Description of document:	Department of Agriculture (USDA) Security Classification Guide 2018
Requested date:	23-May-2024
Release date:	21-August-2024
Posted date:	02-September-2024
Source of document:	FOIA Request United States Dept of Agriculture Office of Information Affairs 1400 Independence Avenue SW Room 4039-A Washington, DC 20250-0706 Email: USDAFOIA@usda.gov USDA Public Access Link (PAL) FOIA.GOV

New Version For Signature

CONTROLLED

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

All individuals handling this information are required to protect it from unauthorized disclosure.

Handling, storage, reproduction, and disposition of the attached document(s) must be in accordance with 32 CFR Part 2002 and applicable agency policy.

Access to and dissemination of CUI shall be allowed as necessary and permissible to any individual(s), organization(s), or grouping(s) of users, provided such access or dissemination is consistent with or in furtherance of a Lawful Government Purpose and in a manner consistent with applicable law, regulations, and Government-wide policies.

901-101
NSN-7540-01-633-7021

OPTIONAL FORM 901 (06-14)
Prescribed by GSA/ISOO | 32 CFR 2002

CONTROLLED

U.S. DEPARTMENT OF AGRICULTURE

SECURITY CLASSIFICATION GUIDE

Issued and Approved by the Secretary of Agriculture:

Sonny Perdue
Sonny Perdue

June 6, 2018
Date

Table of Contents

I. GENERAL INFORMATION

A. BACKGROUND

The U.S. Department of Agriculture (USDA), Departmental Regulation (DR) 3440-001, *USDA Classified National Security Information Regulation* and Departmental Manual (DM) 3440-001, *USDA Classified National Security Information Program Manual* provides for the issuance of a Security Classification Guide (SCG) for programs, projects, and research involving classified information. Executive Order (E.O.) 13526 *Classified National Security Information* addresses the need for SCGs in terms of proper classification of information and uniform derivative classification of information. Specific classification guidance is necessary for effective information security and is instrumental in the allocation of resources for protecting only those items that affect national security. A SCG is a written record of original classification decisions or a series of decisions regarding a system, plan, program, project, or research. This SCG also includes declassification guidance.

Specific and detailed guidance is required when identifying information that must be classified to ensure that information is not over classified or under classified, but classified at the appropriate level. Over classification is costly and inefficient and can hinder innovation and delay operations. Under classification can result in compromise, inadvertent disclosures, and/or confusion. In addition to proper identification of items to be classified, the SCG must identify the length of time the information should remain classified.

The USDA classification guide is a tool for USDA employees and contractors on the proper and uniform derivative classification of information within USDA. This SCG was developed in close coordination with USDA agencies, as well as with the U.S. Department of Health and Human Services and the U.S. Department of Homeland Security. Employees and contractors who are approved to apply derivative classification markings are required to receive training in the mechanics of derivative classification and are limited to the level of classified information to which they are authorized access. All derivative classification actions within USDA should be accomplished by referring to the most recently approved SCG, or using one or more existing current classified source documents, or information received during classified conversations or classified meetings.

Information may be classified only if its unauthorized disclosure could reasonably be expected to result in damage to national security and the Original Classification Authority (OCA) identifies or describes the damage. By definition, the national security is the national defense or foreign relations of the United States.

Classified National Security Information (CNSI) may only be prepared and processed on equipment specifically approved for classified word processing and printing and located in an accredited Secure Working Area. Additionally, derivative classifiers must have the

2024-DA-04836-F

capability to securely store classified information as prescribed in the Title 32 Code of Federal Regulations (CFR) 2001.43 and DM 3440-001.

B. PURPOSE

Classification is necessary so that USDA agencies and staff offices may construct products and periodically update these products which may identify specific components, agents, and process combinations that pose national security risks. That information could be used by a terrorist as a blueprint for attacking the food and agriculture sector.

C. AUTHORITY

DR 3440-001 is the authority that governs the control and issuance of this SCG. This SCG provides authority to cite as classification, declassification, or downgrading actions only in USDA endeavors. If there are any changes to security classification by applying this SCG, they are to be made immediately by the Senior Agency Official (SAO). Finally, E.O. 13526 and 32 CFR 2001.15 state that the OCA be identified by name and position, or personal identifier. The Secretary of Agriculture maintains the authority to originally classify information up to "Secret" through Executive Order 12958 dated September 26, 2002. This authority was reiterated on December 29, 2009, pursuant to Section 1.3 of E.O. 13526. OCA cannot be delegated.

D. OFFICE OF PRIMARY RESPONSIBILITY

The Secretary designated the Assistant Secretary for Administration (ASA) as the SAO responsible for the development and administration of the Classified National Security Information Program (CNSIP). The ASA re-delegated the responsibilities for USDA's CNSI to the Director of the Office of Homeland Security (OHS). The Personnel and Document Security Division (PDSD) of OHS is responsible for the day-to-day operations of the USDA CNSIP. All inquiries and questions regarding this SCG or classification/declassification of information should be directed to PDSD at (202) 720-7373 or via email at PDSD@DM.USDA.gov.

E. CLASSIFICATION CHALLENGES

In accordance with DM 3440-001, classification challenges shall be submitted to PDSD for coordination. A formal challenge must be submitted in writing but need not be any more specific than to question why information is or is not classified, or is classified at a certain level. Information being challenged for classification shall remain classified and protected at its marked level until a final decision is made to declassify it.

F. REPRODUCTION, EXTRACTION AND DISSEMINATION

The USDA SCG can be reproduced and disseminated to those organizations that support USDA efforts to include industry.

G. PUBLIC RELEASE

Public release of the SCG shall be coordinated through PDSD.

H. UPDATING THE SECURITY CLASSIFICATION GUIDE

DR 3440-001 requires that the SCG be reviewed every five (5) years or upon regulatory changes. The SCG updates will be coordinated with Subject Matter Experts (SMEs) and users of the guide.

II. CLASSIFICATION INSTRUCTIONS

A. CATEGORIES OF CLASSIFIABLE INFORMATION

Information shall not be considered for classification unless the unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to national security in accordance with section 1.1(4) of E.O. 13526 and pertains to one or more of the following categories:

- a.) Military plans, weapons systems, or operations;
- b.) Foreign government information;
- c.) Intelligence activities (including covert action), intelligence sources or methods, or cryptology (see note);
- d.) Foreign relations or foreign activities of the United States, including confidential sources;
- e.) Scientific, technological, or economic matters relating to the national security;
- f.) United States Government programs for safeguarding nuclear materials of facilities;
- g.) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection service relating to the national security; or
- h.) The development, production, or use of weapons of mass destruction.

Note: Before documents are derivatively classified using sources outlined in section 1.4(c), consult with the Special Security Officer (SSO) in PDSD.

B. DERIVATIVE CLASSIFICATION

Persons who incorporate, paraphrase, restate, or generate in new form information that is already classified, or who apply classification markings derived from source material or as directed by a SCG, need not possess OCA. The person(s) who apply derivative classification marking shall:

- a.) Be identified by name and position, or by personal identifier, in a manner that is immediately apparent for each derivative classification action;
- b.) Ensure the date of origin of the derivative document is immediately apparent;
- c.) Observe and respect an original classification decision; and
- d.) Carry forward to any newly created documents the pertinent classification marking. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward:

  1. The date or event for declassification that corresponds to the longest period of classification among the sources, or the marking established pursuant to section 1.6(a)(4)(D) of E.O. 13526; and
  2. A listing of the source materials.

Persons who apply derivative classification markings shall receive training in the proper application of derivative classification at least once every two (2) years. Derivative classifiers who do not receive such training at least once every two (2) years shall have their authority to apply derivative classification markings suspended until they have received such training.

A waiver may be granted by the OHS Director if an individual is unable to receive such training due to unavoidable circumstances. Whenever a waiver is granted, the individual shall receive such training as soon as practicable.

All documents created using derivative classification must contain information in the format indicated below:

<div align="center">

Sample Derivative Classification Block
(Declassification Instructions)

Single source document:
</div>

Classified by:	Name and position or personal identifier.
Derived from:	Source and date of source document.
Declassify on:	Repeat declassification date/event from source.

<div align="center">

Multiple source documents
(sources must be included at the end of the document or using footnotes):
</div>

Classified by:	Name and position or personal identifier.
Derived from:	Multiple sources.
Declassify on:	Use declassification date/event furthest into future from among sources.

When classifying information derived from a SCG, utilize this format below:

<div align="center">

Classification guide as source document:
</div>

Classified by:	Name and position or personal identifier.
Derived from:	USDA SCG (date of SCG).
Declassify:	Date/event prescribed by SCG.

C. INTERIM CLASSIFICATION:

When a USDA employee or government contractor who does not have OCA (i.e., anyone other than the Secretary) originates information believed to require classification, the information shall be protected as classified information. The information should be marked "Secret-Currently Under Classification Review." The markings should be located at the top and bottom of each page and on each paragraph containing the potentially classified information. The document or information must be forwarded to PDSD for further evaluation by SMEs and classification experts, who will provide a recommendation to the Secretary. As soon as possible, authors must notify the SSO for coordination.

<div align="center">

7
</div>

D. COMPILATION OF INFORMATION

Information that individually is unclassified at a lower level, may become classified or classified at a higher level when aggregated or compiled in a single document, if the compiled information reveals an additional association or relationship that meets the standards for classification under E.O. 13526, and is not otherwise revealed in the individual data items. When a classification determination is made based on compilation, clear instructions must appear with the compiled information as to the circumstances under which the individual portions constitute a classified compilation, and when they do not.

E. INFORMATION SHARING AND DISSEMINATION

The Office of the Director of National Intelligence has emphasized the need to ensure timely and efficient flow of information to our closest allies. Accordingly, the use of restrictive markings (i.e. Not Releasable to Foreign National (NOFORN) and Originator Controlled (ORCON)) should be the exception rather than the rule. The presumption of disclosure and release should be the primary consideration in the preparation and dissemination of classified information.

Anyone with a desire to share classified information with a non-U.S. entity or person must contact PDSD for instructions and coordination with the appropriate authority.

F. FOREIGN GOVERNMENT INFORMATION (FGI)

The unauthorized disclosure of FGI is presumed to cause damage to U.S. national security. It thus requires that FGI shall retain its original classification markings or shall be assigned a U.S. classification providing a degree of protection at least equivalent to that required by the entity that furnished the information. Whether the information retains its original markings or is brought into the U.S. classification system is based on the governing treaty or international agreement.

If the identity of the specific foreign government(s) providing the information must be concealed in a U.S. intelligence document, then the document's classification banner shall include the "FGI" marking without any specific country trigraphs, and pertinent information shall be portion marked "FGI" together with the classification level, for example "(//FGI C)." When this occurs, a separate record that identifies the foreign government shall be maintained by the document custodian in order to facilitate possible subsequent declassification actions.

If the identity of the specific foreign government(s) providing the information does not have to be concealed in a U.S. document, then the document's classification banner shall include the "FGI" marking with the specific country trigraphs, and pertinent information shall be portion marked with the country of origin and the classification level, for example "(//GBR S)."

Please contact PDSD for more information on FGI.

G. CONTROLLED UNCLASSIFIED INFORMTION (CUI)

CUI is not a classification. CUI is protected under existing laws, regulations, or government wide policy. CUI records are unclassified official information which may be exempt from public release under one or more of the exemption categories of the Freedom of Information Act (FOIA), 5 U.S.C. 552. The fact that information is marked CUI is not a basis for denying information requested under FOIA. The inverse is also true – the fact that information is not marked CUI does not mean it can be released. All information required must be reviewed for its current status under the FOIA at the time of request. Denial of a request is based upon the fact that the information falls under one or more of the exemptions authorized under the FOIA and some significant and legitimate purpose is being served by withholding the information. "Significant and legitimate" means that it would jeopardize some program or system.

CUI includes, but is not limited to Privacy, Tax, Law Enforcement, Critical Infrastructure, Export Control Financial, Intelligence, Procurement and Acquisition and Legal. The loss or improper safeguarding of CUI could be expected to have a serious adverse effect on USDA operations, assets, or employee. Significant degradation in mission capability to an extent and duration that the USDA is able to perform its primary functions, but the effectiveness of the functions is significantly reduced.

CUI information must be marked as such on the top and bottom of each cover page (if any), the first page, and each interior page. Mark pages of unclassified documents that contain CUI, "CONTROLLED," on the top and bottom of every page. Classification marking takes precedence when a page or portion includes both classified information and CUI information.

Mark portions of a classified document containing CUI information, but does not contain classified information, with the abbreviation (U//CUI).

H. DECLASSIFICATION AND DOWNGRADING

Information shall be declassified as soon as it no longer meets the standards for classification under E.O. 13526. Information shall be declassified or downgraded by:

a.) The official who authorized the original classification, if that official is still serving in the same position and has OCA;

b.) The originator's current successor in function, if that individual has OCA;

c.) A supervisory official of either the originator or his or her successor in function, if the supervisory official has OCA; or

d.) Officials delegated declassification authority in writing by the agency head or the SAO of the originating agency.

Request for mandatory review for declassification of information originally classified by USDA will be processed through OHS/PDSD. Request for mandatory review must be of sufficient specificity for USDA to locate the records containing the information. Request for broad types of information may be denied. Individuals who make a request under mandatory declassification review as well as the Freedom of Information Act (FOIA) must select one process or the other. Individuals who fail to make a selection will result in their request being processed under FOIA unless the requested material is only subject to the mandatory declassification review.

OHS will make a final determination on the review for declassification and provide the individual a response within one year from the date of receipt. An individual has 60 days from the date of denial to appeal to USDA appellate authority. A request for an appeal will be addressed to the Assistant Secretary for Administration and a final determination on the appeal will be made within 60 days following receipt of the appeal. The USDA appellate authority will notify the individual in writing of the final determination and their appeal rights to the Interagency Security Classification Appeals Panel.

III. CLASSIFICATION GUIDANCE

Pursuant to Section I(c) above, **USDA does not have the authority to classify information above the SECRET level**. For example, adversarial intent is deliberately omitted in the table below. An Intelligence Community (IC) or law enforcement SCG should be utilized since threat information (i.e., capability, likelihood, and intent) is provided by law enforcement and the IC. The same may be true for other information not covered in this guidance (e.g., complete risk profiles). Please contact PDSD for assistance.

A. SCIENCE AND TECHNOLOGY GUIDANCE

The philosophy behind this classification guidance is that general research shall remain unclassified. However, if USDA possesses unique and specific intelligence information or insight that could be exploited if revealed for the first time, particularly because they are validated by the U.S. Government, the following foundational guidance shall be used to protect that type of information or insight:

- Once gaps in planning are combined with limited or no known countermeasures, information becomes Unclassified//CUI.

- When discussing gaps, vulnerabilities, and/or consequences in a general manner, information shall remain Unclassified. When gaps, vulnerabilities and/or consequences are paired with specific scenario(s) with hypothetical actors, the information shall be Unclassified//CUI. The classification may increase if combined with threat information covered under another non-USDA SCG.

- If a specific actor and specific target are modeled and it results in the discovery of new vulnerabilities and gaps that could be expected to cause serious damage to the national security it will be classified SECRET. Furthermore, if any products or discussions include law enforcement or intelligence information, contact PDSD to confirm classification level or work with a partner with higher classification authority.

Item	Classification Level	Reason for Classification	Duration of Classification	Remarks
Characterization of material (e.g., phenotyping, genotyping, sequencing) isolated from animals and plants related to naturally occurring threats or emerging infectious diseases	Unclassified			
Preparedness, prevention, mitigation, response, and recovery plans/capabilities and associated gaps related to risks to the food and agriculture sector	Unclassified			At the Unclassified level, this includes items for which there are known countermeasures with appropriate capacity
Discussion of potential dual-use applications of current or emerging technologies in food and agriculture which are not paired with a known gap	Unclassified			Known gaps may include lack of surveillance, detection, or response capabilities or capacities; discussion of general consequences associated with applications are permitted per this SCG
General vulnerabilities pertaining to the use of emerging technologies (e.g., gene editing) to negatively target the food and agriculture sector	Unclassified			No mention of specific scenario discussion is permitted at the Unclassified level (e.g. limits on mapping all genetic material entering the United States)
General consequences pertaining to the use of emerging technologies (e.g., gene editing) to negatively target the food and agriculture sector	Unclassified			This may include items such as general economic, yield, or trade impacts

CONTROLLED

Item	Classification Level	Reason for Classification	Duration of Classification	Remarks
Discussion of gaps in preparedness, prevention, mitigation, response or recovery capabilities in the food and agriculture sector related to areas for which there is no known countermeasure or limited capacity to apply countermeasures	Unclassified//CUI			No mention of specific scenario discussion is permitted at the Unclassified//CUI level, e.g., using a particular agent to target a specific location/commodity by a specific actor to exploit a vulnerability in a certain way is considered SECRET
Detailed, scenario-based, specific actor(s) and specific agent discussion of security gaps in the food and agriculture sector related to areas for which there is no known countermeasure and inclusion of associated consequences.	SECRET	1.4 (e, g & h)	10 years	Includes details of how a technology may be applied to food and agriculture to exploit a vulnerability. Generalities may be discussed at the Unclassified/CUI level

13
CONTROLLED

CONTROLLED

Item	Classification Level	Reason for Classification	Duration of Classification	Remarks
Specific vulnerabilities resulting from a specific application of current or emerging technologies (e.g., gene editing) to negatively target the food and agriculture sector that may provide insight into U.S. Government detection or response capabilities.	SECRET	1.4 (e, g & h)	10 years	Vulnerabilities pertaining to the use of emerging technologies (e.g., gene editing) to target the food and agriculture sector; may include scenario-based discussion and/or discussions that reveal: - National security policy objectives - Specific targets - System capabilities - Strengths or weaknesses - Insight or methods for countering detection Generalities may be discussed at the unclassified level
Specific consequences pertaining to the use of emerging technologies (e.g., gene editing) to negatively target the food and agriculture sector that may provide insight into U.S. Government detection or response capabilities.	SECRET	1.4 (e, g & h)	10 years	Consequences pertaining to the use of emerging technologies (e.g., gene editing) to target the food and agriculture sector which reveals: - National security policy objectives - Specific targets - System capabilities - Strengths or weaknesses - Insight or methods for countering detection Generalities may be discussed at the unclassified level

14

CONTROLLED

Item	Classification Level	Reason for Classification	Duration of Classification	Remarks
Use of a specific <u>method</u> or <u>technology</u> to exploit a specific vulnerability and inclusion of associated consequences	SECRET	1.4 (e, g & h)	10 years	Includes details of how a technology may be applied to food and agriculture to exploit a vulnerability and exact damages

15

B. CARVER + SHOCK CLASSIFICATION GUIDANCE

CARVER is a threat assessment tool that originated from the Department of Defense. A brief description of each component of CARVER follows:

- Criticality - public health or economic impact;
- Accessibility - physical access to target;
- Recuperability - ability of the system to recover from the attack;
- Vulnerability - ease of accomplishing the attack;
- Effect - amount of actual direct loss from an attack; and,
- Recognizability - ease of identifying target.

To make the tool applicable to the entire food and agricultural sector, the Homeland Security Council Working Group, which first applied CARVER, also modified it to include a shock component. Shock is the combined measure of the health, psychological, and collateral national economic impacts of a successful attack on the target system.

Definitions:
Node: A step during agricultural production, food preparation, or food processing (includes farm-to-table continuum).
Agent: Select agent, pathogen, disease or pest, or chemical, biological, nuclear, radiological, or otherwise harmful substance.
Product: Agricultural commodity (i.e., soybeans, beef cattle) or food product (i.e., egg products, meat, poultry).

Item	Classification Level	Reason for Classification	Duration of Classification	Remarks
Name of specific threat agent used in conjunction with the CARVER+Shock Results Matrix, Scores, and Criticality Worksheet.	SECRET	1.4 (e, g & h)	25 years	Introduction of agent X at nodes with high scores and public health consequences indicates a vulnerability that could be used to target the food sector
CARVER + Shock Results Matrix, which identifies ALL nodes and their scores.	SECRET	1.4 (e, g & h)	25 years	This matrix identifies the most vulnerable nodes based on their scores which could be used to target the food sector
CARVER + Shock scores identified with a specific node.	SECRET	1.4 (e, g & h)	25 years	When the score is associated with a specific node in the narrative of the report this can reveal appealing targets, system capabilities, and strengths/weaknesses in the system.
CARVER + Shock Criticality Worksheet and Individual Node Worksheets with scores and supporting justification remarks for the scores; including number of deaths and economic loss estimates.	SECRET	1.4 (e, g & h)	25 years	Consequences pertaining to the use of a specific threat agent to target the food at a specific node. Documentation of the subject matter experts' reasoning for specific node scores.
Information on facility visited for a vulnerability assessment.	Unclassified/CUI			Includes general and publicly available information on the facility.

Item	Classification Level	Reason for Classification	Duration of Classification	Remarks
Information collection phase of vulnerability assessments may include discussions to obtain industry and statistical subject matter expertise, which involves the preparation of background information and industry process flow diagrams.	Unclassified			Working papers gathered and developed from subject matter experts that do not include CARVER+Shock scoring.