Description of document:	Department of the Treasury (USDT) Security Classification Guide Number 1, 2021
Requested date:	24-May-2024
Release date:	16-September-2024
Posted date:	06-January-2025
Source of document:	FOIA Request Department of the Treasury 1500 Pennsylvania Ave. NW Washington D.C. 20220 Treasury FOIAXpress PAL Request web page FOIA.gov

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

September 16, 2024

RE: Your FOIA Request to Treasury, Case Number [2024-FOIA-00493]

This is the Office of Intelligence and Analysis's (OIA) final response to your Freedom of Information Act (FOIA) request to the U.S. Department of the Treasury, dated 24 May 2024. You requested copies of records related to:

> "A copy of the Treasury Departmental Offices "Consolidated Classification Guide". See, for example., note B-2 here:
>
> https://www.archives.gov/files/isoo/fcgr/fy-2022-fcgr-report-treasury-.pdf"

Your request has been processed under the provisions of the FOIA, 5 U.S.C. § 552. A reasonable search was conducted for records responsive to your request.

In response to the search, 91 pages were located within the Departmental Offices of Treasury. After carefully considering these records, Treasury is releasing 3 pages in part, releasing 18 pages in full, and withholding 70 pages in full. The withheld information is protected from disclosure under the FOIA pursuant to 5 U.S.C. § 552 (b)(2), (b)(3) [Statute 50 U.S.C. § 3024(i)(1)) (National Security Act of 1947)], and (b)(6).

FOIA Exemption (b)(2), Permits withholding of records and information about Internal personnel rules and practices, including internal matters of a relatively trivial nature and also more substantial internal matters, the disclosure of which would risk circumvention of a legal requirement.

FOIA Exemption (b)(3), Permits withholding information prohibited from disclosure by another federal statute. The applicable statute is: 50 U.S.C. § 3024(i)(1)) (National Security Act of 1947).

FOIA Exemption (b)(6), Permits withholding of records and information about individuals when disclosure would be a clearly unwarranted invasion of personal privacy.

Treasury has considered the foreseeable harm standard when reviewing the records and applying these exemptions.

There are no fees assessed at this time since allowable charges fell below $25.

You have the right to appeal this decision within 90 days from the date of this letter. By filing an appeal, you preserve your rights under FOIA and give the agency a chance to review and reconsider your request and the agency's decision. Your appeal must be in writing, signed by you or your representative, and should contain the rationale for your appeal. Please also cite the FOIA reference number noted above. Your appeal should be addressed to:

FOIA Appeal
FOIA and Transparency
Office of Privacy, Transparency, and Records
Department of the Treasury
1500 Pennsylvania Ave., N.W.
Washington, D.C. 20220

If you submit your appeal by mail, clearly mark the letter and the envelope with the words "Freedom of Information Act Appeal." Your appeal must be postmarked or electronically transmitted within 90 days from the date of this letter.

If you would like to discuss this response before filing an appeal to attempt to resolve your dispute without going through the appeals process, you may contact our FOIA Public Liaison for assistance via email at FOIAPL@treasury.gov, or via phone at (202) 622-8098. A FOIA Public Liaison is a supervisory official to whom FOIA requesters can raise questions or concerns about the agency's FOIA process. FOIA Public Liaisons can explain agency records, suggest agency offices that may have responsive records, provide an estimated date of completion, and discuss how to reformulate and/or reduce the scope of requests in order to minimize fees and expedite processing time.

If the FOIA Public Liaison is unable to satisfactorily resolve your question or concern, the Office of Government Information Services (OGIS) also mediates disputes between FOIA requesters and federal agencies as a non-exclusive alternative to litigation. If you wish to contact OGIS, you may contact the agency directly by email at OGIS@nara.gov, by phone at (877) 684-6448, or by mail at the address below:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road – OGIS
College Park, MD 20740-6001

Please note that contacting any agency official (including the FOIA analyst, FOIA Requester Service Center, FOIA Public Liaison) and/or OGIS is not an alternative to filing an administrative appeal and does not stop the 90-day appeal clock.

You may reach me via telephone at 202-622-0930, extension 2; or via e-mail at FOIA@treasury.gov. Please reference FOIA case number [2024-FOIA-00493] when contacting our office about this request.

Sincerely,

Kate Amlin
Deputy Assistant Secretary
Office of Intelligence and Analysis

Enclosures
Responsive document set (21 pages)

DEPARTMENT OF THE TREASURY

Security Classification Guide Number 1

September 29, 2021

ISSUED BY: Office of Security Programs, 701 Madison Pl NW, Washington, DC 20005

Approved By:

Michael Neufeld
Assistant Secretary for Intelligence and Analysis (Acting)

Security Classification Guide Number 1 dated September 29, 2021 supersedes Department of the Treasury Security Classification Guide dated April 18, 2014.

Security Classification Guide No. 1
September 29, 2021

FOREWORD

The Department of the Treasury (Treasury) Security Classification Guide Number 1 (Treasury SCG #1) provides authoritative derivative classification guidance concerning the security classification; dissemination controls, where applicable; and level of protection afforded Treasury originated national security information based on criteria established in Executive Order 13526, *Classified National Security Information* (the Order) or any successor Order, its implementing directive, 32 CFR Part 2001, *Classified National Security Information* and Treasury implementing policies, directives, and regulations. The Guide is not intended to provide specific guidance concerning the handling, safeguarding, transport, declassification and downgrading, destruction, or administration of classified material, regardless of form. Specific guidance concerning these topics is available in the Order, 32 CFR Part 2001, Treasury Directive (TD) Publication (TD P) 15-71, *Treasury Security Manual*; and those other documents referenced herein.

Security Classification Guide No. 1
September 29, 2021

CHANGE/REVISION HISTORY	DATE PUBLISHED

Security Classification Guide No. 1
September 29, 2021

TABLE OF CONTENTS

Figures

Security Classification Guide No. 1
September 29, 2021

SECTION 1

THE GUIDE AND ITS USE

1. PURPOSE

   a. The Department of the Treasury (Treasury) Security Classification Guide (SCG) Number 1 (Treasury SCG #1), hereafter referred to as "the Guide," provides instructions in the proper and uniform derivative classification of information and is based on a series of predetermined original classification decisions authorized by individuals with delegated authority to exercise original classification authority (OCA), as established in Treasury Order (TO) 105-19, *Delegation of Original Classification Authority; Requirements for Downgrading and Declassification*.

   b. The Guide is the standard reference for derivative classification determinations within Treasury for collateral classified national security information. The Guide does not concern itself with sensitive compartmented information (SCI). For derivative classification decisions of SCI, derivative classifiers must refer to the specific SCI source document(s) and/or classification guide(s) to mark and protect such information.

2. AUTHORITY. This guide is issued under authority of section 2.2 of the Order. Classification of information involved in predetermined original classification decisions authorized by individuals with delegated authority to exercise original classification authority (OCA), as established in TO 105-19, *Delegation of Original Classification Authority; Requirements for Downgrading and Declassification* of June 27, 2011 is governed by, and is in accordance with, 32 CFR 2001.15. This guide constitutes authority and may be cited as the basis for classification, regrading, or declassification of information and material involved in those predetermined original classification decisions presented in this guide. Changes in classification required by application of this guide shall be made immediately. Information identified in this guide for protection as classified information is classified by Deputy Assistant Secretary for Security and Counterintelligence, the Treasury senior agency official, as authorized by section 2a(3) of TO 105-19 and section 2.2(b)(1) of the Order.

3. OFFICE OF PRIMARY RESPONSIBILITY (OPR). The Office of Security Programs is the OPR and issues this guide. All inquiries concerning content and interpretation as well as any recommendations for changes should be addressed to:

   Director, Office of Security Programs
   (Attention: Information Security Program)
   701 Madison Pl NW,
   Washington, DC 20005

4. APPLICABILITY. The Guide is approved for use by all Treasury employees authorized to classify derivatively national security information.

5. ELIGIBILITY FOR CLASSIFICATION. The determined classification level of each element of information presented in this SCG is in accordance with sections 1.4, *Classification Categories*, and 1.7, *Classification Prohibitions and Limitations*, of the Order.

6. CONTROLLED UNCLASSIFIED INFORMATION (CUI)

   a. The CUI Program standardizes the way the executive branch handles information that requires protection under laws, regulations, or Government-wide policies, but that does not qualify as classified under the Order, or any predecessor or successor order, or the Atomic Energy Act of 1954 (42 U.S.C. § 2011, et seq.), as amended.

   b. All approved categories and subcategories of CUI are published in the CUI Registry, as described in 32 CFR 2002.10, *The CUI Registry*. The CUI Registry is the online repository for all information, guidance, policy, and requirements on handling CUI. Among other information, the CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures. The Registry contains the only approved CUI categories, subcategories, and associated markings that may be used by Treasury employees. Treasury may not implement safeguarding or dissemination controls for any unclassified information other than those controls permitted by section 11, *Key Elements of the CUI Program: CUI categories and subcategories*, of TD P 80-08, *Controlled Unclassified Information (CUI) Guide*.

   c. Those CUI categories and subcategories cited, if any, in this SCG are in keeping with the requirements of 32 CFR Part 2002, *Controlled Unclassified Information*, and TD P 80-08. The information contained in the "Controlled Unclassified Information" portion of the SCG is the portion marking that must be applied to information meeting the element standard. As stated in section 19 of TD P 80-08, CUI portion markings are required in classified national security products to ensure that authorized holders can distinguish CUI portions from portions containing classified and uncontrolled unclassified information.

7. SUPPLEMENTAL GUIDANCE. Treasury OCAs are welcome and encouraged to supplement the Guide with additional guidance tailored to their specific requirements or functional responsibilities. All such supplemental guidance must be coordinated with the OPR who has overall responsibility for classification guides within Treasury. Each supplemental guide will be reviewed to ensure that it is consistent with the Guide and it will be coordinated, as appropriate, by the OPR with other internal and external organizations as required to reflect changes in the Order and 32 CFR Part 2001.

8. COMPILATION

   a. Compilations of information that are individually unclassified (or classified at a lower level) may be classified (or classified at a higher level) only if the compiled information reveals an additional association or relationship that:

      (1) Qualifies for classification pursuant to paragraph 5 of this section; and

      (2) Is not otherwise revealed by the individual elements of information.

   b. Classification as a result of compilation must meet the same criteria in terms of justification as other original classification actions.

   c. Classification as a result of compilation requires an original classification decision by an authorized OCA or classification guidance issued by an OCA.

   d. If the classification of an individual element cannot be determined, the information shall be protected at the level of classification of the compilation and the OPR contacted for specific guidance.

9. TENTATIVE CLASSIFICATION. For tentative classification, the following apply:

   a. Individuals who submit information to an OCA identified in TO 105-19 for an original classification decision shall provide that OCA the following information:

      (1) Determination that the information is owned by, produced by or for, or is under the control of the U. S. Government.

      (2) Determination the information falls within one or more of the categories of information listed in section 1.4 of the Order.

      (3) Determination the information has not already been classified by another OCA.

      (4) Determination that classification guidance is not already available in the form of SCGs, plans, or other memorandums.

      (5) Determine that there is a reasonable possibility that the information can be provided protection from unauthorized disclosure.

      (6) Determine and assign the appropriate level of classification (i.e., Top Secret, Secret, or Confidential) to be applied to the information, based on reasoned judgment as to

the degree of damage, which the OCA can describe, that could be caused by unauthorized disclosure. If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

(a) Determine the probable operational, technological, and resource impact of classification.

(b) If decisions must be rendered verbally due to exigencies of an ongoing operation or other emergency, issue written confirmation within seven calendar days of the decision and provide the required declassification and marking instructions.

(c) Be prepared to present, as required, depositions and expert testimony in courts of law concerning classification of national security information and to justify their original decisions.

(d) Be prepared to produce a written description of the damage, as necessary, for a classification challenge, a security classification review, a damage assessment, a request for mandatory review for declassification, a request for release under 5 U.S.C. § 552, *the Freedom of Information Act*, when pertinent to judicial proceedings, or as other statute or regulation may require.

b. Tentatively classify information or documents as working papers, pending approval by the OCA. Final classification decisions must be made as soon as possible, but not later than 180 days from the initial drafting date of the document.

c. Prior to the OCA's classification decision, such information shall be safeguarded as required for the specified level of classification and it shall not be used as a source for derivative classification.

10. CLASSIFICATION CHALLENGES. If at any time, any of the security classification guidance contained herein is challenged, the items of information involved shall continue to be protected at the level prescribed by this Guide until such time as a final decision is made on the challenge by appropriate authority. Classification challenges should be addressed to the OPR.

11. REPRODUCTION, EXTRACTION, AND DISSEMINATION. Authorized recipients of this Guide may reproduce, extract, and disseminate the contents of this Guide, as necessary, for application by specified groups involved in those predetermined original classification decisions presented in this Guide, including industrial activities. Copies of separate guides issued to operating activities in application of this Guide shall be sent to the OPR.

12. PUBLIC RELEASE. The fact that this guide shows certain details of information to be unclassified, including CUI, does not allow automatic public release of this information. Treasury information requested by the media or members of the public or proposed for release to the public by Treasury employees or their contractors shall be processed in accordance with 5 U.S.C. § 552 and/or 5 U.S.C. § 552a, *the Privacy Act of 1974*, and Treasury's implementing FOIA and Privacy regulations and Treasury's implementing FOIA and Privacy regulations (TD 25-05, *The Freedom of Information Act,* and TD 25-04, *The Privacy Act of 1974, as amended*). Such requests shall be processed by program disclosure staff; the Office of Privacy, Transparency, and Records; or by General Counsel.

13. FOREIGN DISCLOSURE. Any disclosure to foreign officials of information classified by this Guide shall be in accordance with National Disclosure Policy-1 (NDP-1), *National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations*, and must be coordinated through the Treasury Foreign Disclosure Office, Office of Information Sharing.

14. DEFINITIONS. For the definition of terms presented in this Guide, refer to Deputy Under Secretary of Defense for Intelligence and Security memorandum, *DoD Security Lexicon* of 13 June 2013. This document can be found at web link *https://my.testecm.gov/offices/securityprograms/pages/publications.aspx*.

SECTION 2

DERIVATIVE CLASSIFICATION GUIDANCE

1. DERIVATIVE CLASSIFIER RESPONSIBILITIES. Derivative classifiers shall:

   a. Observe and respect the classification determinations made by OCAs. If derivative classifiers believe information to be improperly classified, they shall take the actions required by section 1.10 of this Guide and Chapter III of TD P 15-71.

   b. Identify themselves and the classified information by marking it in accordance with subparagraph 2e(1) of this section.

   c. Use only authorized sources for classification guidance (e.g., SCG, memorandums, Treasury publications, and other forms of classification guidance issued by the OCA) and markings on source documents from which the information is extracted for guidance on classification of the information in question. The use of memory alone or "general rules" about the classification of broad classes of information is prohibited.

   d. Use caution when paraphrasing or restating information extracted from a classified source document. Paraphrasing or restating information may change the need for or level of classification.

   e. Take appropriate and reasonable steps, including consulting an SCG or requesting assistance from the appropriate OCA, to resolve doubts or apparent conflicts about the classification, level of classification, and duration of classification. In cases of apparent conflict between a security classification guide and a classified source document regarding a discrete item of information, the instructions in the SCG shall take precedence. Where required markings are missing or omitted from source documents, consult the OCA, appropriate SCG, or other classification guidance for application of the omitted markings.

2. DERIVATIVE CLASSIFICATION MARKINGS

   a. General. All classified documents shall bear the information identified in this section; however, in exceptional cases specific information required by this section may be excluded if it reveals additional classified information. The information is to be shown using these marking elements: portion marks; banner lines; Component, office of origin, and date of origin; and classification authority block. Specific requirements for each marking element are in section 6 of Chapter III of TD P 15-71. Material other than ordinary paper (and comparable electronic) documents shall have the same information

either marked on it or made immediately apparent to holders by another means.

b. Portion Markings. When using the Guide and its national security classification tables to classify derivatively information, the classification level indicated will be used to determine the portion marking. For example, if information were being classified based on the example in Figure 1, below, the portion mark to be used would be "(C)."

TABLE 1.0
Automated Information Systems (AIS)

#	Element of Information	Classification Level	Dissemination Controls	Controlled Unclassified Information	Reason (1.4)	Declassify On Date	Remarks
1	General information concerning Treasury information systems hardware, software, policies, or procedures where disclosure could be used to identify security vulnerabilities	Confidential			1.4(g)	25 years	

Figure 1. Example excerpt of a security classification guide for automated information systems.

c. Banner Lines (Overall Classification Markings). The banner line shall specify the highest level of classification (Confidential, Secret, or Top Secret) of information contained within the document and the most restrictive control markings applicable to the overall document; the classification level must be in English and spelled out completely; control markings included may be spelled out or abbreviated; and the banner line marking will always use upper case letters. For example:

CONFIDENTIAL

or

SECRET//FGI GBR//NOFORN

or

TOP SECRET//REL TO USA, AUS, GBR

d. Treasury Component, Office, and Date of Origin. Every classified document shall show on the first page, title page, or front cover (hereafter referred to as "the face of the document"), the originating agency and office and the date of the document's origin. This information shall be clear enough to allow someone receiving the document to contact the preparing office if issues or questions about the classification arise. If not otherwise evident, the agency and office of origin shall be identified and follow name and position on the ''Classified By:'' line.

e. Derivative Classification Authority Block. The face of each derivatively classified

document shall include a classification authority block consisting of these elements: "Classified By," "Derived From," and "Declassify On."

(1) Classified By: List name and position title or personal identifier of the DERIVATIVE classifier and, if not otherwise evident, include the Component and office of origin. For example:

(b)(6) **Program Analyst, Bureau of Engraving and Printing**

or

555555555

(2) Derived From:

(a) Single Source. Concisely cite the source document or classification guide used for the classification determination, to include the originating Component or agency and, where available, office of origin; type of document (e.g., memorandum, security classification guide, or message); subject; and date. For example:

Secretary of the Treasury ltr dtd 20150101, Subj: Authority for the action

(b) Multiple Sources. When multiple sources (i.e., more than one security classification guide, source document, or combination of these) are used to produce a derivatively classified document:

1. The "Derived From:" line shall state "Multiple Sources."

2. The list of multiple sources shall be included with or annotated on the derivative document. If the document has a bibliography or reference list, this may be used as the list of sources. Annotate it to distinguish the sources of classification from other references.

(3) Declassify On: Specify the date or event for declassification, exemption category with date or event for declassification, or other declassification instruction corresponding to the longest period of classification among the source document(s), security classification guide(s), and other applicable classification guidance issued by the OCA. The standard format YYYYMMDD shall be used when specifying dates in the "Declassify On:" line of the classification authority block. For example, using

Figure 1 declassification guidance of 25 years [from date of origin] and the document's date of origin is 3 September 2019 then the declassification date would be 3 September 2044. In keeping with the formatting requirement of YYYYMMDD:

3 September 2044 will be formatted to read: 20440903

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

(a) Example classification authority block with a single source:

Classified By: (b)(6) **Office of Security, Bureau of Engraving and Printing**
Derived From: Secretary of the Treasury ltr dtd 20150101, Subj: (U) Authority for the action
Declassify On: 20440903

(b) Example classification authority block with multiple sources:

Classified By: (b)(6) **Office of Security, Bureau of Engraving and Printing**
Derived From: Multiple Sources
Declassify On: *For declassification instructions, follow the guidance below.*

1. If the document is classified by "multiple sources" and different declassification instructions apply to information included, determine the MOST RESTRICTIVE declassification instruction that applies to any of the source information (i.e., the one farthest in the future giving the longest period for classification) and place it on the "Declassify On:" line. This will ensure all of the information in the document is protected for as long as necessary. The guidance in the subparagraphs below typically provides the most restrictive date and the longest period for classification, but in some specific cases (e.g., for some 25X instructions) the hierarchy specified may not provide the correct results. In ALL cases, one must determine the period of classification for each source document and select the MOST RESTRICTIVE declassification instruction to carry forward.

   a. When determining the most restrictive declassification instruction, this hierarchy applies:

(1) An ISCAP approved 75-year exemption (i.e., 75X1 through 75X9) with date or event for declassification.

(2) 50X1-HUM or 50X2-WMD.

(3) An ISCAP approved 50-year exemption (i.e., 50X1 through 50X9) with date or event for declassification.

(4) An ISCAP approved 25-year exemption (i.e., 25X1 through 25X9) with a date or event for declassification.

(5) A specific date or event for declassification, within 25 years of the creation of the derivative document.

(6) Absent a declassification instruction or other declassification guidance from the OCA, a calculated date 25 years from the date of the creation of the derivative document in accordance with subparagraph 2e(4)(b)2 of this section.

b. If declassification dates are specified for all of the source documents, place the LATEST date (i.e., the date farthest in the future) on the "Declassify On:" line; for Example: If the information is extracted from documents marked for declassification on 20110320 (i.e., March 20, 2011), 20120601 (i.e., June 1, 2012) and 20150403 (i.e., April 3, 2015), use "Declassify On: 20150403."

c. If the sources of classification indicate a combination of date(s) and event(s), indicate that declassification should occur on the latest date or the occurrence of the event(s), whichever is later; for Example: One source specifies "Declassify On: 20140803"; the other is marked "Declassify On: Completion of tests." Mark the derivatively classified document "Declassify On: 20140803 or Completion of tests, whichever is later."

d. When necessary, use the date or event for declassification associated with a 25, 50, or 75-year exemption to determine which marking is the most restrictive. Where an exemption marking is determined to be the most restrictive, also carry forward the associated date or event for declassification.

2. If a document does not specify a definitive date or event for declassification or

an exemption category determines its declassification date in accordance with this subparagraph and use that date when determining the most restrictive declassification instruction. Carry forward the calculated date to the "Declassify On:" line when it is determined to be the most restrictive.

a. If the source document, classification guide, or other guidance from the OCA does not specify a declassification instruction, use a date of 25 years from the date of the creation of the derivative document.

b. If the source document is missing both a declassification instruction and the date of its origin and there is no other guidance from the OCA, use a date of 25 years from the creation of the derivative document.

3. Follow the guidance in paragraph 3 of this section, when the source document or classification guide contains any of these declassification instructions: "Originating Agency's Determination Required," "OADR," "Source marked OADR," "Manual Review," "MR," Source marked MR," "DCI Only," "DNI Only," or any of the markings "X1," "X2," "X3," "X4," "X5," "X6," "X7," or "X8," or "Source marked X1" or any of the other markings "X2" through "X8." This also applies when these declassification instructions are used with "Source Marked:" and "Date of Source: [date]."

4. Carry over the declassification instruction "50X1-human" from the source document to the derivative document.

3. USE OF CALCULATED DECLASSIFICATION DATE IN PLACE OF PREVIOUS DECLASSIFICATION INSTRUCTIONS

a. Except as provided in subparagraph 3c of this section, when a source document is marked with any of the previously used declassification instructions listed in subparagraphs 3a(1) through 3a(5) of this section, the derivative markings shall use a calculated declassification date that is 25 years from the date of the creation of the derivative document, unless other guidance from the OCA is available.

(1) Originating Agency's Determination Required (OADR) or "Source marked OADR;"

(2) Manual Review (MR) or "Source marked MR;"

(3) DCI Only;

(4) DNI Only; or

(5) X1, X2, X3, X4, X5, X6, X7, X8, or "Source marked X1" or any other markings X2 through X8.

b. The "Derived From:" line or, if multiple sources are used, the listing of source documents shall identify the date of the source document(s), as required by subparagraph 2e(2) of this section.

c. If imagery subject to E.O. 12951, *Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems*, is marked with the declassification instruction "DCI Only" or "DNI Only," use "25X1, E.O. 12951" as the declassification instruction. (Contact the National Geospatial-Intelligence Agency Classification Management Office (NGA/SISCC) for assistance in determining whether specific imagery is subject to E.O. 12951.)

d. If a security classification guide calls for the use of any of the listed declassification instructions, the procedure in subparagraph 3a of this section shall be followed. Additionally, the holder of the classification guide should request updated guidance from the OCA, as all classification guides should reflect the requirements of E.O. 13526 and 32 CFR Parts 2001 and 2002 and those that do not must be updated immediately.

e. When using multiple sources of information all of whose declassification dates must be calculated, the "Declassify On:" line shall be calculated using the source with the MOST RECENT DATE. (Example: In the case of three source documents, one marked "OADR" and dated 2 September 1990, one marked "MR" and dated 3 December 1992, and one marked "X3" and dated 15 October 1995, the most recent date is 15 October 1995. Mark the derivative document "Declassify On: 20201015.")

4. COMPILATION. As previously stated in section 1.8 of this Guide, classification as a result of compilation occurs when the OCA has determined unclassified elements of information are combined and the compilation reveals classified information, or when classified elements are combined and the compilation reveals information at a higher classification level than the individual elements. Therefore, and in keeping with the OCA's determination:

a. Mark each portion with the classification appropriate for the information contained within the portion.

b. An explanation for the classification as a result of compilation shall be provided on the "Derived From:" line or directly below the derivative classification authority block. The explanation must clearly describe the circumstances under which the individual portions constitute a classified compilation, and when they do not. The explanation shall be portion marked as needed. Where specific classification guidance is provided (instead of

citing the document providing the guidance), it is to be protected, using the appropriate classification or CUI marking.

c. The following is the derivate classification authority block for a classification by compilation decision for (b)(6) Security Specialist, Office of Security Programs, United States (U.S.) Mint on 29 October 2019 and using the Figure 2, below, excerpt from the fictitious DoS SCG #15 of 12 January 2019. The CUI marking used in the example is for training purposes only.

Classified By: (b)(6) Security Specialist, Office of Security, U.S. Mint
Derived From: (U//FOUO) DoS SCG #15 dtd 20190112. The compilation of security devices and the specific location used if divulged could result in physical penetration of the area protected.
Declassify On: 20291029 or when security equipment is removed

TABLE 1.0
Security Programs

Item No.	Element of Information	Classification Level	Dissemination Controls	Controlled Unclassified Information	Reason (1.4)	Declassify On Date	Remarks
1	The fact that GSA-approved Deadbolt Devices are used.	U					
2	Specific location using a GSA-approved Deadbolt Device.	C			1.4(g)	10 years or when security equipment is removed.	
3	When the fact that Treasury uses Deadbolt Devices is combined with or used in association with the specific location using a GSA-approved Deadbolt Device.	S			1.4(g)	10 years or when security equipment is removed.	(FOUO) The compilation of security devices and the specific location used if divulged could result in physical penetration of the area protected.

Figure 2. Example excerpt of a security classification guide elements for security program equipment.

The CUI marking used in the example Table is for training purposes only.

5. SPECIAL NOTICES

a. In addition to the information specified by section 2 of this Guide, special notices may be required for specific types or categories of information by TD P 15-71 or other issuances. Unless another directive or legal authority prescribes different placement, these notices shall be placed on the face of the document. Examples of special notices are:

(1) Department of Defense (DoD) Distribution Statements. DoD source documents marked with a distribution statement must be transferred verbatim from the source document onto the derivatively classified document.

(2) Communications Security (COMSEC) Material. The special notice "COMSEC Material - Access by Contractor Personnel Restricted to U.S. Citizens Holding Final

Government Clearance" shall be placed on the face of classified documents handled within the COMSEC Material Control System, when required by National Security Agency/Central Security Service Policy Manual 3/16.

b. Other information requiring special notices include Not Releasable to Foreign Nationals (NOFORN), For Official Use Only (FOUO), Controlled Unclassified Information (CUI), and Foreign Intelligence Surveillance Act (FISA).

(1) NOFORN. The dissemination marking "NOFORN" is an intelligence control marking used to identify intelligence which an originator has determined meets the criteria of Intelligence Community Directive 710, *Classification Management and Control Markings System*, and which may not be provided in any form to foreign governments (including coalition partners), international organizations, foreign nationals, or immigrant aliens without the originator's approval.

(2) FOUO. Within the DoD, FOUO is a control marking for unclassified information that may be withheld from the public if disclosure would reasonably be expected to cause a foreseeable harm to an interest protected under the Freedom of Information Act. DoD's use of the FOUO marking remains in effect until full implementation of DoD Instruction 5200.48, *Controlled Unclassified Information (CUI)*.

(3) CUI. With the exception of DoD, CUI is the control marking for unclassified information the Government creates or possesses (or that an entity creates or possesses for or on behalf of the Government) that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls in accordance with E.O. 13556 and 32 CFR Part 2002. See section 1.6, above, for more information on this topic.

(4) FISA

(a) The FISA control marking denotes the presence of FISA or FISA-derived information in the document. This is an informational marking only to highlight such information. The FISA control marking required by this Volume does not satisfy or alter the legal requirement for such information to be accompanied by the FISA warning or caveat described in subparagraph 4b(4)(b) of this section.

(b) In accordance with 50 U.S.C. § 1801, et. seq., (also known as the Foreign Intelligence Surveillance Act of 1978, as amended), information collected pursuant to the statute may not be disclosed for law enforcement purposes unless the disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with

advance authorization of the Attorney General of the U.S.

(c) Specific wording of the applicable FISA warning or caveat must be provided by the cognizant legal office. The FISA warning or caveat should be collocated with the FISA or FISA-derived information; however, when necessary due to formatting limitations of some electronic systems, the FISA warning or caveat may appear at the top or bottom (e.g., in the header or footer) of the document.

SECTION 3

TREASURY SECURITY CLASSIFICATION TABLES

1. GENERAL. The following tables represent classification guidance for each system, plan, program, project, or mission involving classified information under the respective OCA's jurisdiction.

2. HOW TO READ THE GUIDE. The new format of the tables meets the requirements of 32 CFR 2001.15(b), *General content of classification guides* and is a blended format taken from the ISOO Guide: *Developing and Using Security Classification Guides* of October 2018, the Department of Defense Manual 5200.45, *Instructions for Developing Security Classification Guides* of 2 April 2013, and the Department of Justice SCG #1 of July 2012. The format includes:

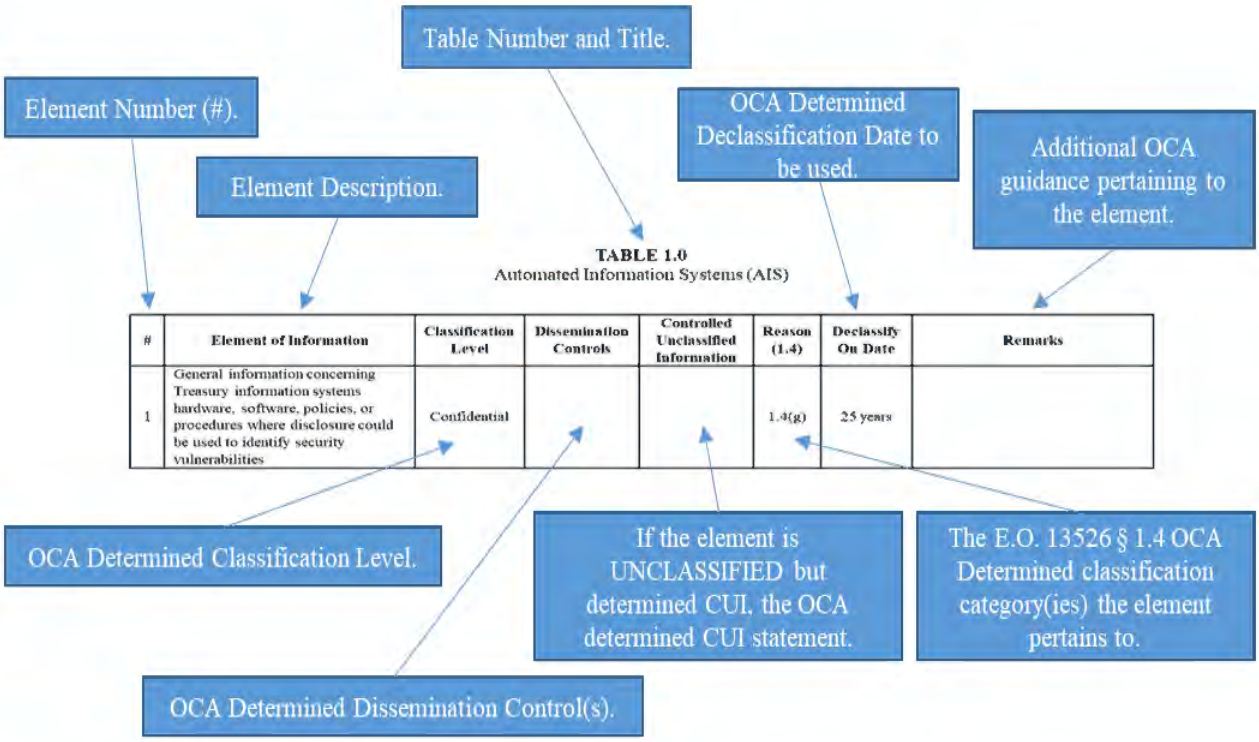

Figure 3. Breakdown of the portions of an element of a security classification guide.

3. TREASURY SECURITY CLASSIFICATION TABLES. The classification guidance issued in each of the tables presented in this Guide will be reviewed by the respective OCA at least once every five years to ensure currency and accuracy, or sooner when necessitated by significant changes in policy or in the system, plan, program, project, or mission, and update the guides as required.