

§ 235.7

rental on property under DoD jurisdiction is sexually explicit. The Board members shall, to the extent practicable, maintain and update relevant information about material offered or to be offered for sale or rental on property under DoD jurisdiction.

(d) If any purchasing agent or manager of a retail outlet has reason to believe that material offered or to be offered for sale or rental on property under DoD jurisdiction may be sexually explicit as defined herein, and such material is not addressed by the Board's guidance issued pursuant to paragraph (e) of this section, he or she shall request a determination from the Board about such material prior to purchase or as soon as possible.

(e) At the conclusion of each review and, as necessary, the Board shall issue guidance to purchasing agents and managers of retail outlets about the purchase, withdrawal, and return of sexually explicit material. The Board may also provide guidance to purchasing agents and managers of retail outlets about material that it has determined is not sexually explicit. Purchasing agents and managers of retail outlets shall continue to follow their usual purchasing and stocking practices unless instructed otherwise by the Board.

(f) Material which has been determined by the Board to be sexually explicit may be submitted for reconsideration every 5 years. If substantive changes in the publication standards occur earlier, the purchasing agent or manager of a retail outlet under DoD jurisdiction may request a review.

§ 235.7 Information requirements.

The Chair of the Board shall submit to the PDUSD(P&R) an annual report documenting the activities, decisions, and membership of the Board. Negative reports are required. The annual report shall be due on October 1st of each year and is not subject to the licensing internal information requirements of DoD 8910.1-M.²

²Copies may be obtained at <http://www.dtic.mil/whs/directives/>.

32 CFR Ch. I (7-1-14 Edition)

PART 236—DEPARTMENT OF DEFENSE (DoD)—DEFENSE INDUSTRIAL BASE (DIB) VOLUNTARY CYBER SECURITY AND INFORMATION ASSURANCE (CS/IA) ACTIVITIES

- Sec.
- 236.1 Purpose.
- 236.2 Definitions.
- 236.3 Policy.
- 236.4 Procedures.
- 236.5 Cyber security information sharing.
- 236.6 General provisions.
- 236.7 DIB participant eligibility requirements.

AUTHORITY: 10 U.S.C. 2224; 44 U.S.C. 3506; 44 U.S.C. 3544.

SOURCE: 78 FR 62435, Oct. 22, 2013, unless otherwise noted.

§ 236.1 Purpose.

Cyber threats to DIB unclassified information systems represent an unacceptable risk of compromise of DoD information and pose an imminent threat to U.S. national security and economic security interests. DoD's voluntary DIB CS/IA program enhances and supplements DIB participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems.

§ 236.2 Definitions.

As used in this part:

(a) *Attribution information* means information that identifies the DIB participant, whether directly or indirectly, by the grouping of information that can be traced back to the DIB participant (e.g., program description, facility locations).

(b) *Compromise* means disclosure of information to unauthorized persons or a violation of the security policy of a system in which unauthorized intentional, or unintentional, disclosure, modification, destruction, loss of an object, or the copying of information to unauthorized media may have occurred.

(c) *Covered defense information* means unclassified information that:

(1) Is:

(i) Provided by or on behalf of the DoD to the DIB participant in connection with an official DoD activity; or

(ii) Collected, developed, received, transmitted, used, or stored by the DIB participant in support of an official DoD activity; and

(2) Is:

(i) Controlled Technical Information means technical information with military or space application (see 10 U.S.C. 130(c)) that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information is to be marked with one of the distribution statements B through F, in accordance with Department of Defense Instruction 5230.24, "Distribution Statements of Technical Documents." The term does not include information that is lawfully publicly available without restrictions. "Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data—Noncommercial Items" (48 CFR 252.227-7013). Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code;

(ii) Information subject to export control under the International Traffic in Arms Regulations (ITAR) (http://pmdtc.state.gov/regulations_laws/itar_official.html), or the Export Administration Regulations (EAR). (15 CFR part 730);

(iii) Information designated as Critical Program Information (CPI) in accordance with DoD Instruction 5200.39, "Critical Program Information (CPI) Protection within the Department of Defense";

(iv) Critical Information (Operations Security) includes specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Oper-

ations Security process as described in 5205.02-M, "DoD Operations Security (OPSEC Program Manual)";

(v) Personally Identifiable Information (PII) that can be used to distinguish or trace an individual's identity in accordance with DoD Directive 5400.11, "DoD Privacy Program";

(vi) Information bearing current and prior designations indicating controlled unclassified information (e.g., For Official Use Only, Sensitive But Unclassified, and Limited Official Use, DoD Unclassified Controlled Nuclear Information, Sensitive Information) that has not been cleared for public release in accordance with DoD Directive 5230.29, "Clearance of DoD Information for Public Release" (see also DoD 5200.01 M Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)"); ; or

(vii) Any other information that is exempt from mandatory public disclosure under DoD Directive 5400.07, "DoD Freedom of Information Act (FOIA) Program", and DoD Regulation 5400.7-R, "DoD Freedom of Information Program".

(d) *Covered DIB systems* means an information system that is owned or operated by or for a DIB participant and that processes, stores, or transmits covered defense information.

(e) *Cyber incident* means actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.

(f) *Cyber intrusion damage assessment* means a managed, coordinated process to determine the effect on defense programs, defense scientific and research projects, or defense warfighting capabilities resulting from compromise of a DIB participant's unclassified computer system or network.

(g) *Defense Industrial Base (DIB)* means the Department of Defense, Government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to satisfy military requirements.

(h) *DIB participant* means a DIB company that has met all of the eligibility

§ 236.3

32 CFR Ch. I (7–1–14 Edition)

requirements to participate in the voluntary DIB CS/IA information sharing program as set forth in this part (see § 236.7).

(i) *Government* means the United States Government.

(j) *Government Furnished Information (GFI)* means information provided by the Government under the voluntary DIB CS/IA program, including but not limited to cyber threat information and information assurance practices.

(k) *Information* means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

(l) *Information system* means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

(m) *Threat* means any circumstance or event with the potential to adversely impact organization operations (including mission, functions, image, or reputation), organization assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service.

(n) *U.S. based* means provisioned, maintained, or operated within the physical boundaries of the United States.

(o) *U.S. citizen* means a person born in the United States or naturalized.

§ 236.3 Policy.

It is DoD policy to:

(a) Establish a comprehensive approach for enhancing and supplementing DIB information assurance capabilities to safeguard covered defense information on covered DIB systems.

(b) Increase the Government and DIB situational awareness of the extent and severity of cyber threats to DoD information.

§ 236.4 Procedures.

(a) The Government and each DIB participant will execute a voluntary standardized agreement, referred to as a Framework Agreement (FA), to share, in a timely and secure manner,

on a recurring basis, and to the greatest extent possible, cyber security information relating to information assurance for covered defense information on covered DIB systems.

(b) Each such FA between the Government and a DIB participant must comply with and implement the requirements of this part, and will include additional terms and conditions as necessary to effectively implement the voluntary information sharing activities described in this part with individual DIB participants.

(c) DoD's DIB CS/IA Program Office is the overall point of contact for the program. The DoD Cyber Crime Center's DoD-DIB Collaborative Information Sharing Environment (DC3/DCISE) is the operational focal point for cyber threat information sharing and incident reporting under the DIB CS/IA program.

(d) The Government will maintain a Web site or other Internet-based capability to provide potential DIB participants with information about eligibility and participation in the program, to enable the online application or registration for participation, and to support the execution of necessary agreements with the Government. <http://dibnet.dod.mil/>.

(e) Prior to receiving GFI from the Government, each DIB participant shall provide the requisite points of contact information, to include security clearance and citizenship information, for the designated personnel within their company (e.g., typically 3–10 company designated points of contact) in order to facilitate the DoD-DIB interaction in the DIB CS/IA program. The Government will confirm the accuracy of the information provided as a condition of that point of contact being authorized to act on behalf of the DIB participant for this program.

(f) GFI will be issued via both unclassified and classified means. DIB participant handling and safeguarding of classified information shall be in compliance with the National Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22-M). The Government shall specify transmission and distribution procedures for all GFI, and shall inform DIB participants of any