BILLING CODE 5001-06

DEPARTMENT OF DEFENSE

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: Final rule.

SUMMARY: This final rule responds to public comments regarding the establishment of the DIB CS/IA program, 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.

EFFECTIVE DATE: This rule is effective [INSERT 30 DAYS FROM DATE OF PUBLICATION IN THE FEDERAL REGISTER].

FOR FURTHER INFORMATION CONTACT: Mr. Dan Prieto at 703-571-5911, or the DIB Cyber Security and Information Assurance Program Office: (703) 604-3167, toll free (855) 363-4227, email osd.ncr.dod-cio.mbx.dib-cs-ia-program-registration@mail.mil.

SUPPLEMENTARY INFORMATION:

Executive Summary

This final rule responds to public comments regarding the establishment of the DIB CS/IA program, a voluntary cyber security information sharing activity between DoD and eligible DIB

companies to enhance and supplement DIB participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems.

The program is codified at 32 CFR Part 236 and implements DoD statutory authorities 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.). It also fulfills important elements of DoD's critical infrastructure protection responsibilities, as the sector specific agency for the DIB sector see (Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience"). This program allows eligible DIB companies to receive U.S. Government (USG) threat information and to share information about network intrusions that could compromise DoD programs and missions. In addition, the program permits DIB companies and DoD to assess and reduce damage to DoD programs and missions when DoD information is potentially compromised. Furthermore, the information sharing arrangements between the DoD and each participating DIB company that implement the requirements of this are memorialized in a standardized bilateral agreement, known as a Framework Agreement (FA), signed by the participating DIB company and the Government.

The rule also provides the eligibility requirements for a company to participate in the DIB CS/IA program.

Costs for DIB participants include obtaining access to DoD's secure voice and data transmission systems supporting the DIB CS/IA program and acquiring DoD approved medium assurance certificates. There also are costs associated with the collection requirements for providing point

of contact information and cyber incident reporting. Government costs include onboarding new companies and collecting and analyzing cyber incidents from DIB participants.

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 additional information regarding the Government's safeguarding of information received from the DIB companies, with specific focus on PII, see the Privacy Impact Assessment (PIA) for the DIB CS/IA Program (http://dodcio.defense.gov/Portals/0/Documents/DIB%20CS-IA%20PIA_FINAL_signed_30jun2011_VMSS_GGMR_RC.pdf).

In addition, 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/).

This rule is not intended to implement the new requirements from section 941 of the National Defense Authorization Act for Fiscal Year 2013.

Comments

DoD published an interim final rule on May 11, 2012 (77 FR 27615). Fifty comments from twelve respondents were received and reviewed by the USG.

Comment: Four comments questioned the eligibility and scope of the program, to include recommending that the program remain voluntary, and questioning whether the program was

"under inclusive or overly restrictive because the program is only available to companies that have a Facility Security Clearance and a Communications Security account."

Response: The DIB CS/IA program will remain a voluntary program to enhance and supplement DIB participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems. The eligibility requirements for the program (§ 236.7) are based on security requirements to ensure the protection of Government furnished information (GFI) at DIB companies in possession of DoD information, as described in the definition for "covered defense information," (§ 236.2(c)). No change is made to the rule.

Comment: One comment asserted that the rule should not have been published as an interim rule.

Response: In light of the growing cyber threat activity against DoD information and DIB information systems and the associated risk to U.S. national security, the Government determined it appropriate to issue an interim rule. This allowed eligible DIB companies to receive cyber threat information, without delay in order to enhance their capability to defend against ongoing and continuous cyber threats and to safeguard DoD information. No change is made to the rule.

Comment: One comment asserted that the Framework Agreement (FA) should be available for public review to evaluate the estimates of projected paperwork for participants.

Response: The Framework Agreement is a representation of the federal rule converted into an agreement format for implementation of the program. In addition, all information required to evaluate the projected cost and time for the information collection requirements is available in the rule. No change is made to the rule.

Comment: One comment asserted that transparency into public-private cyber security programs is crucial to ensure that federal agencies respect privacy rights and comply with their obligations.

Response: Extensive coordination across the Government has ensured that the privacy rights of U.S. citizens are protected under the DIB CS/IA voluntary program, including developing a comprehensive Privacy Impact Assessment (PIA) for the DIB CS/IA program. The PIA is publically available at: http://dodcio.defense.gov/Portals/0/Documents/DIB%20CS-IA%20PIA_FINAL_signed_30jun2011_VMSS_GGMR_RC.pdf. No change is made to the rule.

Comment: One comment asserted that the Defense Department opted to issue a rule even though no law has been passed by Congress regarding Government-industry cyber security activities and that rulemaking should come after Congress concludes its legislative efforts.

Response: The rule implements DoD statutory authorities and responsibilities to establish a program to protect DoD information and information systems, including 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.). No change is made to the rule.

Comment: Three comments asserted the rule should create an oversight and accountability structure that includes public, congressional, and executive branch reporting. One comment recommended using DHS oversight procedures as a model to ensure the program's compliance with regulations and relevant guidelines.

Response: The DIB CS/IA program is subject to numerous procedures, requirements, and oversight to ensure compliance with DoD and national policies for collecting, handling,

safeguarding, and sharing sensitive information with non-Government organizations in accordance with DoD Directive 5500.1, DoD Privacy Program and 5400.11-Regulation, Department of Defense Privacy Program, which proscribes uniform procedures for the DoD Privacy Program. 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 (PIA) for the DIB CS/IA Program (http://DoDcio.defense.gov/Portals/0/Documents/DIB%20CS-IA%20PIA_FINAL_signed_30jun2011_VMSS_GGMR_RC.pdf). In addition, DoD annually reports to Congress on the progress of DoD in defending the DoD and the Defense Industrial Base from cyber events. No additional oversight is warranted at this time. No change is made to the rule.

Comment: One comment recommended distinguishing between classified and unclassified GFI, and that classified GFI should be handled per the NISPOM.

Response: As stated in § 236.4(f) of the rule, GFI will be issued via both unclassified and classified means, and that handling and safeguarding of classified GFI shall be in compliance with the National Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22-M). No change is made to the rule.

Comment: One comment recommended not to apply sharing limitations under the rule to non-sensitive GFI.

Response: As defined in the rule at § 236.2(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." GFI is typically nonpublic information that is sensitive based either on the content of the information itself or the context in which the information is relevant (e.g., cyber threat information).

Accordingly, the handling requirements applicable to GFI are designed to protect sensitive information. No change is made to the rule.

Comment: Three comments requested a narrow interpretation of the Freedom of Information Act (FOIA) exemptions, and one asked that the records not be exempted under Privacy Act provisions.

Response: As recognized in the Background section of the Interim Rule (77 FR 27615, at 27616), a foundational element of this program is the recognition that the information being shared includes extremely sensitive nonpublic information. This includes the GFI shared by the Government, as well as the information regarding cyber incidents that is shared by the DIB participants, which they typically treat as extremely sensitive proprietary, commercial, or operational information for which release and dissemination is tightly controlled. Accordingly, as stated in § 236.6 of the rule, confidentiality of such sensitive information exchanged under this program will be protected to the maximum extent authorized by law, regulation, and policy. This includes taking appropriate measures, including the use of any applicable exemptions under FOIA or the Privacy Act, to safeguard against unauthorized public disclosure and in full compliance with applicable laws, regulations, policies, and procedures (see § 236.2(c)(2)(vii) and § 236.5(h)). No change is made to the rule.

Comment: Four comments addressed DoD working with private contractors without appropriate safeguards for privacy rights, maintaining a database on law abiding Americans and subverting due process and gathering information about an unsuspecting populace.

Response: The DIB CS/IA program focuses on sharing cyber security related information and minimizes the collection of information from participating DIB companies, seeking only the information that is necessary to support this cyber security program. The PIA for the DIB CS/IA

program details the comprehensive processes to safeguard PII. The operational implementation of the DIB CS/IA program receives PII from DIB Companies in two ways: (i) for program administration and management purposes, the DIB companies share with DoD the typical business contact information for its personnel that are serving as company points of contact for the program activities or specific cyber incidents; and (ii) for cyber incident response and analysis purposes, DIB companies may share PII as a necessary part of the information that they have determined is relevant to cyber incident response, analysis, or damage assessment. In addition, DIB companies are prohibited from sharing any information unless they have determined that the information has been lawfully collected and is authorized to be shared with DoD. The DIB CS/IA Program restricts access to such PII and attribution information only to those authorized personnel who have a need-to-know such information for duties in support of the DIB CS/IA Program and are subject to strict nondisclosure obligations. The PII is only maintained as long as necessary for DIB CS/IA Program activities, and is managed and disposed of in accordance with applicable records management requirements. No change is made to the rule.

Comment: One comment stated that the rule allows a number of private companies to sell and share private citizens' data including to other Governments, including "any data that 'transits' any government system."

Response: The voluntary DIB CS/IA program does not authorize participating companies to sell any information, to anyone, in any context whatsoever. The program also does not authorize DIB companies to share any information with anyone other than program participants. The program does not permit the sharing of information with any governments other than authorized U.S. Government participants. No change is made to the rule.

Comment: One comment stated that the rule does not properly ensure implementation of the new Controlled Unclassified Information (CUI) framework from Executive Order 13556 into its treatment of covered defense information.

Response: As stated in the Background Section above, the program is designed to ensure consistency with and support for, federal activities related to the handling and safeguarding of controlled unclassified information that are being led by the National Archives and Records Administration pursuant to Executive Order 13556. As CUI implementation evolves in the Government, the rule will be modified as necessary to ensure compliance. No change is made to the rule.

Comment: Two comments stated that the interim final rule lacks sufficient safeguards to limit the sharing and use of personally identifiable information and content of private communications.

Response: The program utilizes significant handling and sharing restrictions to ensure appropriate protections for any and all sensitive information managed by the program, including but not limited to PII. These safeguards are addressed in more detail in the PIA, which will be updated appropriately as the program evolves. No change is made to the rule.

Comment: Three comments recommended that the rule should require companies to remove sensitive information (e.g., PII), and to anonymize as much information as possible without hindering cyber security efforts, and that the Government should immediately dispose of inadvertently collected PII that is not directly relevant to the "cyber incident."

Response: DoD agrees with the underlying premise of the comment, and the DIB CS/IA program uses procedures to minimize the collection and sharing of PII. The DIB participants remove unnecessary sensitive information (e.g., PII), and only share information if it is relevant

to a cyber incident (e.g., for forensics or cyber intrusion damage assessment). All PII received by DoD is provided voluntarily by authorized DIB company representatives and is subject to mutually agreed upon restrictions for cyber security purposes. In addition, the DIB participants are required, prior to sharing any information with the Government under this program, to review and determine that their activities under the program are in compliance with all applicable laws and regulations, including restrictions on the interception, monitoring, access, use, and disclosure of electronic communications (see § 236.6(b) and (c)). Information determined to be relevant is maintained, controlled, and disposed of when no longer reasonably necessary for forensics analysis, and damage assessment activities (or other legal, audit or operational purposes). Companies are required to abide by all sharing restrictions. The PIA for the DIB CS/IA program addresses the handling safeguards in more detail. No change is made to the rule.

Comment: Two comments stated that the PII the Government obtains through the DIB CS/IA program should be used only for cyber security operations and not general law enforcement or intelligence fact gathering. The rule should also limit Government use of information shared for cyber security purposes.

Response: The primary purpose of the DIB CS/IA program is to share cyber security information to promote more effective cyber security, not only for the DIB, but also for the DoD and U.S. Government. The program contains numerous information handling and sharing restrictions, applicable to both the Government and DIB participants, to safeguard against any unauthorized collection, use, or dissemination of such information. However, the program does not limit the Government's ability to conduct lawful activities, including law enforcement, counterintelligence activities, or other activities in the interest of U.S. national security (§ 236.6(d)). No change is made to the rule.

Comment: One comment recommended that the rule incorporate privacy protections of the National Cyber Security Division's Joint Cybersecurity Services Pilot (JCSP).

Response: The detailed processes summarized in the PIA for the DIB CS/IA program are comprehensive and ensure appropriate safeguards for PII provided by DIB participants in a similar manner as described in the PIA prepared for the Department of Homeland Security's JSCP. No change is made to the rule.

Comment: One comment stated the interim rule should be amended to impose fines on private companies that intentionally or negligently disclose "excessive PII."

Response: It is not clear what the commenter meant by the term "excessive PII." As discussed above, the DIB CS/IA program only receives PII in two ways: (i) for program administration and management purposes; and (ii) for cyber incident response and analysis purposes. In both cases, DIB companies share information only when it is relevant for those authorized purposes. In addition, DIB companies are prohibited from sharing any information, including PII, unless they have determined that it has been lawfully collected and is authorized to be shared with the Government. If it were to appear that a company is reporting excessive information not relevant to the program, the Government would seek to work with the company to clarify the sharing guidelines and support the company's efforts to refine its processes to implement more effective limits on sharing unnecessary information. If, despite these efforts, a company continued to share information that the Government deemed inappropriate within the scope of the program, the Government would take appropriate actions on a case by case basis, including potentially terminating the information sharing relationship with that participant. This is a voluntary program and fines are not part of the program. No change is made to the rule.

Comment: Two comments recommended changes to the definitions of cyber incident, compromise and threat.

Response: The rule leverages established definitions to the maximum extent possible. The source for the definition of "compromise", "cyber incident" and "threat" are from the Committee on National Security Systems Instruction No. 4009, "National Information Assurance Glossary," (http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf). These definitions are established and widely accepted Government definitions. No change is made to the rule.

Comment: One comment stated that U.S. based systems are not adequately defined.

Response: To further clarify terms, the term "U.S. based" has been added to the definitions section (§ 236.2(n)).

Comment: One comment recommended changing the definition of U.S. citizen to eliminate the phrase "holding a U.S. passport," and adding text on "Green Cards."

Response: The recommendation to add "U.S. citizen" to the definitions section is accepted and is added to § 236.2(o). For the purpose of the rule, a U.S. citizen includes a person born in the U.S. or naturalized. The recommendation to eliminate "holding a U.S. passport" as part of the U.S. citizen definition is also accepted in the definition of "U.S. citizen," (see § 236.2(o)).

Comment: One comment recommended changing the definition of GFI to a more descriptive term so as not to tie it to Government procurement.

Response: The definition of GFI in the rule is applicable only to the DIB CS/IA program (see § 236.2(j)), and does not relate to any specific procurement activities. There is no indication that the use of this term has led to any confusion amongst the DIB participants. No change is made to the rule.

Comment: Two comments dealt with aspects of sharing information that could ward against threats and improve Operational Security (OPSEC).

Response: The purpose of the DIB CS/IA program is to enable cyber threat information sharing with DIB participants to improve operational security of DIB networks and information systems. No change is made to the rule.

Comment: One comment suggested replacing the phrase "to use the GFI on non-U.S. based covered DIB systems," with "to reside on non-U.S. based covered DIB" in § 236.4(g).

Response: After evaluation, the recommended change in terminology from "use" to "reside" does not provide additional technical clarity. No change is made to the rule.

Comment: Two comments recommended the language be amended to include the words "or as soon as practicable thereafter" following the word "discovery" and expressed caution that less knowledgeable participants will be prone to over report which consumes scarce Government and industry resources and obscures the significant incidents (§ 236.5(b)).

Response: Timeliness in reporting cyber incidents involving covered defense information is an integral component of the DIB CS/IA program. The rule makes provisions for initial and follow-up reporting (§ 236.5(b) and (c)). While the DIB CS/IA program is voluntary, cyber security encourages sharing information as quickly as possible to provide the clearest understanding of the cyber threat targeting DoD program information. This enables cyber threat information provided by DIB participants to be shared with other DIB participants and Government stakeholders on a timely basis. No change is made to the rule.

Comment: Two comments recommended the draft "DFARS regulatory initiative on Safeguarding Unclassified DoD Information (Safeguarding Rule) being addressed under DFARS

Case 2011–D039" be written to avoid conflicting and duplicative requirements for participants in the DIB CS/IA program.

Response: The DoD is committed to using both internal coordination processes, and public review and comment procedures such as those used in rulemaking for this program and for proposed DFARS revisions, to ensure that its cyber security activities are evaluated to avoid conflicting or duplicative elements. No change is made to the rule.

Comment: Two comments recommended specific word changes to the program requirements relating to each party conducting a legal review of its policies and practices that support the program, including deletion of the requirement for a "determination" of compliance with law because it may be interpreted as requiring the company to retain outside counsel for such a determination, limiting the compliance only to "U.S" law, and deleting the second sentence of § 236.6(c) to avoid threatening the attorney-client privilege.

Response: The requirement at § 236.6(c) for a determination of legal compliance is expressly stated as a requirement that "the DIB participant shall perform a legal review . . . and shall make a determination" that it is compliant. There is neither an express nor implied requirement that the DIB participant retain outside counsel for such a determination, and thus no change to that language is warranted. In § 236.6, the rule retains "applicable laws and regulations" as an accurate description of the requirement. Finally, the second sentence of § 236.6(c) was intended merely to provide notice that the Government may request additional information from the DIB company, and was not intended to imply that there was a requirement to provide such information as a condition of the program, regardless of whether such information were protected by the attorney-client privilege. To avoid any unnecessary confusion or unintended implications, the second sentence is deleted.

Comment: One comment expressed full support for the Defense Industrial Base Voluntary Cyber Security and Information Assurance Activities.

Response: Government evaluation of the program concurs that the voluntary DIB CS/IA program contributes to the safeguarding of DoD information. No change is made to the rule.

Comment: One comment urged a renewed look at how classification schemes are balanced with disclosure schemes.

Response: In accordance with the rule (§ 236.4(f)), handling and safeguarding of classified GFI shall be in compliance with the National Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22-M). No change is made to the rule.

Comment: One comment recommended that the DIB CS/IA program have a more robust role in industry engagement.

Response: The DIB CS/IA program will continue to evaluate outreach opportunities to enhance engagement with industry, to include industry associations. No change is made to the rule.

Comment: Two comments recommended that the infrastructure of the internet be upgraded and that the rule should incorporate "technology neutral terms."

Response: Other activities within the Government are examining the infrastructure of the internet. The rule focuses on cyber threat sharing and the risk of compromise of DoD information that resides on, or transits, DIB unclassified information systems. No change is made to the rule.

Regulatory Procedures

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 final rule contain information collection requirements. These collection requirements were published in the preamble of the interim final rule that published on May 11, 2012 (77 FR 27617) for public comment. No comments were received on the collection requirements. OMB preapproved the collection requirements and assigned them OMB Controls Numbers 0704-0489 and 0704-0490.

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 revised to read as follows:

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

Sec.

236.2 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) Controlled Technical Information means technical information with military or space application (see 10 USC 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 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; 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.

DATED: September 30, 2013.

PATRICIA L. TOPPINGS

OSD Federal Register

Liaison Officer

Department of Defense

[FR Doc. 2013-24256 Filed 10/21/2013 at 8:45 am; Publication Date: 10/22/2013]