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]

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

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://pmddtc.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 Operations 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

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

revisions to previously specified transmission or procedures.

(g) Except as authorized in this part or in writing by the Government, DIB participants may use GFI to safeguard covered defense information only on covered DIB systems that are U.S. based; and share GFI only within their company or organization, on a need to know basis, with distribution restricted to U.S. citizens. However, in individual cases, upon request of a DIB participant that has determined that it requires the ability to share the information with a non U.S. citizen, or to use the GFI on a non-U.S. based covered DIB system, and can demonstrate that appropriate information handling and protection mechanisms are in place, the Government may authorize such disclosure or use under appropriate terms and conditions.

(h) DIB participants shall maintain the capability to electronically disseminate GFI within the Company in an encrypted fashion (e.g., using Secure/Multipurpose Internet Mail Extensions (S/MIME), secure socket layer (SSL), Transport Layer Security (TLS) protocol version 1.2, DoD-approved medium assurance certificates).

(i) The DIB participants shall not share GFI outside of their company or organization, regardless of personnel clearance level, except as authorized in this part or otherwise authorized in writing by the Government.

(j) If the DIB participant utilizes a third-party service provider (SP) for information system security services, the DIB participant may share GFI with that SP under the following conditions and as authorized in writing by the Government:

(1) The DIB participant must identify the SP to the Government and request permission to share or disclose any GFI with that SP (which may include a request that the Government share information directly with the SP on behalf of the DIB participant) solely for the authorized purposes of this program;

(2) The SP must provide the Government with sufficient information to enable the Government to determine whether the SP is eligible to receive such information, and possesses the capability to provide appropriate protections for the GFI;

(3) Upon approval by the Government, the SP must enter into a legally binding agreement with the DIB participant (and also an appropriate agreement with the Government in any case in which the SP will receive or share information directly with the Government on behalf of the DIB participant) under which the SP is subject to all applicable requirements of this part and of any supplemental terms and conditions in the DIB participant's FA with the Government, and which authorizes the SP to use the GFI only as authorized by the Government.

(k) The DIB participant may not sell, lease, license, or otherwise incorporate the GFI into its products or services, except that this does not prohibit a DIB participant from being appropriately designated an SP in accordance with paragraph (j) of this section.

§ 236.5 Cyber security information sharing.

(a) *GFI.* The Government shall share GFI with DIB participants or designated SPs in accordance with this part.

(b) *Initial incident reporting.* The DIB participant shall report to DC3/DCISE cyber incidents involving covered defense information on a covered DIB system. These initial reports will be provided within 72 hours of discovery. DIB participants also may report other cyber incidents to the Government if the DIB participant determines the incident may be relevant to information assurance for covered defense information or covered DIB systems or other information assurance activities of the Government.

(c) *Follow-up reporting.* After an initial incident report, the Government and the DIB participant may voluntarily share additional information that is determined to be relevant to a reported incident, including information regarding forensic analyses, mitigation and remediation, and cyber intrusion damage assessments.

(d) *Cyber intrusion damage assessment.* Following analysis of a cyber incident, DC3/DCISE may provide information relevant to the potential or known compromise of DoD acquisition program information to the Office of the

Secretary of Defense's Damage Assessment Management Office (OSD DAMO) for a cyber intrusion damage assessment. The Government may provide DIB participants with information regarding the damage assessment.

(e) *DIB participant attribution information.* The Government acknowledges that information shared by the DIB participants under this program may include extremely sensitive proprietary, commercial, or operational information that is not customarily shared outside of the company, and that the unauthorized use or disclosure of such information could cause substantial competitive harm to the DIB participant that reported that information. The Government shall take reasonable steps to protect against the unauthorized use or release of such information (e.g., attribution information and other nonpublic information) received from a DIB participant or derived from such information provided by a DIB participant, including applicable procedures (see §236.5(h)). The Government will restrict its internal use and disclosure of attribution information to only Government personnel and Government support contractors that are bound by appropriate confidentiality obligations and restrictions relating to the handling of this sensitive information and are engaged in lawfully authorized activities.

(f) *Non-attribution information.* The Government may share non-attribution information that was provided by a DIB participant (or derived from information provided by a DIB participant) with other DIB participants in the DIB CS/IA program, and may share such information throughout the Government (including with Government support contractors that are bound by appropriate confidentiality obligations) for cyber security and information assurance purposes for the protection of Government information or information systems.

(g) *Electronic media.* Electronic media/files provided by DIB participants to DC3 under paragraphs (b), (c) and (d) of this section are maintained by the digital and multimedia forensics laboratory at DC3, which implements specialized handling procedures to maintain its accreditation as a digital and multimedia forensics laboratory. DC3 will maintain, control, and dispose of all electronic media/files provided by DIB participants to DC3 in accordance with established DoD policies and procedures.

(h) *Freedom of Information Act (FOIA).* Agency records, which may include qualifying information received from non-federal entities, are subject to request under the Freedom of Information Act (5 U.S.C. 552) (FOIA), which is implemented in the Department of Defense by DoD Directive 5400.07 and DoD Regulation 5400.7–R (see 32 CFR Parts 285 and 286, respectively). Pursuant to established procedures and applicable regulations, the Government will protect sensitive nonpublic information under this Program against unauthorized public disclosure by asserting applicable FOIA exemptions, and will inform the non-Government source or submitter (e.g., DIB participants) of any such information that may be subject to release in response to a FOIA request, to permit the source or submitter to support the withholding of such information or pursue any other available legal remedies.

§236.6 General provisions.

(a) Confidentiality of information that is exchanged under this program will be protected to the maximum extent authorized by law, regulation, and policy.

(b) The Government and DIB participants will conduct their respective activities under this program in accordance with applicable laws and regulations, including restrictions on the interception, monitoring, access, use, and disclosure of electronic communications or data. The Government and the DIB participant each bear responsibility for their own actions under this program.

(c) Prior to sharing any information with the Government under this program pursuant to the FA, the DIB participant shall perform a legal review of its policies and practices that support its activities under this program, and shall make a determination that such policies, practices, and activities comply with applicable legal requirements.

(d) This voluntary DIB CS/IA program is intended to safeguard covered

defense information. None of the restrictions on the Government's use or sharing of information under the DIB CS/IA program shall limit the Government's ability to conduct law enforcement, counterintelligence activities, or other activities in the interest of national security; and participation does not supersede other regulatory or statutory requirements.

(e) Participation in the DIB CS/IA program is voluntary and does not obligate the DIB participant to utilize the GFI in, or otherwise to implement any changes to, its information systems. Any action taken by the DIB participant based on the GFI or other participation in this program is taken on the DIB participant's own volition and at its own risk and expense.

(f) A DIB participant's voluntary participation in this program is not intended to create any unfair competitive advantage or disadvantage in DoD source selections or competitions, or to provide any other form of unfair preferential treatment, and shall not in any way be represented or interpreted as a Government endorsement or approval of the DIB participant, its information systems, or its products or services.

(g) The DIB participant and the Government may each unilaterally limit or discontinue participation in this program at any time. Termination shall not relieve the DIB participant or the Government from obligations to continue to protect against the unauthorized use or disclosure of GFI, attribution information, contractor proprietary information, third-party proprietary information, or any other information exchanged under this program, as required by law, regulation, contract, or the FA.

(h) Upon termination of the FA, and/or change of Facility Security Clearance status below Secret, GFI must be returned to the Government or destroyed pursuant to direction of, and at the discretion of, the Government.

(i) Participation in this program does not abrogate the Government's or the DIB participants' rights or obligations regarding the handling, safeguarding, sharing, or reporting of information, or regarding any physical, personnel, or other security requirements, as required by law, regulation, policy, or a valid legal contractual obligation.

§ 236.7 DIB participant eligibility requirements.

To be eligible to participate in this program, a DIB company must:

(a) Have or acquire DoD-approved medium assurance certificates to enable encrypted unclassified information sharing between the Government and DIB participants;

(b) Have an existing active Facility Security Clearance (FCL) granted under the National Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22–M) with approved safeguarding for at least Secret information, and continue to qualify under the NISPOM for retention of its FCL and approved safeguarding (*http://www.dtic.mil/whs/directives/corres/pdf/522022m.pdf*);

(c) Have or acquire a Communication Security (COMSEC) account in accordance with the NISPOM Chapter 9, Section 4 (DoD 5220.22–M), which provides procedures and requirements for COMSEC activities;

(d) Obtain access to DoD's secure voice and data transmission systems supporting the DIB CS/IA program,

(e) Own or operate covered DIB system(s), and

(f) Execute the standardized FA with the Government (available during the application process), which implements the requirements set forth in §§ 236.4 through 236.6.

PART 237a—PUBLIC AFFAIRS LIAISON WITH INDUSTRY

Sec.

AUTHORITY: 5 U.S.C. 301.

SOURCE: 35 FR 10889, July 7, 1970, unless otherwise noted.

§ 237a.1 Purpose.

This part establishes (a) guidance for preparation of the Defense Industry Bulletin, and (b) includes guidance and procedures governing Department of Defense cooperation with industry on (1) public affairs matters in general, (2)