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]

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

Sec.

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

[2] Copies may be obtained at *http://www.dtic.mil/whs/directives/*.

SOURCE: 77 FR 27618, May 11, 2012, 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) Technical information marked for restricted distribution in accordance with DoD Directive 5230.25, ''Withholding of Unclassified Technical Data From Public Disclosure,'' or DoD Directive 5230.24, ''Distribution Statements on Technical Documents'';

(ii) Information subject to export control under the International Traffic in Arms Regulations (ITAR) (*http://pmddtc.state.gov/regulations_laws/itar_official.html*), or the Export Administration Regulations (EAR) (*http://ecfr.gpoaccess.gov*, Title 15, 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) Information that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical intelligence in time to be useful to adversaries 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 unclassified controlled information (e.g., For Official Use Only, Sensitive But Unclassified, and Limited Official Use, DoD Unclassfied 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 Appendix 3 of DoD 5200.1–R, ''Information Security Program Regulation''); 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 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.

§ 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