(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

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 (i.e., provisioned, maintained, or operated within the physical boundaries of the United States); and share GFI only within their company or organization, on a need to know basis, with distribution restricted to U.S. citizens (i.e., a person born in the United States, or naturalized, holding a U.S. passport). 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 pursuant to paragraph (h) of this section. 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.