D000CX-0166.000)"

DTIC appreciates the opportunity to review and comment on the draft DoD Inspector General report entitled, "Audit of the Development and Maintenance of Department of Defense Security Classification Guides (Project No. D2020-D000CX-0166.000)," dated February 28, 2022. DTIC also thanks the IG team for its professionalism and collegiality during the audit process to improve community access to security classification guides (SCGs). This document details DTIC's response to the IG's findings and recommendations, specifically Recommendation 2 and Recommendation 3.

Recommendation 2

We recommend that the Defense Technical Information Center Administrator, in coordination with the Under Secretary of Defense for Intelligence and Security, establish business rules for the security classification guide index, including a security classification guide naming, numbering, and formatting convention that will facilitate original classification authority searches of existing classification guidance to enable consistent classification of similar information throughout the DoD.

DTIC's Position Re: RECOMMENDATION 2. NON-CONCUR.

The SCGs audit revealed the following issues: inconsistency between actual SCG Title and the DTIC Index of SCG Titles (hereinafter DTIC Index), duplicate SCGs, and missing SCGs. The proposed solution, establishment of complex business rules, fails to address the issues identified, one of quality control across the community process. Rather than guarantee a complete, accurate, and easily searchable DTIC Index, the proposed solution increases opportunities for error, potentially making retrieval of SCGs by users more difficult, not less. Finally, the proposed solution would not have prevented and will not prevent duplicate or missing SCGs. We have taken positive action to add layers of quality control that address both duplicate and misnamed SCGs. DTIC does not have visibility of unsubmitted SCGs.

DTIC (cont'd)

In response to the audit, DTIC: modified its SCG's standard operating procedures, creating quality control measures to ensure that all DTIC Index titles mirror, verbatim, the actual SCG titles; removed and resolved all "duplicate" SCG issues; and has taken positive action to address those SCGs that were not included in the DTIC SCG index but should have been.

Recommendation 3

We recommend that the Under Secretary of Defense for Intelligence and Security, in coordination with the Under Secretary of Defense for Research and Engineering, direct the Defense Technical Information Center to re-establish the 5-year reminder process to ensure that original classification authorities review and update security classification guides as required.

DTIC's Position Re: RECOMMENDATION 3. CONCUR.

DTIC acknowledges and accepts its current obligation under DoD Manual 5200.01, Volume 1, February 24, 2012, Incorporating Change 2, July 28, 2020, encl.6, para. 8 ("DTIC will send reminders to organizations as security classification guides near their 5-year required reviews."). DTIC has developed a standard operating procedure to timely remind Original Classification Authorities (OCAs), at the organizational level, of their quinquennial (every 5 years) review and update requirement.

DTIC continuously endeavors to provide the highest quality of service and support to those within the DoD as well as our non-DoD customers. DTIC remains available to discuss the best path to ensure the effective and efficient search for and retrieval of SCGs.

Point of contact for this action is [redacted]

THOMAS.CHRIS
TOPHER.E.[redacted]

Christopher E. Thomas
Administrator

DTIC Response to IG SCG Audit (Project No. D2020-D000CX-0166.000) 2

Acronyms and Abbreviations

DARPA	Defense Advanced Research Projects Agency
DTIC	Defense Technical Information Center
FCGR	Fundamental Classification Guidance Review
MDA	Missile Defense Agency
OCA	Original Classification Authority
SCG	Security Classification Guide
SCO	Strategic Capabilities Office
TRMC	Test Resource Management Center
USCYBERCOM	U.S. Cyber Command
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USEUCOM	U.S. European Command
USINDOPACOM	U.S. Indo-Pacific Command
USSOCOM	U.S. Special Operations Command

Glossary

CONFIDENTIAL. The level of classification for information that could cause damage to national security, if compromised.

Derivative Classification. The process of incorporating, paraphrasing, restating, or generating, in new form, information that is already classified and marking the newly developed material consistent with the classification markings in classification guidance.

Duration of Classification. Information that identifies the specific date or events for downgrading or declassifying information included in an SCG.

Internal Controls. Processes that provide reasonable assurance that programs are operating as intended and are used to evaluate the effectiveness of the controls.

Level of Classification. Information that identifies whether the information is TOP SECRET, SECRET, or CONFIDENTIAL.

National Advantage. The benefits, direct and indirect, accruing or expected to accrue to the United States based on classifying information.

Original Classification Authority (OCA). An individual authorized in writing, either by the President, Vice President, or an agency head, to classify sensitive information in the first instance and is responsible for developing and maintaining the accuracy of SCGs.

SECRET. The level of classification for information that could cause serious damage to national security, if compromised.

Security Classification Guide (SCG). Document that identifies the classification of a system, plan, program, project, or mission, including the level and duration of classification.

TOP SECRET. The level of classification for information that could cause exceptionally grave damage to national security, if compromised.


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Whistleblower Protection
U.S. Department of Defense

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible fraud, waste, and abuse in Government programs. For more information, please visit the Whistleblower webpage at http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whisteblower-Reprisal/ or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

For more information about DoD OIG reports or activities, please contact us:

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098