



Department of Defense MANUAL

NUMBER 3020.45-M, Volume 3
February 15, 2011

USD(P)

SUBJECT: Defense Critical Infrastructure Program (DCIP) Security Classification Manual (SCM)

References: See Enclosure 1

1. PURPOSE

a. Manual. This Manual is composed of several volumes, each containing its own purpose. The purpose of the overall Manual is to provide uniform procedures for the execution of DCIP activities in accordance with the authority in DoD Directives (DoDDs) 5111.13 and 3020.40 (References (a) and (b)) and the guidelines and responsibilities in DoD Instruction (DoDI) 3020.45 (Reference (c)).

b. Volume. This Volume provides uniform guidance for the classification of information concerning DCIP activities, to ensure that necessary data and information is protected from unauthorized disclosure. It shall:

(1) Reissue the DCIP Security Classification Guide (Reference (d)) to implement policy established in References (b) and (c) for the risk management of Defense Critical Infrastructure (DCI).

(2) Establish the original classification authority (OCA) for DCI, the DCIP, and information collected or developed in support of these activities.

2. APPLICABILITY

a. This Volume applies to:

(1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components")

FOR OFFICIAL USE ONLY

(2) The Defense Infrastructure Sector Lead Agents (DISLAs) established by Reference (b).

b. This Volume does NOT:

(1) Address threat or intelligence information. Threat or intelligence information is classified by the agency that generated it.

(2) Address DoD Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) information. DoD DIB CS/IA information is classified according to guidance developed by OSD(NII)/DoD CIO.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy, according to Reference (b), that:

a. DCI risk management actions shall be coordinated and accomplished by responsible authorities, support incident management, and protect sensitive DCI-related information.

b. Information on DCIP plans, programs, and assets shall be safeguarded in accordance with pertinent DoD issuances on information and operations security.

5. RESPONSIBILITIES

a. Defense Critical Infrastructure Officer (DCIO). As the principal advisor to the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD(HD&ASA)) for critical infrastructure protection (CIP), the DCIO shall:

(1) Oversee and monitor compliance with this Manual.

(2) Support the ASD(HD&ASA), in his or her role as OCA for information covered by this Manual.

(3) Function as the point of contact for the Office of Primary Responsibility (OPR) for the maintenance of this Manual.

b. Heads of the DoD Components and DISLAs. The Heads of the DoD Components and DISLAs shall ensure compliance with this Manual in accordance with Reference (b).

6. PROCEDURES

a. This Volume shall be cited as the authority for classification, reclassification, and

declassification of all DCIP-related information and materials under DoD cognizance and control. Changes in classification guidance required for operational necessity will be made immediately upon notification and concurrence of the OCA. A formal review of this Volume will occur every 2 years and the Volume will be updated as necessary.

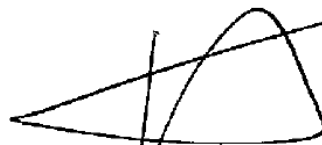
b. All inquiries concerning content and interpretation of this Volume, as well as recommendations for changes, should be addressed to:

Critical Infrastructure Protection Office
OASD (HD&ASA)
1235 S. Clark Street, Suite 1540
Arlington, VA 22202
Phone: (703) 602-5730

c. Detailed procedures are contained in Enclosure 2.

7. RELEASABILITY. RESTRICTED. This Volume is approved for restricted release. Authorized users may obtain copies on the SECRET Internet Protocol Router Network from the DoD Issuances Website at <http://www.dtic.smil.mil/whs/directives>.

8. EFFECTIVE DATE. This Volume is effective upon its publication to the DoD Issuances Website.



Paul Stockton
Assistant Secretary of Defense for Homeland
Defense and Americas' Security Affairs

Enclosures

1. References
 2. Procedures
 3. Classification Tables
- Glossary

TABLE OF CONTENTS

ENCLOSURE 1: REFERENCES.....5

ENCLOSURE 2: PROCEDURES.....7

 CLASSIFICATION7

 General.....7

 Reasons for Classification.....7

 Classification Standards.....8

 Classification by Compilation.....8

 Exceptional Circumstances.....9

 Challenges to Classification.....9

 Marking Requirement.....10

 Foreign Government Information (FGI).....10

 Reproduction, Extractions, and Dissemination.....11

 Release of Information.....11

 Protected Critical Infrastructure Information (PCII) Program.....12

ENCLOSURE 3: CLASSIFICATION TABLES13

 DCIP GENERAL CLASSIFICATION GUIDANCE13

 DCIP SPECIFIC CLASSIFICATION GUIDANCE.....16

 DIB CLASSIFICATION GUIDANCE17

GLOSSARY26

 ABBREVIATIONS AND ACRONYMS.....26

 DEFINITIONS.....27

TABLES

 1. DCIP General Classification Guidance13

 2. DCIP Specific Classification Guidance.....16

 3. DIB Classification Guidance17

FIGURES

 1. Derivative Downgrading Instruction from this Manual.....10

 2. Derivative Downgrading Instruction from Multiple Sources10

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5111.13, "Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD(HD&ASA))," January 16, 2009
- (b) DoD Directive 3020.40, "DoD Policy and Responsibilities for Critical Infrastructure," January 14, 2010
- (c) DoD Instruction 3020.45, "Defense Critical Infrastructure Program (DCIP) Management," April 21, 2008
- (d) "Defense Critical Infrastructure Program (DCIP) Security Classification Guide," May 2007 (hereby cancelled)
- (e) DoD 5200.1-R, "Information Security Program," January 14, 1997
- (f) Executive Order 13526, "Classified National Security Information" December 29, 2009
- (g) Executive Order 12829, "National Industrial Security Program (NISP)," January 6, 1993, as amended
- (h) DoD Manual 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)," February 28, 2006
- (i) Information Security Oversight Office Directive No. 1 "Classified National Security Information," part 2001 of title 32, Code of Federal Regulations
- (j) Under Secretary of Defense for Intelligence Directive-Type Memorandum 04-010, "Interim Information Security Guidance," April 16, 2004
- (k) DoD 5200.1-PH, "DoD Guide to Marking Classified Documents," April 1, 1997
- (l) DoD Directive 5230.24, "Distribution Statements on Technical Documents," March 18, 1987
- (m) U.S. Security Authority for NATO Affairs, Instruction 1-07, "North Atlantic Treaty Organization (NATO) Security," April 5, 2007¹
- (n) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008
- (o) DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," January 8, 2009
- (p) DoD Directive 5122.05, "Assistant Secretary of Defense for Public Affairs (ASD(PA))," September 5, 2008
- (q) DoD 5400.07-R, "DoD Freedom of Information Act Program," September 4, 1998
- (r) DoD Directive 5400.07, "DoD Freedom of Information Act (FOIA) Program," January 2, 2008
- (s) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information," October 9, 2008
- (t) DoD Instruction 5405.3, "Development of Proposed Public Affairs Guidance (PPAG)," April 5, 1991
- (u) DoD Manual 5205.02-M, "DoD Operations Security (OPSEC) Program Manual," November 3, 2008

¹ Reference may be obtained from the Central U.S. Registry.

- (v) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992
- (w) DoD Directive 5530.3, "International Agreements," February 18, 1991
- (x) Section 522 of title 5, U.S. Code (also known as The Freedom of Information Act)
- (y) Sections 131-134 of part 29 of title 6, Code of Federal Regulations
- (z) DoD Instruction 5200.39, "Critical Program Information (CPI) Protection Within the Department of Defense," July 16, 2008
- (aa) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms" as amended
- (ab) DoD Instruction O-3600.02, "Information Operation (IO) Security Classification Guidance," November 28, 2005

ENCLOSURE 2

PROCEDURES

1. CLASSIFICATION

a. General

(1) Security Classification Criterion. The criterion used in the selection of a security classification is the level of damage that unauthorized disclosure of the information could reasonably be expected to cause to the national security of the United States as outlined in, and in accordance with, DoD 5200.1-R; the provisions of Executive Order (E.O.) 13526; E.O. 12829; DoD 5220.22-M; and the Information Security Oversight Office (ISOO), Directive No. 1 (References (e) through (i), respectively). Enclosure 3 of this Volume provides guidance on the level and duration of classification for each specific topic covered by this document, as determined by the OCA. Reference (f) provides further guidance on the level and duration of classification and describes all classification duration options available to the OCA.

(2) DCIP

(a) The DCIP mission is to enhance risk management decision-making capability at all levels to ensure that DCI is available when required.

(b) The effectiveness of the DCIP depends on safeguarding information concerning the identification of, and risk to, DCI. This entails properly identifying, categorizing, and marking such information; managing access to classified information; and applying need-to-know criteria to determine access for specific organizations and personnel. The free and open exchange and dissemination of information is encouraged if it does not conflict with existing policies. Classified information may be disseminated to Government agencies, non-U.S. Government agencies, and contractors who possess the proper security clearances and a demonstrated need-to-know. Subparagraph 1.j.(3) of this enclosure discusses foreign disclosure.

(3) Classification of specific capabilities is generally covered under individual DoD Component program, system, or operations planning security classification guides (SCGs). Those guides should be consulted for classification guidance regarding specific capabilities.

(4) For security classification guidance on intelligence information related to DCIP activities or related to other DoD programs, refer to the appropriate published SCG.

b. Reasons and Length of Classification

(1) Classification is reserved for specific categories of information, or the compilation of related information, meeting the standards and criteria for classification as defined in References (e), (f), (h), and Directive-Type Memorandum 04-010 (Reference (j)).

(2) References (e) and (j) provide guidance on the duration of classification.

c. Classification Standards

(1) In order for information to be properly classified, it must meet the standards for classification as cited in Reference (f). As such, for information to be classified the following conditions must be met:

(a) An OCA, which for the purposes of this Volume is the ASD(HD&ASA), is classifying the information. This Manual provides the basic classification decisions for the DCIP.

(b) The information is owned by, produced by or for, or is under the control of the U.S. Government. In this context and per Reference (i), “control” means the authority of the agency that originates the information, or its successor in function, to regulate access to the information.

(c) The information falls within one or more of the categories of information listed in Reference (f).

(d) The OCA determines that the unauthorized disclosure of the information could reasonably be expected to result in damage to the national security, which includes defense against transnational terrorism, and the OCA is able to identify or describe the damage.

(2) When making classification decisions, due consideration must be given to ensure the information being considered meets the standards for classification as cited in subparagraphs 1.c.(1)(a) through (d) of this enclosure.

(3) Persons who only reproduce, extract, or summarize classified information, or who apply classification markings derived from source material or as directed by a classification guide, shall not be designated as an OCA.

d. Classification by Compilation

(1) A compilation is an orderly arrangement of preexisting materials (e.g., facts and statistics) gathered from multiple sources into one document or other single repository, such as a data base or data management system. A compilation of unclassified information is normally not classified. However, in certain circumstances, information that would otherwise be marked UNCLASSIFIED may become classified when combined with other unclassified information. If the compiled information reveals an additional association or relationship that meets the standards for classification in this Manual and that is not otherwise revealed in the individual items of information, then it may be classified because of the association revealed (as discussed). Users of this SCM must be aware of such a possibility when compiling unclassified information. When the determination is made by an OCA that classification by compilation is necessary, that OCA must provide explicit instructions as to what elements of the compilation, when combined, require classification and the reason why.

(2) Compilations of classified information should be classified at the same level as the highest classification level of any item of information contained therein until the OCA can render a judgment on the classification of the compilation. Consistent with sound classification principles, under certain conditions a compilation of multiple items of information, all of which are classified at one level (e.g., CONFIDENTIAL), can be classified at a higher level (e.g., SECRET) if the total damage caused by the unauthorized release of all of these items of information in compilation would equal or exceed the damage caused by the release of one single item of information classified at that higher level.

e. Exceptional Circumstances

(1) A situation may arise where a holder of information has reason to believe:

(a) Information should be classified but it is not covered by this SCM;

(b) A compilation of unclassified information should be classified; or

(c) Information should be classified, and thus handled and safeguarded, at a higher level of classification.

(2) Under such circumstances the information shall be marked with the anticipated level of classification and the notation "Pending Classification Review," appropriately safeguarded, and issue transmitted to the OPR (DCIO) for a classification determination by the OCA. The OPR shall issue the determination within 60 days of receipt of the request for review.

f. Challenges to Classification

(1) If holders of information have substantial reason to believe that the information is improperly or unnecessarily classified, they shall communicate that belief to their security manager or the classifier of the information to bring about any necessary correction. This action may be done as provided for in paragraph C4.9. of Reference (e).

(2) If, at any time, any of the security classification guidance contained herein is challenged, the items of information involved shall be protected at the higher level until the OCA renders a final decision on the challenge. Classification challenges should be addressed to the OCA via the activity security manager and the originator of the classified information. Appeal procedures for classification challenges can be found in paragraph C4.9. of Reference (e).

(3) If a conflict occurs between classification in this Manual and that associated with other specific capabilities, programs, or guidance, the OCAs of all concerned programs shall be promptly notified to adjudicate the differences. Until resolved, the more stringent guidance shall be followed.

(4) Organizations wishing to classify DCIP-produced data at levels higher than the prescribed minimums listed in this Manual must submit to the OCA a letter detailing the

justification for the increased level of classification. Include with this letter request an alternate means or method by which this data can be displayed and used at the prescribed level (such as removal of certain baseline elements of information categories of data). The OCA will review the submitted request and issue a formal adjudication within 60 days of receipt.

g. Marking Requirement

(1) Documents and other products covered by this Manual will be marked in accordance with Reference (e), (i), (j), DoD 5200.1-PH (Reference (k)), and DoDD 5230.24 (Reference (l)).

(2) When a document is derivatively classified, specific downgrading information must be used:

(a) For publications whose classification source is this Volume, see Figure 1.

Figure 1. Derivative Downgrading Instruction from this Manual

Derived From: DoDM 3020.45-M-V3, "Defense Critical Infrastructure Program (DCIP): Security Classification Manual (SCM)," date Declassify On: (Use the date/event stated in the declassification column of the appropriate topic in the SCM)
--

(b) When the classification source is more than one source document or classification guide, see Figure 2.

Figure 2. Derivative Downgrading Instruction from Multiple Sources

Derived From: Multiple Sources Declassify On: (Use the single most restrictive declassification guidance from all the source documents)
--

(c) If "Multiple Sources" are used for a derivatively classified document, a record of the sources used will be maintained with the file copy of the document.

h. Foreign Government Information (FGI)

(1) In accordance with paragraph C.5.7.4 of Reference (e), documents that contain FGI shall include the marking "This Document Contains (indicate country of origin) Information." The portions of the document that contain the FGI shall be marked to indicate the government and classification level, using accepted country code standards, e.g., "(Country code-C)." If the identity of the specific government must be concealed, the document shall be marked "This Document Contains Foreign Government Information," and pertinent portions shall be marked "FGI" together with the classification level, e.g., "(FGI-C)." In such cases, a separate record that identifies the foreign government shall be maintained in order to facilitate subsequent declassification actions.

(2) North Atlantic Treaty Organization (NATO)-classified information shall be safeguarded in compliance with the U.S. Security Authority for NATO Affairs, Instruction 1-07 (Reference (m)).

i. Reproduction, Extraction, or Dissemination. Authorized recipients of this Manual may, as necessary, reproduce, extract, and disseminate the contents of this Manual consistent with References (e) and (l).

j. Release of Information

(1) Public Release. Unclassified information is not always automatically releasable to the public. DoD information requested shall be processed in accordance with Reference (e), DoDD 5230.09, DoDI 5230.29, DoDD 5122.05, DoD 5400.7-R, DoDD 5400.07, DoDI 5200.01, DoDI 5405.3, and DoD Manual 5205.02 (References (n) through (u), respectively). Forward all proposed public release requests to the OPR for review and coordination with the Office of Security Review prior to release.

(2) Release to U.S. Government Agencies and Contractors

(a) All requests for release of classified DCIP information outside of DoD must be approved by the ASD(HD&ASA), in accordance with policy established by References (e) and (h). DoD annually releases the DIB Critical Asset List to the Department of Homeland Security and the Federal Bureau of Investigation in accordance with References (b) and (c).

(b) In addition to requirements in paragraph 1j(2)(a) of this enclosure, classified information or controlled unclassified information (CUI) may be provided to other DoD Components, other U.S. Government agencies, and U.S. contractors only in accordance with the contract requirements; applicable laws and regulations; and upon determination by the holder of the information that the requester has the proper level of security clearance and has a valid "need-to-know." If a DoD support contractor, in performance of direct support to a DoD agency or organization, requires access to proprietary information, a non-disclosure agreement will be prepared, signed, and placed on file with the DoD OPR prior to releasing the information.

(3) Foreign Disclosure. Classified information is a national security asset that shall be protected and will be shared with foreign governments only when there is a clearly defined benefit to the United States. Any disclosure to foreign officials of information classified by this Manual shall be in accordance with the procedures set forth in the National Disclosure Policy as implemented in Reference (e), DoDD 5230.11 (Reference (v)), DoDD 5530.3 (Reference (w)), and in any applicable international agreement(s).

(4) CUI

(a) In addition to classified information, there are certain types of unclassified information that do not meet the standards and criteria for classification under Reference (d), but for which Executive Branch agencies require application of controls and protective measures for a variety of reasons. Such information is referred to collectively as CUI. CUI includes

information labeled “For Official Use Only (FOUO),” “Sensitive But Unclassified (SBU),” “Drug Enforcement Agency Sensitive,” and “Law Enforcement Sensitive.” Mark and handle CUI, including FOUO and other sensitive information, in accordance with current DoD policy. See Reference (s) and Appendix 3 to Reference (e) for further information.

(b) FOUO is a designation that is applied to unclassified information that may be exempt from mandatory release to the public under section 552 of title 5, United States Code, also known and hereafter referred to as “The Freedom of Information Act (FOIA)” (Reference (x)). FOIA specifies nine exemptions that may qualify certain information to be withheld from release to the public if, by its disclosure, a foreseeable harm would occur. See Reference (q) for guidance on FOIA exemptions.

k. Protected Critical Infrastructure Information (PCII) Program. PCII is another form of CUI. Individuals with questions regarding the handling and marking of PCII should contact the DoD PCII Program Office at 703-602-5730 or at Info-PCII@osd.mil. See sections 131-134 of part 29 of title 6, Code of Federal Regulations (Reference (y)) for further information.

ENCLOSURE 3CLASSIFICATION TABLES

1. DCIP GENERAL CLASSIFICATION GUIDANCE. Table 1 provides security classification guidance for topics related to the overall DCIP effort. The classification of the material associated with that topic, declassification date, reason for classification, and any specific guidance on determining the correct classification level is given for each topic. Refer to Enclosure 2 for DCIP classification by compilation issues not covered in Table 1. Classifications will be marked as (U) Unclassified, (C) Confidential, (S) Secret, and (TS) Top Secret. FOIA exemptions cited in the tables of this enclosure may be found in Reference (q).

Table 1. DCIP General Classification Guidance (FOUO)

TOPIC	MIN CLASS	REASON See Reference (e)	DURATION	REMARKS
DCIP PROGRAMATICS				
1.1. Existence of DCIP.	U	N/A	N/A	
1.2. Acronym DCIP	U	N/A	N/A	
1.3. The concept that: DoD operations depend on specific assets and infrastructures; or, Disruption of an asset or infrastructure may adversely affect DoD operations.	U	N/A	N/A	
1.4. The fact that the Department of Defense analyzes: The criticality and vulnerability of its assets and infrastructures; or, Its dependence on commercial assets and infrastructures; or, Actions to remediate or mitigate its vulnerabilities and to assure its military operations.	U	N/A	N/A	

Table 1. DCIP General Classification Guidance (FOUO), Continued

TOPIC	MIN CLASS	REASON See Reference (e)	DURATION	REMARKS
1.5. The method used to determine if an asset is considered critical.	See Remarks			Classifications of the methods used to determine criticality will be based upon the classification level associated with the methods' governing publication.
DCIP ADMINISTRATION				
1.6. DCIP program/project milestone schedule.	U	N/A	N/A	Milestone schedules for CIP, shown by themselves, are not generally classified. Milestone schedules associated with a classified program shall be classified at the same level as is required for the program itself. If associated with lists of specific critical assets or to specific vulnerabilities, they may be classified at the same level as the asset or vulnerability.
1.7. Compilation of Defense Infrastructure Sector characterization data, including identification of sector-related assets.	U	N/A	N/A	<p>Mark FOUO in accordance with FOIA Exemption (2). If the asset, or the impact of loss of the asset, when associated with a plan or operation is at a higher classification level, then this information is classified, at a minimum, at the classification level of the asset identified, or as is required for the plan or operation identified.</p> <p>Any sector compilation of characterization data associated with an asset's criticality to the Department of Defense, such as used in conjunction with the terms task critical assets (TCAs), defense critical assets (DCAs), or DCI, is classified in accordance with sections 2.1 through 2.6. of Table 2 of this enclosure.</p>

Table 1. DCIP General Classification Guidance (FOUO), Continued

TOPIC	MIN CLASS	REASON See Reference (e)	DURATION	REMARKS
1.8. DCIP analysis that identifies association of assets with specific METs, Sector functions, or operational capabilities.	U	N/A	N/A	<p>Mark FOUO in accordance with FOIA Exemption (2). If the asset, or the impact of loss of the asset, when associated with a plan or operation is at a higher classification level, then this information is classified, at a minimum, at the classification level of the asset identified, or as is required for the plan or operation identified.</p> <p>Any compilation of data associated with an asset's criticality to the Department of Defense, such as used in conjunction with the terms task critical assets (TCAs), defense critical assets (DCAs), or DCI, is classified in accordance with sections 2.1 through 2.6. of Table 2 of this enclosure.</p>
1.9. DCIP accounting or appropriation data; budget estimates; and/or funding levels.	U	N/A	N/A	<p>Mark FOUO in accordance with FOIA Exemption (5) for documents used in the formal Planning, Programming, Budgeting and Execution System (PPBES) process; otherwise mark in accordance with FOIA Exemption (2).</p> <p>Funding levels for CIP, shown by themselves, are not generally classified. Funding levels associated with a classified program shall be classified at the same level as is required for the program itself. If associated with lists of specific critical assets or with specific vulnerabilities, they may be classified at the same level as the asset or vulnerability.</p>
1.10. Classification guidance contained in this Volume.	U	N/A	N/A	Mark FOUO in accordance with FOIA Exemption (2).

2. **DCIP SPECIFIC CLASSIFICATION GUIDANCE.** Table 2 provides security classification guidance for topics related to more specific requirements. The appropriate classification(s) of the material associated with that topic, declassification date, reason for classification, and any specific guidance on determining the correct classification level is given for each topic. Refer to Enclosure 2 of this Volume for DCIP classification by compilation issues not covered in Table 2.

Table 2. DCIP Specific Classification Guidance (FOUO)

TOPIC	MIN CLASS	REASON See Reference (e)	DURATION	REMARKS
TASK CRITICAL ASSETS (TCAs)				
2.1. Individual or lists of TCAs when associated with the term “Task Critical Asset(s)” or “TCA(s).”	S	1.4.(a)	10 years from date of this Volume	If the asset by itself, or the association of the asset or impact of loss of the asset, when associated with a plan or operation is at a higher classification level, then this information is classified, at a minimum, at the classification level of the asset identified, or as is required for the plan or operation identified.
2.2. Information when associated with the term “Task Critical Asset(s)” or “TCA(s)” that will provide an analyst with the identity, location, vulnerabilities, inter- or intra-sector dependencies, or risk response actions, or risk response actions related to a TCA or the missions the TCA supports.	S	1.4.(a)	10 years from date of this Volume	If the asset by itself, or the association of the asset or impact of loss of the asset, when associated with a plan or operation is at a higher classification level, then this information is classified, at a minimum, at the classification level of the asset identified, or as is required for the plan or operation identified.
2.3. Individual or lists of assets associated with the term “Task Critical Asset(s)” or “TCA(s)” when also associated with a Special Access Program (SAP) or Sensitive Compartmented Information (SCI)-related program.	See Remarks			If the asset, or impact or loss of an asset, is associated with a SAP or SCI-related program, then this information is classified, at a minimum, at the classification level of the SAP or SCI-related program.

Table 2. DCIP Specific Classification Guidance (FOUO), Continued

TOPIC	MIN CLASS	REASON See Reference (e)	DURATION	REMARKS
DCAs				
2.4. Individual or lists of assets including DCA nominations by the Chairman of the Joint Chiefs of Staff, when associated with the term “Defense Critical Asset(s)” or “DCA(s).”	TS	1.4.(a)	25 years from date of this Volume	If the asset by itself, or the association of the asset or impact of loss of the asset, when associated with a plan or operation is at a higher classification level, then this information is classified, at a minimum, at the classification level of the asset identified, or as is required for the plan or operation identified.
2.5. Information when associated with the term “Defense Critical Asset(s)” or “DCA(s).” that will provide an analyst with the identity, location, vulnerabilities, or risk response actions related to a DCA or the missions the DCA supports.	TS	1.4.(a)	25 years from date of this Volume	If the asset by itself, or the association of the asset or impact of loss of the asset, when associated with a plan or operation is at a higher classification level, then this information is classified, at a minimum, at the classification level of the asset identified, or as is required for the plan or operation identified.
2.6. Individual or lists of DCAs including DCA nominations by the Chairman of the Joint Chiefs of Staff, when associated with the term “Defense Critical Asset(s)” or “DCA(s)” when associated with a SAP or SCI-related program.	See Remarks			If the asset, or impact or loss of an asset, is associated with a SAP or SCI-related program, then this information is classified, at a minimum, at the classification level of the SAP or SCI-related program.

3. **DIB CLASSIFICATION GUIDANCE.** Table 3 provides general and specific security classification guidance for information on non-DoD-owned DIB facilities. Information related to DoD-owned DIB facilities is covered by their existing DoD classification and information protection requirements. The classification of the material associated with that topic, declassification date, reason for classification, and any specific guidance on determining the correct classification level is given for each topic. Refer to Enclosure 2 of this Volume for DCIP classification by compilation issues not covered in Table 3.

Table 3. DIB Classification Guidance (FOUO)

TOPIC	MIN CLASS	REASON See Reference (e)	DURATION	REMARKS
GENERAL DoD-DIB ASSOCIATION				
3.1. The term and/or definition, "Defense Industrial Base (DIB)."	U	N/A	N/A	
3.2. Program data containing CUI, including FOUO, SBU, PCII, and Critical Program Information as defined in DoDI 5200.39 (Reference (z)).	U	N/A	N/A	Mark FOUO in accordance with FOIA Exemption (2) Information that may qualify as CUI under this program could require classification and application of special handling caveats if warranted by other program, system, or operations planning classification guidance. Consult appropriate classification guides. See paragraph 2.k. of Enclosure 2 of this Volume for PCII guidance.
3.3. The fact that the Department of Defense is working with unidentified DIB members to improve their security; formulating security policies; and developing capabilities associated with this activity.	U	N/A	N/A	(See Rules #1 and 3.)
3.4. Identification of DIB members participating in DCIP.	U	N/A	N/A	

Table 3. DIB Classification Guidance (FOUO), Continued

TOPIC	MIN CLASS	REASON See Reference (e)	DURATION	REMARKS
3.5. Identification of one or more DIB locations on the “DIB important” list as defined by the DIB Sector.	U	N/A	N/A	Mark FOUO in accordance with FOIA Exemptions (2) and (4).
3.6. Any association of one or more DIB locations with the term “TCA.”	See Remarks			Classify in accordance with the TCA table of this Volume.
3.7. Any association of one or more DIB locations with the term “DCA.”	See Remarks			Classify in accordance with the DCA table of this Volume.
3.8. Proprietary information collected from DIB or commercial partners to determine the criticality of the location to the Department of Defense.	U	N/A	N/A	Mark FOUO in accordance with FOIA Exemptions (2) and (4). (See Rule #1.)
3.9. Meetings supporting DCIP, if held at a DIB member location or other location.	U	N/A	N/A	Knowledge of the meeting may be unclassified, while the substance of the meeting may be classified.
3.10. General budget information (e.g., total program spending) on DoD DIB-related DCIP activities.	U	N/A	N/A	Mark FOUO in accordance with FOIA Exemption (5) for documents used in the formal PPBES process; otherwise, mark in accordance with FOIA Exemption (2). Information as published in the Unclassified budget is unclassified and requires no special marking or handling. Funding levels, shown by themselves, are not generally classified. Funding levels associated with a classified program shall be classified at the same level as is required for the program itself. If associated with lists of specific identified critical assets or to specific vulnerabilities, refer to the TCA or DCA tables of this Volume.

Table 3. DIB Classification Guidance (FOUO), Continued

TOPIC	MIN CLASS	REASON See Reference (e)	DURATION	REMARKS
3.11. Specific budget information (e.g., funding levels for specific tasks) on DoD DIB-related DCIP activities.	U	N/A	N/A	Mark FOUO in accordance with FOIA Exemption (5) for documents used in the formal PPBES process; otherwise, mark in accordance with FOIA Exemption (2). Information as published in the Unclassified budget is unclassified and requires no special marking or handling. Funding levels, shown by themselves, are not generally classified. Funding levels associated with a classified program shall be classified at the same level as is required for the program itself. If associated with lists of specific critical assets or to specific vulnerabilities, may be classified, refer to the TCA or DCA tables of this Volume.
3.12. DIB member Internet protocol (IP) address.	U	N/A	N/A	Mark FOUO in accordance with FOIA Exemption (4).
DIB-RELATED THREATS AND RESPONSE				
3.13. The fact the Defense Contract Management Agency:				
a. Is involved in DCIP.	U	N/A	N/A	
b. Leverages, integrates, generates, disseminates, and analyzes threat information products for the DIB.	U	N/A	N/A	Mark FOUO in accordance with FOIA Exemptions (2) and (4).
3.14. DIB-generated indications and warning (I&W) information of a general nature related to the DIB that does not reveal sources and methods.	U	N/A	N/A	Mark FOUO in accordance with FOIA Exemptions (2) and (4). (See Rule #3.)

Table 3. DIB Classification Guidance (FOUO), Continued

TOPIC	MIN CLASS	REASON See Reference (e)	DURATION	REMARKS
3.15. DIB-generated specific I&W information related to the DIB that includes sources or methods or other information identifying the adversary.	U	N/A	N/A	Mark FOUO in accordance with FOIA Exemptions (2) and (4). (See Rules #2 and 3.)
3.16. USG-generated I&W information of a general nature related to the DIB that does not reveal sources and methods.	See Remarks	N/A	N/A	(See Rule #2.) Classification of I&W from non-intelligence sources will be classified at the level designated by the source of that information.
3.17. U.S. Government-generated specific I&W information related to the DIB that includes sources or methods or other information identifying the adversary.	See Remarks	N/A	N/A	(See Rule #2.) Classification of I&W from non-intelligence sources will be classified at the level designated by the source of that information.
3.18. General information about the transmittal of threat information to the DIB.	U	N/A	N/A	(See Rules #2 and 3.) Mark and handle in accordance with Reference (e).
DIB-RELATED VULNERABILITY ASSESSMENTS AND VULNERABILITY ASSESSMENT RESULTS				
3.19. The fact a DoD vulnerability assessment is being considered or planned for a DIB or commercial partner.	U	N/A	N/A	Mark FOUO in accordance with FOIA Exemptions (2) and (4). (See Rule #3.)

Table 3. DIB Classification Guidance (FOUO), Continued

TOPIC	MIN CLASS	REASON See Reference (e)	DURATION	REMARKS
3.20. Proprietary data collected during a DoD vulnerability assessment of a DIB member or commercial partner.	U	N/A	N/A	<p>Mark FOUO in accordance with FOIA Exemptions (2) and (4). (See Rule #3.)</p> <p>Classify higher if required by other information security requirements of the DIB member, such as DIB configurations that are required to be classified for the storage and use of DoD classified data.</p> <p>If data collected includes PCII, see paragraph 2.k. of Enclosure 2 of this Volume for PCII guidance.</p>
3.21. Information revealing a DIB member or commercial partner vulnerabilities.	U	N/A	N/A	<p>Mark FOUO in accordance with FOIA Exemptions (2) and (4). (See Rules #1 through 3.)</p> <p>If the vulnerability is compiled with a DIB facility designation of a TCA or DCA, then classify in accordance with the TCA or DCA table of this Volume.</p> <p>Classification of vulnerability data from non-intelligence sources will be classified at the level designated by the source of that information.</p> <p>If data collected includes PCII, see paragraph 2.k. of Enclosure 2 of this Volume for PCII guidance.</p>
3.22. A DIB member IP address paired with a vulnerability.	U	N/A	N/A	<p>Mark FOUO in accordance with FOIA Exemptions (2) and (4). (See Rules #1 through 3.)</p>

Table 3. DIB Classification Guidance (FOUO), Continued

TOPIC	MIN CLASS	REASON See Reference (e)	DURATION	REMARKS
3.23. The specific technology being pursued in response to a DIB vulnerability.	U	N/A	N/A	Mark FOUO in accordance with FOIA Exemptions (2) and (4). (See Rules #1 through 3.)
DIB ATTACKS OR INCIDENTS				
3.24. General information regarding a physical or cyber-related incident or attack at a DIB member location.	U	N/A	N/A	Mark FOUO in accordance with FOIA Exemptions (2) and (4). Consult appropriate security classification guides. (See Rules #1 through 3.)
3.25. If one or more DIB members has or have been the victim of a physical or cyber attack or incident, and/or identifying the exploited DIB member(s) by name.	U	N/A	N/A	Mark FOUO in accordance with FOIA Exemptions (2) and (4). Consult appropriate security classification guides. (See Rules #1 through 3.)
3.26. The fact that a DIB member has been exploited and/or the identifying the tactics, techniques, and procedures (TTPs) used when: the TTPs are NOT attributed to a specific adversary; and the TTPs are known via unclassified collection methods.	U	N/A	N/A	Mark FOUO in accordance with FOIA Exemptions (2) and (4). (See Rules #1 through 3.)
3.27. If a DIB member has been exploited and/or identifying the TTPs used when: the TTPs are attributed to a specific adversary; and/or the TTPs are known via classified collection methods.	S	1.4.(c)	10 years from date of this Volume	Higher classification and special handling caveats may be required and shall be applied if warranted by program, system, or operations planning classification guidance. Consult appropriate classification guides. (See Rules #1 through 3.)
3.28. Identification of a DIB target of an attack paired with the effect of the event.	U	N/A	N/A	Mark FOUO in accordance with FOIA Exemptions (2) and (4). (See Rules #1 through 3.)

Table 3. DIB Classification Guidance (FOUO), Continued

TOPIC	MIN CLASS	REASON See Reference (e)	DURATION	REMARKS
3.29. Incident reporting information about specific events related to a DIB member.	U	N/A	N/A	Mark FOUO in accordance with FOIA Exemptions (2) and (4). (See Rules #1 through 3.)
3.30. The title or existence of an intrusion event report, an interim compromise assessment, or a loss assessment report (if the title does not reveal the status or conduct of the report in association with a company, intrusion, or exfiltration).	See Remarks	N/A	N/A	Normally UNCLASSIFIED but higher classification may be required if there is content or compilation of data as identified in this or other classification guides. (See Rules #1 through 3.)
3.31. The fact that a DoD loss assessment was, is being, or will be conducted to determine the impact to DoD programs or that there are ongoing investigations and operations (law enforcement or counterintelligence).	U	N/A	N/A	Mark FOUO in accordance with FOIA Exemptions (2) and (4). (See Rules #1 through 3.)
3.32. The results, either preliminary or final, of a damage assessment.	S	1.4(g)	25 years from date of this Volume	(See Rules #1 and 2.) Higher classification and special handling caveats may be required and shall be applied if warranted by program, system, or operations planning classification guidance. Consult appropriate classification guides.
3.33. DIB-generated report information about specific threat methodology.	U	N/A	N/A	Mark FOUO in accordance with FOIA Exemptions (2) and (4). Higher classification may be required if there is content or compilation of data as identified in this or other classification guides. (See Rules #1 through 3.)

Table 3. DIB Classification Guidance (FOUO), Continued

TOPIC	MIN CLASS	REASON See Reference (e)	DURATION	REMARKS
3.34. Identification of potentially affected DoD programs resulting from an attack.	U	N/A	N/A	<p>Mark FOUO in accordance with FOIA Exemptions (2) and (4). (See Rules #1 and 2.)</p> <p>Higher classification and special handling caveats may be required and shall be applied if warranted by program, system, or operations planning classification guidance. Consult appropriate classification guides.</p> <p>Classification of vulnerability data from non-intelligence sources will be classified at the level designated by the source of that information.</p>

- Rule #1: Association of this data with a DIB TCA or DCA will be classified in accordance with the TCA or DCA table (Table 2). Higher classification and special handling caveats may be required and shall be applied if warranted by program, system, or operations planning classification guidance.
- Rule #2: Intelligence information will be classified in accordance with the appropriate DoD program or intelligence-related security classification guidance.
- Rule #3: For proprietary and privacy reasons, the Department of Defense declines to provide the names of participating companies; it is the prerogative of individual companies, if they choose, to highlight their participation.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ASD(HD&ASA)	Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs
CIP	critical infrastructure protection
CUI	controlled unclassified information
DCA	defense critical asset
DCI	defense critical infrastructure
DCIO	Defense Critical Infrastructure Officer
DCIP	Defense Critical Infrastructure Program
DIB	defense industrial base
DISLA	Defense Infrastructure Sector Lead Agent
DSS	Defense Security Service
E.O.	Executive order
FGI	foreign government information
FOIA	Freedom of Information Act
FOUO	For Official Use Only
IP	Internet protocol
I&W	indications and warnings
NATO	North American Treaty Organization
OCA	original classification authority
OPR	office of primary responsibility
PCII	protected critical infrastructure information
PKI	Public Key Infrastructure
SAP	special access program
SBU	sensitive but unclassified
SCG	security classification guide
SCM	security classification manual
SCI	sensitive compartmented information
TCA	task critical asset
TTP	tactics, techniques, and procedures

PART II. DEFINITIONS

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

adversary. Defined in Joint Publication 1-02 (Reference (aa)).

asset. Defined in Reference (b).

baseline elements of information. Defined in Volume 1 of this Manual.

CIP. Defined in Reference (b).

CUI. Defined in Appendix 3 of Reference (e).

DCA. Defined in Reference (b).

DCI. Defined in Reference (b).

DIB. Defined in Reference (b).

DIB member. An individual company of the DIB.

PCII. Not a classification; can be in either classified or unclassified documents. Validated critical infrastructure information, including information covered by section 29.6 (b) and (f) of Reference (y), including the identity of the submitting person or entity and any person or entity on whose behalf the submitting person or entity submits the critical infrastructure information, that is voluntarily submitted, directly or indirectly, to the Department of Homeland Security for its use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other appropriate purpose, and any information, statement, compilations or other material reasonably necessary to explain the critical infrastructure information, not customarily in public domain, put the critical infrastructure information in context, describe the importance or use of the critical infrastructure information, when accompanied by an express statement as described in section 29.5 of Reference (y). For PCII that involves information operations, see also DoD Instruction O-3600.02 (Reference (ab)).

TCA. Defined in Reference (c).