



<RULE>

<PREAMB>

DEPARTMENT OF DEFENSE

BILLING CODE 5001-06

Office of the Secretary

32 CFR Part 236

DOD-2009-OS-0183/RIN 0790-AI60

Department of Defense (DoD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities

AGENCY: Office of the DoD Chief Information Officer, DoD.

ACTION: Interim final rule.

SUMMARY: DoD is publishing an interim final rule to establish a voluntary cyber security information sharing program between DoD and eligible DIB companies. The program enhances and supplements DIB participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems.

DATES: This rule is effective [insert date of publication in the Federal Register]. Comments must be received by [insert 60 days from date of publication in the Federal Register].

ADDRESSES: You may submit comments, identified by docket number and/or RIN number and title, by any of the following methods:

- Federal Rulemaking Portal: <http://www.regulations.gov>. Follow the instructions for submitting comments.
- Mail: Federal Docket Management System Office, 4800 Mark Center Drive, East Tower, Suite 02G09, Alexandria, VA 22350-3100.

Instructions: All submissions received must include the agency name and docket number or Regulatory Information Number (RIN) for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at <http://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: DIB Cyber Security and Information

Assurance Program Office: (703) 604-3167, toll free (855) 363-4227, email

DIB.CS/IA.Reg@osd.mil.

SUPPLEMENTARY INFORMATION:

Background.

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.

This rule is being published as an interim final rule to:

- (a) Allow eligible DIB companies to receive USG threat information and share information about network intrusions that could compromise critical DOD programs and missions.
- (b) Permit DIB companies and DOD to assess and reduce damage to critical DOD programs and missions when DOD information is compromised.
- (c) Fulfill statutory requirements to ensure the protection of DOD information.
- (d) Address vigorous congressional and public interest in increasing cyber security and information assurance activities through government-industry cooperation.

(e) Immediately provide a voluntary framework for DOD and DIB companies to share information to address sophisticated cyber threats that represent an imminent threat to U.S. national security and economic security interests.

Until this rule is published as an interim final rule, eligible DIB companies cannot receive USG information about cyber threats and mitigation strategies or share information about cyber incidents that may compromise critical DOD programs and missions. Without this information, eligible DIB companies' ability to protect USG information cannot be fully effective. While this vulnerability remains open, the USG faces an elevated risk that critical program information could be compromised, resulting in potential economic losses or damage to U.S. national security. For example, the compromise of such information can significantly diminish return on DIB company and U.S. Government research and development investment and represents a loss of intellectual property that compromises the security and technical advantages of DoD weapons systems.

DIB CS/IA activities, including the collection, management and sharing of information for cyber security purposes, support and implement the following national and DoD-specific guidance and authority: information assurance (IA) requirements to establish programs and activities to protect DoD information and DoD information systems, including information and information systems operated and maintained by contractors or others in support of DoD activities (see 10 U.S.C. § 2224; and the Federal Information Security Management Act (FISMA), codified at 44 U.S.C. §§ 3541 et seq.); critical infrastructure protection responsibilities, in which DoD is the sector specific agency for the DIB sector, (see Homeland Security Presidential Directive 7 (HSPD-7), "Critical Infrastructure Identification, Prioritization, and Protection").

The DoD established the voluntary DIB CS/IA program to enhance and supplement DIB participant's capabilities to safeguard DoD unclassified information that resides on, or transits, DIB unclassified information systems. At the core of the program is a bilateral cyber security information sharing activity, in which DoD provides cyber threat information and information assurance (IA) best practices to DIB companies to enhance and supplement DIB companies' capabilities to safeguard DoD unclassified information; and in return, DIB companies report certain types of cyber intrusion incidents to the Defense Cyber Crime Center's DoD-DIB Collaborative Information Sharing Environment (DCISE), DoD's operational focal point for cyber threat information sharing and incident response under this program. The DoD analyzes the information reported by the DIB company regarding any such cyber incident, to glean information regarding cyber threats, vulnerabilities, and the development of effective response measures. In addition to this initial reporting and analysis, the DoD and DIB company may pursue, on a voluntary basis, follow-on, more detailed, digital forensics analysis or damage assessments of individual incidents, including sharing of additional electronic media/files or information regarding the incident or the affected systems, networks, or information. The information sharing arrangements between the DoD and each participating DIB company are memorialized in a standardized bilateral Framework Agreement (FA), signed by the participating DIB company and the Government, that implements the requirements of this part and is signed by the participating DIB company and the Government. The FA is available to eligible DIB companies during the application process. As provided by the FA, participation in the program is entirely voluntary and does not obligate any DIB participant change its information systems or otherwise alter its normal conduct of cyber security activities. In keeping with the voluntary, collaborative nature of the activity described in the FA, each Party bears responsibility for its

own actions under this FA. The FA emphasizes sharing to the greatest extent possible information to provide the clearest understanding of the cyber threat. This will allow the Company to improve defense and remediation efforts and allow the Government to assess the damage or impact to defense information and programs entrusted to the Company.

A foundational element of this bilateral information sharing model is the recognition that the information being shared between the parties includes extremely sensitive nonpublic information, which must be protected against unauthorized uses and disclosures in order to preserve the integrity of the program. For example, the cyber threat information shared by the Government must be protected against compromise by the cyber threat, which may already have a presence on the DIB participant's system; and thus the DIB participants must utilize security measures and limited sharing within the company, to ensure that the cyber threat information retains its operational value--for the benefit of all of the DIB participants. Similarly, the DIB participants typically treat information regarding potential cyber intrusion incidents on their networks as extremely sensitive proprietary, commercial, or operational information and tightly control that information within the company, let alone sharing outside the company. The DIB participants share this type of information with the Government only on the condition that the Government safeguards that information against any unauthorized use or release (both within the Government and outside the Government), which could cause substantial competitive harm to the DIB participant that reported that information. In addition, during any follow-on forensics or damage assessment activities, the Government and DIB companies may share additional types of sensitive information, which may include information regarding the types of DoD information or DIB company information that may have been compromised during the reported incident – potentially including the most sensitive types of unclassified information (e.g., critical program

information relating to DoD weapons systems, DIB company trade secrets related to DoD programs, personally identifiable information (PII) regarding individuals). For additional information regarding the Government's safeguarding of information received from the DIB companies, with specific focus on PII, see the Privacy Impact Assessment for the DIB CS/IA Program (http://dodcio.defense.gov/Portals/0/Documents/DIB%20CS-IA%20PIA_FINAL_signed_30jun2011_VMSS_GGMR_RC.pdf).

As part of DoD's instantiation of the voluntary DIB CS/IA program, DoD developed new policies and procedures, developed a dedicated threat sharing and collaboration system, and validated on-line application procedures in order to support participation by a large number of companies. The on-line application procedures provide the administrative and security requirements for DIB participants, including the standardized bilateral FA that implements the requirements of the DIB CS/IA program. The FA will typically be executed by a senior DoD official, such as the DoD Chief Information Officer (CIO), and by a DIB company corporate senior official (e.g., Company CIO or equivalent).

This interim-final rule establishes a new part 236 in title 32 of the Code of Federal Regulations, with the following new sections: Section 236.2 establishes the definitions of terms used in the new part, leveraging established definitions to the maximum extent possible (e.g., those provided in the Committee on National Security Systems Instruction No. 4009, "National Information Assurance Glossary") (http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf); Section 236.4 sets forth the basic requirements and procedures of the voluntary program, including information collection requirements; Section 236.5 characterizes cyber security information sharing and collection procedures; Section 236.6 establishes the general provisions of the voluntary DIB

CS/IA program; and Section 236.7 sets forth the eligibility requirements to participate in the voluntary program.

Nothing in this rule or program is intended to be inconsistent with any other related or similar federal agency or private sector activity or requirement. For example, nothing in this rule or program abrogates 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.

Similarly, this rule and program are intended to be consistent and coordinated with, and updated as necessary to ensure consistency with and support for, other federal activities related to the handling and safeguarding of controlled unclassified information, such as those that are being led by the National Archives and Records Administration pursuant to Executive Order 13556 "Controlled Unclassified Information" (November 4, 2010) (see <http://www.archives.gov/cui/>).

Executive Orders 12866, "Regulatory Planning and Review" and 13563, "Improving Regulation and Regulatory Review"

It has been certified that 32 CFR part 236 does not:

- (a) Have an annual effect on the economy of \$100 million or more, or adversely affect in a material way, the economy; a section of the economy; productivity; competition; jobs; the environment; public health or safety; or State, local, or tribal governments or communities;
- (b) Create a serious inconsistency, or otherwise interfere with, an action taken or planned by another Agency;
- (c) Materially alter the budgetary impact of entitlements, grants, user fees, or loan programs, or the rights and obligations of recipients thereof; or

(d) Raise novel legal or policy issues arising out of legal mandates, the President’s priorities, or the principles as set forth in these Executive Orders.

Public Law 104-121, “Congressional Review Act” (5 U.S.C. 801)

It has been determined that 32 CFR part 236 is not a “major” rule under 5 U.S.C. 801, enacted by Public Law 104-121, because it will not result in an annual effect on the economy of \$100 million or more; a major increase in costs or prices for consumers, individual industries, Federal, State, or local government agencies, or geographic regions; or significant adverse effects on competition, employment, investment, productivity, innovation, or on the ability of United States-based enterprises to compete with foreign-based enterprises in domestic and export markets.

Sec. 202, Public Law 104-4, “Unfunded Mandates Reform Act”

It has been certified that 32 CFR part 236 does not contain a Federal mandate that may result in expenditure by State, local and tribal governments, in aggregate, or by the private sector, of \$100 million or more in any one year.

Public Law 96-354, “Regulatory Flexibility Act” (5 U.S.C. 601)

It has been certified that 32 CFR part 236 is not subject to the Regulatory Flexibility Act (5 U.S.C. 601) because it would not, if promulgated, have a significant economic impact on a substantial number of small entities. DIB participation in the DIB CS/IA Program is voluntary.

Public Law 96-511, “Paperwork Reduction Act” (44 U.S.C. Chapter 35)

Sections 236.4 and 236.5 and 236.7 of this interim final rule contain information collection requirements. DoD has submitted the following proposal to Office of Management and Budget (OMB) under the provisions of the Paperwork Reduction Act (44 U.S.C. Chapter 35).

Comments are invited on: (a) whether the proposed collection of information is necessary for

the proper performance of the functions of DoD, including whether the information will have practical utility; (b) the accuracy of the estimate of the burden of the proposed information collection; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the information collection on respondents, including the use of automated collection techniques or other forms of information technology.

(a) Title: *Defense Industrial Base Cyber Security/Information Assurance (DIB CS/IA) Points of Contact Information*

Type of Request: New..

Projected Responses Per Respondent: One response is required initially and thereafter only on an “as needed/required” basis, as changes to the points of contact occur.

Annual Responses: 275, which includes the additional responses required on an “as needed/required” basis.

Average Burden Per Response: 20 minutes.

Annual Burden Hours: Total annual burden for respondents 92 hours.

Total Annualized Cost to Respondents: One-time cost of ~\$12 per respondent. Total cumulative annual cost for 250 respondents (275 responses) is \$3,337.

Needs and Uses: The DIB CS/IA program collects Point of Contact (POC) information from DIB participants. POC information is needed to facilitate communication between DoD and DIB participants, as well as prospective participants. The POC information includes the names, security clearance information, citizenship, work addresses, including division/group, work email addresses and work telephone numbers of company-identified representatives. DIB POCs include the Chief Executive Officer (CEO), Chief Information Officer (CIO), Chief Information Security Officer (CISO), General Counsel, the Chief Privacy Officer, and the Corporate Security

Officer (CSO) or Facility Security Officer (FSO), or their equivalents. DIB participants also provide POC information for personnel responsible for the implementation and execution of the DIB CS/IA program within their company including designated personnel authorized to report incidents and any policy, administrative, or technical personnel identified to interact with DOD in the operational implementation of the program.

Affected Public: Business or other for-profit and not-for-profit institutions participating in the voluntary DIB CS/IA program.

Frequency: On occasion.

Respondent's Obligation: Voluntary.

(b) Title: *DIB Cyber Security/Information Assurance Cyber Incident Reporting*

Type of Request: New.

Phased expansion of DIB CS/IA Number of Participants increases to 750 over three years.

Projected Responses Per Participant: 5.

Annual Responses: Year 1 responses are 1,250. Year 2 responses are 2,500. Year 3 responses are 3,750.

Average Burden Per Response: 7 hours (this includes searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information).

Annual Burden Hours: Year 1 burden hours are 8,750 hours. Year 2 burden hours are 17,500 hours. Year 3 burden hours are 26,250 hours.

Needs and Uses: The collection of this information is necessary to enhance and supplement DIB participants' information security capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems. The requested information supports the information assurance objectives, cyber threat information sharing, and incident reporting

between DoD and the DIB participants. In most cases, DIB participants report incidents using a DIB CS/IA standardized Incident Collection Form (ICF). In some cases, a company may elect to report the incident without using the ICF; and companies may report incidents through a variety of communications channels, including email, fax, or by phone, if necessary.

Affected Public: Business or other for-profit and not-for-profit institutions participating in the DIB CS/IA program.

Frequency: On occasion.

Respondent's Obligation: Voluntary.

OMB Desk Officer:

Written comments and recommendations on the information collection should be sent to Ms Jasmeet Seehra at the Office of Management and Budget, DoD Desk Officer, Room 10102, New Executive Office Building, Washington, DC 20503, with a copy to the Director, DIB CS/IA Program Office, at the Office of the DoD Chief Information Officer, 6000 Defense Pentagon, Attn: DIB CS/IA Program Office, Washington, D.C. 20301, or email at DIB.CS/IA.Reg@osd.mil. Comments can be received from 30 to 60 days after the date of this notice, but comments to OMB will be most useful if received by OMB within 30 days after the date of this notice.

You may also submit comments, identified by docket number and title, by the following method:
Federal Rulemaking Portal: <http://www.regulations.gov>. Follow the instructions for submitting comments.

Instructions: All submissions received must include the agency name, docket number and title for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the

Internet at <http://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

To request more information on this information collection or to obtain a copy of the proposal and associated collection instruments, please write to Director, DIB CS/IA Program Office, at Office of the DoD Chief Information Officer, Attn: DIB CS/IA Program Office, 6000 Defense Pentagon, Washington, D.C. 20301.

Executive Order 13132, “Federalism”

It has been certified that 32 CFR part 236 does not have federalism implications, as set forth in Executive Order 13132. This rule does not have substantial direct effects on:

- (a) The States;
- (b) The relationship between the National Government and the States; or
- (c) The distribution of power and responsibilities among the various levels of Government.

List of Subjects in 32 CFR Part 236

Contracts, Security measures.

Accordingly 32 CFR Part 236 is added to read as follows:

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.

§ 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://pmdtc.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 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 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 website 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.

(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. The Government may request from any DIB participant additional information or assurances regarding such DIB participant's policies or practices, or the determination by the DIB participant that such policies or practices 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 sections 236.4 through 236.6 of this part.

DATED: April 30, 2012.

PATRICIA L. TOPPINGS

OSD Federal Register

Liaison Officer

Department of Defense

<FRDOC> [FR Doc. 2012-10651 Filed 5-2-12; 8:45 am]

<BILCOD>BILLING CODE 5001-06-P

[FR Doc. 2012-10651 Filed 05/10/2012 at 8:45 am; Publication Date: 05/11/2012]