Department of Defense
MANUAL

NUMBER O-5205.13
April 26, 2012

DoD CIO

SUBJECT: Defense Industrial Base (DIB) Cyber Security and Information Assurance (CS/IA) Program Security Classification Manual (SCM)

References: See Enclosure 1

1. PURPOSE. In accordance with the authority in DoD Directive (DoDD) 5144.1 (Reference (a)); Executive Order (E.O.) 13526 (Reference (b)); E.O. 12829 (Reference (c)); and part 2001 of title 32, Code of Federal Regulations (also known as "Information Security Oversight Office (ISOO) Directive No. 1") (Reference (d)) and the guidance in DoD Manual 5200.01-V1 (Reference (e)), this SCM:

a. Establishes security classification guidance and identifies the original classification authority (OCA) for DIB information developed during the implementation of DoD Instruction (DoDI) 5205.13 (Reference (f)) in order to mitigate risks to critical DoD unclassified information supporting present and future DoD warfighting capabilities and residing on, or transiting, DIB unclassified private networks.

b. Identifies the level of protection required for information and materials produced under the DIB CS/IA program, including information within the DIB CS/IA cyber intrusion damage assessment process, between the DoD and DIB companies participating in the DIB CS/IA Program (hereinafter referred to as "DIB participants"), and as described in the DoD-DIB Framework for Cyber Security Information Sharing (Reference (g)) (hereinafter referred to as the "Framework Agreement").

c. Provides uniform criteria for the classification of aggregated DIB information and information related to cyber intrusion damage assessments to protect it from unauthorized disclosure. This SCM is the primary source of derivative classification guidance for reports and assessments developed within the DIB CS/IA program.

d. Incorporates and cancels the DoD DIB CS/IA Interim Security Classification Guidance (Reference (h)).

2. APPLICABILITY

a. This SCM 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 DoD, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the "DoD Components").

(2) Information developed and disseminated in direct support of the DIB CS/IA program. Information originating from another DoD program or intelligence source is governed by the appropriate program security classification guidance.

(3) Companies and programs participating in the DIB CS/IA program in accordance with the Framework Agreement and contracts that contain DIB cyber security requirements for safeguarding DoD classified and unclassified information. DIB participants shall handle classified and sensitive unclassified information, such as controlled unclassified information (CUI) (which includes For Official Use Only (FOUO) information), Critical Program Information (CPI) (as described in DoDI 5200.39, (Reference (i)), as required by law and regulation, the Framework Agreement, contracts, or this SCM.

b. This SCM does not address threat or intelligence information and materials generated outside the DIB CS/IA program. Threat or intelligence information is classified by the agency that generated the information.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. In accordance with Reference (b), information shall not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the United States' national security, and it pertains to one or more of the following:

(1) Military plans, weapons systems, or operations;

(2) Foreign government information;

(3) Intelligence activities (including covert action), intelligence sources or methods, or cryptology;

(4) Foreign relations or foreign activities of the U.S., including confidential sources;

(5) Scientific, technological, or economic matters relating to the national security;

(6) U.S. Government programs for safeguarding nuclear materials or facilities;

(7) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or

(8) The development, production, or use of weapons of mass destruction.

b. In accordance with Reference (b), Reference (c), Reference (e), DoD 5220.22-M (Reference (j)), classified transmissions will adhere to Government regulations and procedures for the transmission of classified information (e.g., SIPRNet, DIBNet-Secret, secure FAX, Secure Terminal Equipment).

c. In accordance with the Framework Agreement and DoD Instruction 8520.02 (Reference (k)), unclassified transmissions of unclassified cyber threat information products from the DoD to a DIB participant, and exchanges of information from the DIB participant to the DoD, will use DoD-approved Public Key Infrastructure (PKI) certificates.

d. Information provided by a DIB participant is inherently unclassified since the DIB does not have original classification authority (Reference (e)). Information provided by the U.S. Government must be properly classified in accordance with the appropriate program security classification guide or manual.

5. RESPONSIBILITIES

a. DoD Chief Information Officer (DoD CIO). The DoD CIO shall:

(1) Oversee and monitor DoD compliance with this SCM.

(2) Exercise Original Classification Authority (OCA) for information and materials produced under the DIB CS/IA program in accordance with References (a), (j), and (e).

(3) Oversee review of this SCM every 2 years and update it at least every 5 years.

b. Assistant Secretary of Defense for Global Strategic Affairs (ASD(GSA)). The ASD(GSA) shall, through the Deputy Assistant Secretary of Defense (DASD) for Cyber Policy, and under the authority, direction, and control of the Under Secretary of Defense for Policy (USD(P)), coordinate with DoD CIO on security classification decisions, integrating DIB CS/IA cyber threat information sharing, and enhancing DoD and DIB cyber situational awareness in accordance with Reference (e).

c. Heads of the DoD Components. The Heads of the DoD Components shall oversee Component compliance with this SCM in accordance with Reference (e).

6. PROCEDURES

a. This SCM shall be cited as the authority for classification, changes in classification, and declassification of all DIB CS/IA-related information and materials under DoD cognizance and control. Changes in classification guidance required for operational necessity will be made upon

notification and concurrence of the OCA.

b. The OCA shall retain classification authority for information and materials produced under the DIB CS/IA program. Users shall adhere to this Manual and shall cite authority derived from this Manual when classification and markings are applied.

c. All inquiries concerning the content and interpretation of this guidance, as well as any recommendations for changes, should be addressed to the Office of Primary Responsibility (OPR) at:

DIB CS/IA Program Office
DoD CIO
6000 Defense Pentagon
Washington DC 20301-6000
E-mail: DIB.CS/IA.Reg@osd.mil

d. Authorized recipients of this SCM may, as necessary, reproduce, extract, and disseminate the contents of this SCM consistent with References (e), (g), (j), or contract requirements.

e. Detailed procedures are contained in Enclosure 2.

7. RELEASABILITY. RESTRICTED. This SCM is approved for restricted release. It is available to users with Common Access Card authorization on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

8. EFFECTIVE DATE.

a. This SCM is effective upon its publication to the DoD Issuances Website.

b. If this SCM is not otherwise reissued or cancelled in accordance with DoD Instruction 5025.01 (Reference (l)), it will expire effective April 26, 2022 and be removed from the DoD Issuances Website.

Teresa M. Takai
DoD Chief Information Officer

Enclosures
1. References
2. Procedures
3. Classification Tables

Glossary

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005
(b) Executive Order 13526, "Classified National Security Information," December 29, 2009
(c) Executive Order 12829, "National Industrial Security Program," January 6, 1993, as amended
(d) Part 2001 of title 32, Code of Federal Regulations (also known as Information Security Oversight Office (ISOO) Directive No. 1, "Classified National Security Information; Final Rule," June 28, 2010)
(e) DoD Manual 5200.01-V1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012
(f) DoD Instruction 5205.13, "Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities," January 29, 2010
(g) DoD-DIB Framework for Cyber Security Information Sharing (also known as the "Framework Agreement")[1]
(h) DoD Defense Industrial Base (DIB) Cyber Security/Information Assurance (DIB CS/IA) Interim Security Classification Guidance, November 20, 2009 (hereby cancelled)[2]
(i) DoD Instruction 5200.39, "Critical Program Information (CPI) Protection Within the Department of Defense," July 16, 2008
(j) DoD 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006
(k) DoD Instruction 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," May 24, 2011
(l) DoD Instruction 5025.01, "DoD Directives Program," October 28, 2007
(m) DoD Manual 5200.01-V2, "DoD Information Security Program: Marking of Classified Information," February 24, 2012
(n) DoD Directive 5230.24, "Distribution Statements on Technical Documents," March 18, 1987
(o) U.S. Security Authority for NATO Affairs Instruction 1-07, "North Atlantic Treaty Organization (NATO) Security," April 5, 2007[3]
(p) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008
(q) DoD Directive 5230.25, "Withholding of Unclassified Technical Data From Public Disclosure," November 6, 1984
(r) DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," January 8, 2009
(s) DoD 5400.7-R, "DoD Freedom of Information Act Program," September 4, 1998

[1] Reference may be obtained from the DIB CS/IA Program Office, DoD CIO, 6000 Defense Pentagon, Washington DC 20301-6000, E-mail: DIB.CS/IA.Reg@osd.mil
[2] Reference may be obtained from the DIB CS/IA Program Office, DoD CIO, 6000 Defense Pentagon, Washington DC 20301-6000, E-mail: DIB.CS/IA.Reg@osd.mil
[3] Reference may be obtained from the Central U.S. Registry (https://secureweb.hqda.pentagon.mil/cusr/)

(t) DoD Directive 5400.07, “DoD Freedom of Information Act (FOIA) Program,” January 2, 2008
(u) DoD 5205.02-M, “DoD Operations Security (OPSEC) Program Manual,” November 3, 2008
(v) National Disclosure Policy (NDP-1), "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations," (short title: National Disclosure Policy (NDP-1)), October 1, 1988
(w) DoD Directive 5230.11, “Disclosure of Classified Military Information to Foreign Governments and International Organizations,” June 16, 1992
(x) DoD Directive 5530.3, “International Agreements,” June 11, 1987
(y) Executive Order 13556, “Controlled Unclassified Information,” November 4, 2010
(z) Joint Publication 1-02, “Department of Defense Dictionary of Military and Associated Terms,” current edition

ENCLOSURE 2

CLASSIFICATION PROCEDURES

1. GENERAL

a. This enclosure provides guidance on the level and duration of classification for each specific topic covered by this SCM, as determined by the OCA. References (b) and (e) provide further guidance on the level and duration of classification and describe all classification duration options available to the OCA.

b. DIB CS/IA is the DoD program to protect critical DoD unclassified program, technology, and operational information residing on, or transiting, DIB unclassified networks. DoD Components and industry participants collaborate to protect DoD information through the development, implementation, and execution of DoD and DIB processes and procedures.

c. Classification of specific system capabilities is generally addressed in individual DoD Component program, system, or operations planning security classification guides or manuals. For security classification guidance on threat, intelligence information, or information related to other DoD programs that may be included in information and materials produced under the DIB CS/IA program, refer to the appropriate published security classification guide or manual or the agency that originated the information in question.

d. DoD Components are responsible for validating compliance with this SCM for their specific contractor or industry support.

2. REASONS AND LENGTH OF CLASSIFICATION

a. Classification is reserved for specific categories of information, or the compilation of related information, meeting the standards and criteria for classification as defined in Reference (e) and DoD Manual 5200.01-V2 (Reference (m)).

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

3. CLASSIFICATION STANDARDS

a. Information and materials produced under the DIB CS/IA program must meet the standards for classification as cited in Reference (b) and implemented by Reference (e). When determining classification of information produced under the DIB CS/IA program, the OCA must determine whether:

(1) Information and materials produced under the DIB CS/IA program is owned by, produced by or for, or is under the control of the U.S. Government. In this context “control”

means the authority of the agency that originates the information, or its successor in function, to regulate access to the information.

(2) Information and materials produced under the DIB CS/IA program falls within one or more of the categories of information listed in References (b) and (e).

(3) Unauthorized disclosure of the information and materials produced under the DIB CS/IA program could reasonably be expected to result in damage to U.S. national security, which includes defense against transnational terrorism, and the OCA is able to identify or describe the damage.

b. Organizations that only reproduce, extract, or summarize classified information, or who apply classification markings derived from source material or as directed by a security classification guide or manual, need not possess original classification authority.

4. CLASSIFICATION BY COMPILATION

a. . A compilation of unclassified information is normally not classified. Information originating from contractors is unclassified. However, in certain circumstances, a compilation of unclassified information could become classified. If the compiled information infers an additional association or relationship that meets the standards for classification in Reference (e), then it could be classified because of the association revealed. When the OCA determines that classification by compilation is necessary, the OCA must provide an explicit explanation as to what elements of the compilation, when combined, require classification and the reason for classification and the proposed level of classification.

b. A compilation 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. 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 meets the criteria for a higher classification.

c. In accordance with References (e) and (m), when a document is classified by compilation, the overall classification must be marked conspicuously at the top and bottom of each page. An explanation for classification by compilation must be placed on the face of the document or in the text. If portions standing alone are unclassified, but the document is classified by compilation or association, mark the portions “U” and the document and pages with the classification of the compilation. The statements in Figure 1 must be used to explain the classification.

Figure 1. Classification Explanations

Classified by: DoD CIO or other OCA Reason: (Insert justification) Declassify on: (Enter appropriate date)* * 5 years for CONFIDENTIAL; 10 years for SECRET; 25 for TOP SECRET

5. EXCEPTIONAL CIRCUMSTANCES

a. A situation may arise where a holder of U.S. Government information has reason to believe:

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

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

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

b. Under such circumstances the information shall be marked with the anticipated level of classification and the notation "Pending Classification Review" and transmitted to the OCA for a classification determination.

6. CHALLENGES TO CLASSIFICATION

a. If holders of information have substantial reason to believe that the information is improperly or unnecessarily classified, they shall communicate those reasons to their security manager or the classifier of the information.

b. If any of the security classification guidance contained in this SCM is challenged, the items of information involved shall be protected at the higher level until the OCA renders a final decision on the challenge. Address classification challenges to the OCA, through the DIB CS/IA Program, via the activity security manager and the originator of the classified information.

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

d. Organizations wishing to classify DIB CS/IA-produced data (e.g., reports or threat products) at levels higher than the prescribed minimums listed in this SCM must submit to the OCA a letter detailing the justification for the increased level of classification. Include with the submission a means by which this data can be displayed and used at the prescribed level, and an assessment of whether all holders of the information can be notified of the change in classification. The OCA will review the submitted request and issue a formal adjudication within 60 days of receipt. If the decision is to upgrade the classification, the OCA shall notify all holders of the change in classification.

7. MARKING REQUIREMENT

a. Documents and other products covered by this SCM will be marked in accordance with References (b), (e), (m), and DoDD 5230.24 (Reference (n)).

b. When information is derivatively classified:

(1) Using this SCM as the source, markings should reflect the information in Figure 2.

Figure 2. Derivative Classification Markings

Classified by: (Use name and title or personal identifier of document author) Derived From: DoDM 5205.13, date Declassify On: (Use the date or event stated in the declass column of the appropriate topic in tables 1 through 6 of Enclosure 3 of DoDM 5205.13

(2) On the basis of more than one source document or classification guide, the marking should reflect the information in Figure 3. If "Multiple Sources" are used for a derivatively classified document, the derivative classifier shall include a listing of the source materials on, or attached to, the derivatively classified document.

Figure 3. Derivative Classification Markings (Multiple Sources)

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

8. FOREIGN GOVERNMENT INFORMATION

a. The U.S. Government affords protection to information provided by foreign governments. Classification designations for foreign government information in many cases do not parallel U.S. classification designations. Many foreign governments and international organizations have a fourth level of classification "Restricted", and a category of unclassified information that is

protected by the originating country and must be treated "in confidence". The portions of the document that contain the foreign government information shall be marked to indicate the government and classification level, using accepted country code standards. If information produced under the DIB CS/IA program contains foreign government information, follow the proper safeguarding, marking, and handling of foreign government information as directed in Reference (e).

b. NATO classified information shall be safeguarded in compliance with U.S. Security Authority for NATO Affairs Instruction 1-07 (Reference (o)).

9. RELEASE OF INFORMATION

a. Public Release

(1) Government unclassified information is not releasable to the public without review. DoD information requested or proposed for release shall be processed in accordance with DoDD 5230.09 (Reference (p)), DoDD 5230.25 (Reference (q)), DoDI 5230.29 (Reference (r)), DoD 5400.7-R (Reference (s)), DoDD 5400.07 (Reference (t)), and DoD 5205.02-M (Reference (u)).

(2) DoD shall take reasonable steps, by controlled access and need-to-know procedures, to protect against public release of DIB participant information. Full use of the exemptions of the DoD Freedom of Information Act (FOIA) Program (Reference (t)) shall be used to protect against disclosure of DIB participant information to unauthorized persons.

b. Release to U.S. Government Agencies and Contractors

(1) Classified DoD information will be released to U.S. Government agencies and contractors in accordance with References (e), (g), and (j).

(2) Based on this SCM, sensitive unclassified information, critical program information, proprietary information, or attribution information may be provided to other DoD Components, other U.S. Government agencies, and U.S. contractors only in accordance with the signed Framework Agreement 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." DIB attribution or proprietary information will be protected and distribution limited in accordance with the Framework Agreement, if applicable, and Federal statutes.

(3) Pursuant to this SCM, authority is delegated to the Heads of the Defense Criminal Investigative Organizations (DCIOs) to release information and materials produced under the DIB CS/IA program marked FOUO, to local U.S. law enforcement counterparts, when the release is required in the timely performance of law enforcement activities, and when accomplished in accordance with applicable law and regulations.

(4) Defense Cyber Crime Center (DC3) products for the DIB CS/IA program, incident reports, and cyber intrusion damage assessment documents prepared by DoD shall use

DISTRIBUTION STATEMENT F in Reference (n) as shown in Figure 4, as appropriate. Documents that are export controlled must have the required export controlled warning statement applied. In addition, the documents will be labeled with the appropriate FOIA exemption, in accordance with Reference (t).

Figure 4. Distribution Statements

Further distribution only as directed by DoD CIO in the DoD-DIB Framework for Cyber Security Information Sharing or higher DoD authority; [date].

c. Foreign Disclosure

(1) Classified information is a national security asset that shall be protected and shall be shared with foreign governments only when there is a clearly defined benefit to the U.S. Government. Disclosure to foreign officials of information classified by this SCM shall be in accordance with the procedures set forth in the National Disclosure Policy (Reference (v))as implemented in Reference (b), Reference (j), DoDD 5230.11 (Reference (w)), DoDD 5530.3 (Reference (x)), and in other established agreements.

(2) Release or disclosure to foreign officials of information and materials produced under the DIB CS/IA program is authorized only in accordance with this SCM or with DIB CS/IA policy or program guidance, including the Framework Agreement and must follow disclosure procedures in References (b), (e), (w), and (x). For law enforcement purposes only, after appropriate foreign disclosure review, DCIOs are authorized to release information and materials produced under the DIB CS/IA program marked FOUO to foreign law enforcement counterparts in accordance with applicable law and regulations.

d. CUI

(1) There are certain types of unclassified information that do not meet the standards and criteria for classification established in Reference (b), but for which Executive Branch agencies require application of controls and protective measures for a variety of reasons. This information is referred to collectively as CUI (see Glossary). E.O. 13556 (Reference (y)), establishes the National Archives and Records Administration as the Executive Agent for establishing a program for managing CUI. Upon establishment of the executive branch CUI program, CUI categories and subcategories shall serve as exclusive designations for identifying unclassified information throughout the executive branch that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies.

(2) FOUO is a designation applied to unclassified information (Reference (e)) that may be exempt from mandatory release to the public under the FOIA (Reference (t)). The 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 (s) for guidance on the FOIA exemptions. Once the CUI program is established, FOUO in this security classification manual shall be replaced with the appropriate CUI designation.

ENCLOSURE 3

CLASSIFICATION TABLES

1. Tables 1 through 6 provide security classification guidance for information and materials produced under the DIB CS/IA program. In each table:

a. Column 1 provides the specific element, item, or category of information to be protected.

b. Column 2 provides the minimum classification for those items listed in Column 1.

c. Columns 3 and 4 provide the reason for classification and the declassification specification in accordance with Reference (e).

d. Column 5 provides special marking and handling guidance and remarks.

2. If information is designated FOUO, a determination of which FOIA exemption applies must be made when the information is requested under the FOIA. For information and materials produced under the DIB CS/IA program, exemptions 2, 4, or 7 commonly apply.

3. The markings and classifications listed are the minimum to be applied. Data associated with a specific DoD classification level (e.g., SECRET) will be handled in accordance with References (b), (e), (g), (j), and (w). Network and information security requirements will be included in contracts via Federal Acquisition Regulations, Defense Federal Acquisition Regulations, the DD-254 "DoD Department of Defense Contract Security Classification Specification", and the "Addendum to DD Form 254 (Block 10j) FOR OFFICIAL USE ONLY."

4. When intelligence or information from another DoD program is involved, always refer to the originating intelligence or DoD program source, document, or security classification guidance for the proper (derivative) classification.

Table 1. Terms

TOPIC (Element, Item, Category of Information)	CLASSIFICATION	REASON (Reference (b))	DECLASS	REMARKS
The term and/or definition of "DIB CS/IA."	UNCLASSIFIED	N/A	N/A	
The term and/or definition of "Advanced Persistent Threat."	UNCLASSIFIED	N/A	N/A	
The term and/or definition of "Passive network security measure."	UNCLASSIFIED	N/A	N/A	
The term and/or definition of "DIB CS/IA Incident Report" or "Intrusion Event."	UNCLASSIFIED	N/A	N/A	
The term and/or definition of "DIB Cyber Intrusion Damage Assessment Report."	UNCLASSIFIED	N/A	N/A	
The term and/or definition of "Damage Assessment."	UNCLASSIFIED	N/A	N/A	

Table 2. General Information

TOPIC (Element, Item, Category of Information)	CLASSIFICATION	REASON (Reference (b))	DECLASS	REMARKS
DIB created network mapping or other collected network data on a DIB participant unclassified network provided to DoD.	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO. Use FOIA exemption (b)(4) Classification and special handling restrictions may be required and shall be applied if warranted by program, system, or operations planning classification guidance. General and specific Government provided information will be classified and handled in accordance with appropriate security classification guidance and other appropriate guidance. Consult appropriate classification guides.

Table 2. General Information, Continued

TOPIC (Element, Item, Category of Information)	CLASSIFICATION	REASON (Reference (b))	DECLASS	REMARKS
				• Proprietary information collected during collaboration with a DIB participant will be protected at a minimum as FOUO and handled in accordance with the Framework Agreement and the non-disclosure agreement (NDA), as applicable, with the respective DIB participant. Mark document with distribution statement as required by section 9 of Enclosure 2.
General budget information on DIB CS/IA activities (pre-decisional or pre-Program Objective Memorandum).	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO. Use FOIA exemption (b)(5). • Pre-decisional documents shall be marked "Unauthorized release of this document is prohibited." • NDA must be on file for non-Government access to specific planning, programming, budgeting, and execution data.
Specific budget information on DIB CS/IA activities (pre-decisional or pre-Program Objective Memorandum).	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO. Use FOIA exemption (b)(5). • Pre-decisional documents shall be marked "Unauthorized release of this document is prohibited." • NDA must be on file for non-Government access to specific planning, programming, budgeting, and execution data.

Table 2. General Information, Continued

TOPIC (Element, Item, Category of Information)	CLASSIFICATION	REASON (Reference (b))	DECLASS	REMARKS
An Advanced Persistent Threat (APT) cover name by itself or an abbreviation of a cover name.	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO. Use FOIA exemption high (b)(2). • Cover names are not generally used in unclassified channels because information becomes classified when the cover name is associated with many types of information. A cover name abbreviation should be treated in the same way as the cover name itself.
The broad concepts and general discussions associated with the DIB CS/IA activity.	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO if identifying a specific DIB participant unless the DIB participant has self-disclosed its identity. Use FOIA exemption (b)(4).
The fact that the DoD participates with the DIB to assist with improving the protection of its unclassified networks containing critical DoD unclassified information and network defense activities.	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO if identifying a specific DIB participant unless the DIB participant has self-disclosed its identity. Use FOIA exemption (b)(4). • DoD declines to provide the names of participating companies; it is the prerogative of individual companies if they choose to self-disclose their participation. Mark document with distribution statement as required by section 9 of Enclosure.
The fact that DC3 is involved and leverages, integrates, generates, disseminates and analyzes cyber threat information products, processes, and systems.	UNCLASSIFIED	N/A	N/A	• Information will be cleared for public release in accordance with References (p) and (r).

Table 2. General Information, Continued

TOPIC (Element, Item, Category of Information)	CLASSIFICATION	REASON (Reference (b))	DECLASS	REMARKS
The fact that DoD is evaluating, formulating polices for, and developing capabilities associated with DIB cyber security.	UNCLASSIFIED	N/A	N/A	• Information will be cleared for public release in accordance with References (p) and (r).
The fact that the Damage Assessment Management Office (DAMO) Case Management System tool is used to analyze files and data. (DAMO is located in the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics.)	UNCLASSIFIED	N/A	N/A	• Information will be cleared for public release in accordance with References (p) and (r).
Information on or a description of the cyber intrusion damage assessment process that would be found in flowcharts, project schedules, written descriptions, concepts of operations, and standard operating procedures.	UNCLASSIFIED	N/A	N/A	• Information will be cleared for public release in accordance with References (p) and (r).
The general fact that the DC3 Defense Computer Forensics Laboratory is analyzing a specific intrusion or doing digital forensics work.	UNCLASSIFIED	N/A	N/A	• Information will be cleared for public release in accordance with References (p) and (r).
Information revealing specifics of a DoD-led counterintelligence investigation of a DIB intrusion.	CONFIDENTIAL	1.4(c)	5 years	• Intelligence information will be classified in accordance with the appropriate intelligence classification guidance.
Information revealing specifics of a DoD led law enforcement investigation of a DIB intrusion.	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO. Use FOIA exemption (b)(7).

Table 3. Associations

TOPIC (Element, Item, Category of Information)	CLASSIFICATION	REASON (Reference (b))	DECLASS	REMARKS
DIB participant provided information associating domain name of attack source with IP address of attack source.	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO. Use FOIA exemption (b)(6). • General and specific Government provided information will be classified and handled in accordance with appropriate classification guidance.
Associating name of DIB participant or attribution information with a named APT.	SEE REMARKS	SEE REMARKS	SEE REMARKS	• Intelligence information will be classified in accordance with the appropriate intelligence classification guidance. • Mark and handle as FOUO if identifying a specific DIB participant. Use FOIA exemption (b)(4). • DoD declines to provide the names of participating companies; it is the prerogative of individual companies if they choose to self-disclose their participation. Mark document with distribution statement as required by section 9 of Enclosure 2.
Associating name of DIB participant(s) with a specific cyber intrusion damage assessment case number.	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO if identifying a specific DIB participant. Use FOIA exemption (b)(4). • DoD declines to provide the names of participating companies; it is the prerogative of individual companies if they choose to self-disclose their participation. Mark document with distribution statement as required by section 9 of Enclosure 2.

Table 4. Threats

TOPIC (Element, Item, Category of Information)	CLASSIFICATION	REASON (Reference (b))	DECLASS	REMARKS
Information revealing Foreign Intelligence Entity attribution or tools, tradecraft, or procedures, when derived from classified information, including classification resulting from the compilation of unclassified DoD information.	SECRET	1.4(c)	10 years	• Intelligence information will be classified in accordance with the appropriate intelligence classification guidance.
General information regarding a DIB CS/IA incident.	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO. Use FOIA exemption (b)(4).
General information about the transmittal of classified or unclassified cyber threat information products.	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO. Use FOIA exemption (b)(2).
Cyber threat information products.	SEE REMARKS	SEE REMARKS	SEE REMARKS	• Intelligence information will be classified in accordance with the appropriate intelligence classification guidance. • Mark and handle in accordance with Reference (j) and the guidance within the cyber threat information product; if unclassified, mark and handle as FOUO. Use FOIA exemption high (b)(2). • Sharing of cyber threat information products data, classified or unclassified, is restricted in accordance with the Framework Agreement.
The fact that an unnamed DIB participant has been exploited.	UNCLASSIFIED	N/A	N/A	• Information will be cleared for public release in accordance with References (p) and (r).

Table 4. Threats, Continued

TOPIC (Element, Item, Category of Information)	CLASSIFICATION	REASON (Reference (b))	DECLASS	REMARKS
The fact that a named DIB participant has been exploited.	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO. Use FOIA exemption (b)(4). • Strict "need to know" basis. • Intelligence information will be classified in accordance with the appropriate intelligence classification guidance. • DoD declines to provide the names of participating companies; it is the prerogative of individual companies if they choose to highlight their participation. Mark document with distribution statement as required by section 9 of Enclosure 2.
The fact that a DIB participant has been exploited and the tactics, techniques, and procedures (TTPs) identified: - Are not attributed to a specific adversary; or - When the TTPs are known via unclassified collection methods.	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO. Use FOIA exemption (b)(4). • Strict "need to know" basis. Limited distribution in accordance with the Framework Agreement. • Intelligence information will be classified in accordance with the appropriate intelligence classification guidance. • DoD declines to provide the names of participating companies; it is the prerogative of individual companies if they choose to highlight their participation. Mark document with distribution statement as required by section 9 of Enclosure 2.

Table 4. Threats, Continued

TOPIC (Element, Item, Category of Information)	CLASSIFICATION	REASON (Reference (b))	DECLASS	REMARKS
The fact a DIB participant has been exploited and the TTPs identified: - Are attributed to a specific adversary; or - When the TTPs are known via classified collection methods.	SECRET	1.4(c)	10 years	• Intelligence information will be classified in accordance with the appropriate intelligence classification guidance. • General and specific Government provided information will be classified and handled in accordance with appropriate security classification guidance. • DoD declines to provide the names of participating companies; it is the prerogative of individual companies if they choose to highlight their participation. Mark document with distribution statement as required by section 9 of Enclosure 2.

Table 5. Incident Reporting and Cyber Intrusion Damage Assessment (FOUO)

TOPIC (Element, Item, Category of Information)	CLASSIFICATION	REASON (Reference (b))	DECLASS	REMARKS
Information revealing Foreign Intelligence Entity attribution or TTPs, when derived from classified information, including classification resulting from the compilation of unclassified DoD information.	SECRET	1.4(c)	10 years	• Intelligence information will be classified in accordance with the appropriate intelligence classification guidance.
The title or existence of an intrusion event report, an interim compromise assessment, or a cyber intrusion damage assessment report (if the title does not reveal the status or conduct of the report in association with a DIB participant, intrusion, or exfiltration).	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO. Use FOIA exemption (b)(4). • Classification may be required if there is content or compilation of data as identified in this or other classification guides.
DIB participant generated report information about specific threat methodology.	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO. Mark document with distribution statement as required by section 9 of Enclosure 2. Use FOIA exemption (b)(4).
Information on intrusion event reported by DIB participant, to include: - Date(s)/time incident occurred or was discovered - Type of incident - Security category - Classification of information affected - Critical infrastructure affected - Description of attack - Method of detection - IP address of attacker(s) - Domain name of attacker(s) - Destination port(s) and protocol(s)	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO. Mark document with distribution statement as required by section 9 of Enclosure 2. Use FOIA exemption (b)(4). • Dissemination of incident reports (e.g., Incident Collection Forms, Consolidated Report Forms) will be in accordance with law and regulations, and the Framework Agreement.

Table 5. Incident Reporting and Cyber Intrusion Damage Assessment, Continued (FOUO)

TOPIC (Element, Item, Category of Information)	CLASSIFICATION	REASON (Reference (b))	DECLASS	REMARKS
- Suspected method of intrusion or attack - Suspected perpetrators or possible motivations - Name of Trojan(s) or malicious code(s) - Evidence of spoofing - Security structure in place - Number of machines affected - IP address of affected machine(s) - Domain name of affected machine(s) - Operating system(s) of affected machine(s) - Time of last patch of affected machine(s) - Functions of affected machine(s) - Application software affected - Damage to machine(s) if applicable				• DIB participant generated information reporting is transmitted via signed and encrypted email using DoD-approved PKI certificates in accordance with the Framework Agreement. If DoD-approved PKI is not available, transmission will be via landlines or other DoD-approved method. • Classification and special handling restrictions may be required and shall be applied if warranted by program, system, or operations planning classification guidance. Consult appropriate classification guides. • Intelligence information will be classified in accordance with the appropriate intelligence classification guidance. This includes methods of information collection employed in the intrusion. More information on this issue can be provided by DC3. • Any report of an intrusion involving classified information or systems must be reported to Defense Security Service (DSS) via procedures set forth in Reference (j).

Table 5. Incident Reporting and Cyber Intrusion Damage Assessment, Continued (FOUO)

TOPIC (Element, Item, Category of Information)	CLASSIFICATION	REASON (Reference (b))	DECLASS	REMARKS
Information associating a DIB participant with an intrusion event, interim compromise assessment reports, or with unclassified elements of a cyber intrusion damage assessment report that does not identify threat actors.	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO. Use FOIA exemption (b)(4). • Strict "need to know" basis. Limited distribution in accordance with the Framework Agreement. • Sharing of DIB participant attribution or proprietary information is protected in accordance with law and regulations, and the Framework Agreement. Mark document with distribution statement as required by section 9 of Enclosure 2.
Identification of potentially impacted DoD programs resulting from an unauthorized intrusion or compromise.	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO. Use FOIA exemption (b)(4). • Strict "need to know" basis. Limited distribution in accordance with the Framework Agreement. • Classification and special handling restrictions may be required and shall be applied if warranted by program, system, or operations planning classification guidance. Consult appropriate classification guides. • Mark document with distribution statement as required by section 9 of Enclosure 2.

Table 5. Incident Reporting and Cyber Intrusion Damage Assessment, Continued (FOUO)

TOPIC (Element, Item, Category of Information)	CLASSIFICATION	REASON (Reference (b))	DECLASS	REMARKS
Disk images of computers in support of incident investigations.	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO. Use FOIA exemption (b)(4). • Classify in accordance with the classification of the system or if required by other criteria such as if possession of disk images reveals classified associations, or if disks contain classified data. • Pursuant to Reference (j), DSS is responsible for incident investigation if the system is classified or if the disks contain classified information (other than coincidentally by compilation of unclassified information).
The fact that a cyber intrusion damage assessment was done, is ongoing, or will be conducted to determine damage impact to DoD programs.	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO. Use FOIA exemption high (b)(2).
Cyber Intrusion Damage assessment report, preliminary or final.	SECRET	1.4(g)	10 years	• Classification and special handling restrictions may be required and shall be applied if warranted by program, system, or operations planning classification guidance. Consult appropriate classification guides. • Mark document with distribution statement as required by section 9 of Enclosure 2. • Intelligence information will be classified in accordance with the appropriate intelligence classification guidance.

Table 5. Incident Reporting and Cyber Intrusion Damage Assessment, Continued (FOUO)

TOPIC (Element, Item, Category of Information)	CLASSIFICATION	REASON (Reference (b))	DECLASS	REMARKS
				• Consider compilation of data when classifying and, if applicable, use appropriate justification marking.
Details of the assessed loss or effects or impacts of the compromise to DoD program(s) or systems in the cyber intrusion damage assessment report, compromise impact assessment, or any other document or briefing.	SECRET	1.4(g)	10 years	• Classification and special handling restrictions may be required and shall be applied if warranted by program, system, or operations planning classification guidance. Consult appropriate classification guides. • Mark document with distribution statement as required by section 9 of Enclosure 2. Intelligence information will be classified in accordance with the appropriate intelligence classification guidance.
Details of loss or effects or impacts to the DIB participant infrastructure or information protection capability when such infrastructure or information protection capabilities do not involve information systems or networks that may impact or are used by DoD Components.	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO. Use FOIA exemption (b)(4). • Strict "need to know" basis. Limited distribution in accordance with the Framework Agreement. Mark document with distribution statement as required by section 9 of Enclosure 2.

Table 5. Incident Reporting and Cyber Intrusion Damage Assessment, Continued (FOUO)

TOPIC (Element, Item, Category of Information)	CLASSIFICATION	REASON (Reference (b))	DECLASS	REMARKS
Metrics or statistical facts that do NOT reveal details of loss or impact (e.g., amount of data analyzed, types of files, number of files, number of programs affected).	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO. Use FOIA exemption low (b)(2). • Mark document with distribution statement as required by section 9 of Enclosure 2.
DIB participant IP Address.	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO. Use FOIA exemption (b)(4).
DIB participant IP address paired with a vulnerability.	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO. Use FOIA exemption (b)(4). • Strict "need to know" basis. Mark document with distribution statement as required by section 9 of Enclosure 2.
Metrics or statistical facts that reveal details of loss of information or impact.	SECRET	1.4(g)	10 years	• Classification and special handling restrictions may be required and shall be applied if warranted by program, system, or operations planning classification guidance. Consult appropriate classification guides. • Mark document with distribution statement as required by section 9 of Enclosure 2. • Intelligence information will be classified in accordance with the appropriate intelligence classification guidance.

Table 5. Incident Reporting and Cyber Intrusion Damage Assessment, Continued (FOUO)

TOPIC (Element, Item, Category of Information)	CLASSIFICATION	REASON (Reference (b))	DECLASS	REMARKS
Periodic DIB participant status updates providing projected schedules, timelines, participants, general information, and assessment progress without revealing preliminary results.	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO. Use FOIA exemption (b)(4). • Mark document with distribution statement as required by section 9 of Enclosure 2.
Forensic assessment analysis reports.	SEE REMARKS	SEE REMARKS	SEE REMARKS	• Marking and handling instructions are as required by OCA. • Classify in accordance with applicable security classification guide.
The triage report or analysis revealing specific programs or DIB participants.	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO. Use FOIA exemption (b)(4). • Classification and special handling restrictions may be required and shall be applied if warranted by program, system, or operations planning classification guidance. Consult appropriate classification guides. • Mark document with distribution statement as required by section 9 of Enclosure 2. • Intelligence information will be classified in accordance with the appropriate intelligence classification guidance.

Table 6. Vulnerabilities

TOPIC (Element, Item, Category of Information)	CLASSIFICATION	REASON (Reference (b))	DECLASS	REMARKS
Information on vulnerabilities for commercial off-the-shelf (COTS) systems or components (hardware, firmware, or software) for which the vulnerability information is available within the public domain and there is no value-added analysis by a DoD Component.	UNCLASSIFIED	N/A	N/A	
Information on vulnerabilities for COTS systems or components (hardware, firmware, or software) for which the vulnerability information is not available within the public domain and there is value-added analysis by a DoD Component.	SECRET	1.4(g)	10 years	• Classification and special handling restrictions may be required and shall be applied if warranted by program, system, or operations planning classification guidance. Consult appropriate classification guides.
Information on unpatched vulnerabilities of DIB participant unclassified information systems or networks (including analysis or assessment).	UNCLASSIFIED	N/A	N/A	• Mark and handle as FOUO. Use FOIA exemption (b)(4). • Classification and special handling restrictions may be required and shall be applied if warranted by program, system, or operations planning classification guidance. Consult appropriate classification guides. • Mark document with distribution statement as required by section 9 of Enclosure 2.

GLOSSARY

PART I. ACRONYMS AND ABBREVIATIONS

APT	Advanced Persistent Threat
COTS	commercial off-the-shelf
CPI	Critical Program Information
CUI	controlled unclassified information
DAMO	Damage Assessment Management Office
DC3	DoD Cyber Crime Center
DCIP	Defense Critical Infrastructure Program
DCIO	Defense Criminal Investigative Organization
DIB	Defense Industrial Base
DIB CS/IA	Defense Industrial Base Cyber Security/Information Assurance
DoDD	DoD Directive
FOIA	Freedom of Information Act
FOUO	For Official Use Only
IA	information assurance
LES	Law Enforcement Sensitive
NDA	non-disclosure agreement
OCA	original classification authority
PKI	Public Key Infrastructure
RDA	research, development and acquisition
TTP	tactics, techniques and procedures

PART II. DEFINITIONS

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

adversary. A party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged.

APT. An extremely proficient, patient, determined, and capable adversary, including such adversaries working together.

attribution information (regarding a DIB participant). Information that identifies a company or its programs, whether directly or indirectly by the grouping of information that can be traced back to the company (e.g., program description, facility locations, number of personnel).

compilation. An arrangement of preexisting materials (e.g., facts and statistics) gathered from multiple sources into one document or other single repository, such as a database or data management system.

Critical Program Information. Elements or components of an RDA program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability. CPI includes information about applications, capabilities, processes, and end items; elements or components critical to a military system or network mission effectiveness; or technology that would reduce the U.S. technological advantage if it came under foreign control.

CUI. The designation "CUI" identifies information that does not meet the standards for national security classification consistent with Reference (b), but is pertinent to the national interest of the U.S. or to the important interests of entities outside the U.S. Government, and under law or policy requires protection from unauthorized access or disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. CUI includes information labeled "FOUO," "Sensitive But Unclassified (SBU)," "Drug Enforcement Agency Sensitive," and "Law Enforcement Sensitive (LES)." Mark and handle CUI, including FOUO and other sensitive information, in accordance with current DoD policy. See Reference (j) for further information.

cyber security. Includes preventing damage to, unauthorized use of, or exploitation of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; also includes restoring electronic information and communications systems in the event of a terrorist attack or natural disaster.

DIB. See Joint Publication 1-02 (Reference (z)).

DIB participant. Commercial company signatory of the Framework Agreement.