DEPARTMENT OF DEFENSE **BILLING CODE 5001-06**

Office of the Secretary

32 CFR Part 236

[DOD-2014-OS-0097/RIN 0790-AJ29]

Department of Defense (DoD)'s Defense Industrial Base (DIB) Cybersecurity (CS) Activities

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

ACTION: Final rule.

SUMMARY: This final rule responds to public comments and updates DoD's Defense Industrial Base (DIB) Cybersecurity (CS) Activities. This rule implements mandatory cyber incident reporting requirements for DoD contractors and subcontractors who have agreements with DoD. In addition, the rule modifies eligibility criteria to permit greater participation in the voluntary DIB CS information sharing program.

DATES: *Effective Date*: This rule is effective on [INSERT DATE 30 DAYS FROM PUBLICATION IN THE FEDERAL REGISTER].

FOR FURTHER INFORMATION CONTACT: Vicki Michetti, DoD's DIB Cybersecurity Program Office: (703) 604-3167, toll free (855) 363-4227, or OSD.DIBCSIA@mail.mil.

SUPPLEMENTARY INFORMATION:

PURPOSE: This final rule responds to public comments to the interim final rule published on October 2, 2015. This rule implements statutory requirements for DoD contractors and subcontractors to report cyber incidents that result in an actual or potentially adverse effect on a covered contractor information system or covered defense information residing therein, or on a contractor's ability to provide operationally critical support.

The mandatory reporting applies to all forms of agreements between DoD and DIB companies (contracts, grants, cooperative agreements, other transaction agreements, technology investment agreements, and any other type of legal instrument or agreement). The revisions provided are part of DoD's efforts to establish a single reporting mechanism for such cyber incidents on unclassified DoD contractor networks or information systems. Reporting under this rule does not abrogate the contractor's responsibility for any other applicable cyber incident reporting requirement. Cyber incident reporting involving classified information on classified contractor systems will be in accordance with the National Industrial Security Program Operating Manual (DoD–M 5220.22 (http://dtic.mil/whs/directives/corres/pdf/522022M.pdf)).

The rule also addresses the voluntary DIB CS information sharing program that is outside the scope of the mandatory reporting requirements. By modifying the eligibility criteria for the DIB CS program, the rule enables greater participation in the voluntary program. Expanding participation in the DIB CS program is part of DoD's comprehensive approach to counter cyber threats through information sharing between the Government and DIB participants.

BENEFITS: The DIB CS program allows eligible DIB participants to receive Government furnished information and cyber threat information from other DIB participants, thereby providing greater insights into adversarial activity targeting the DIB. The program builds trust between DoD and DIB and provides a collaborative environment for participating companies and DoD to share actionable unclassified cyber threat information that may be used to bolster cybersecurity posture. The program also offers access to government classified cyber threat information to better understand the threat, as well as providing technical assistance from the DoD Cyber Crime Center (DC3) including analyst-to-analyst exchanges, mitigation and remediation strategies, and best practices. Through cyber incident reporting and voluntary cyber

threat information sharing, both DoD and the DIB have a better understanding of adversary actions and the impact on DoD information and warfighting capabilities.

RELATED REGULATIONS: The definitions in the rule are consistent with Controlled Unclassified Information as used by the National Archives and Records Administration pursuant to Executive Order (E.O.) 13556 ‘‘Controlled Unclassified Information’’ (November 4, 2010) and 32 Code of Federal Regulations (CFR) 2002, "Controlled Unclassified Information" (September 14, 2016). The rule is also harmonized with Defense Federal Acquisition Regulation Supplement (DFARS) Case 2013-D018, "Network Penetration Reporting and Contracting for Cloud Services" and FAR Case 2011–020, "Basic Safeguarding of Contractor Information Systems."

AUTHORITIES: The mandatory cyber incident reporting requirements support implementation of sections 391, 393, and 2224 of Title 10, United States Code (U.S.C); the Federal Information Security Modernization Act (FISMA), codified at 44 U.S.C. § 3551 et seq.; and 50 U.S.C. § 3330(e), and the Intelligence Authorization Act for Fiscal Year 2014. Cyber threat information sharing activities under this rule fulfill important elements of DoD's critical infrastructure protection responsibilities, as the sector specific agency for the DIB (see Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience," available at https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil).

ASSOCIATED COSTS: Under this rule, contractors will incur costs associated with identifying and analyzing cyber incidents and their impact on covered defense information, or a contractor's ability to provide operationally critical support, and reporting those incidents to DoD. Contractors must obtain DoD-approved medium assurance certificates to ensure authentication

and identification when reporting cyber incidents to DoD. Medium assurance certificates are individually issued digital identity credentials used to ensure the identity of the user in online environments. Certificates typically cost about $175 each. If a contractor submits five cyber incident reports and participates in the voluntary DIB CS program, the annual cost to the contractor is estimated at $1,045. If the contractor elects to receive classified information electronically, the cost to establish the capability is approximately $4,500. The Government incurs cost to collect and analyze cyber incident information and develop trends and other analysis products, analyze malicious software, analyze media, onboard new companies into the voluntary DIB CS information sharing program, and facilitate collaboration activities related to the cyber threat information sharing.

CYBERSECURITY AND PRIVACY: A foundational element of the mandatory reporting requirements, as well as the voluntary DIB CS program, is the recognition that the information being shared between the parties includes extremely sensitive information that requires protection. For additional information regarding the Government's safeguarding of information received from the contractors that require protection, see the Privacy Impact Assessment (PIA) for DoD's DIB Cybersecurity Activities located at http://dodcio.defense.gov/IntheNews/PrivacyImpactAssessments.aspx. The PIA provides detailed procedures for handling personally identifiable information (PII), attributional information about the strengths or vulnerabilities of specific covered contractor information systems, information providing a perceived or real competitive advantage on future procurement action, and contractor information marked as proprietary or commercial or financial information.

PUBLIC COMMENTS

DoD published an interim final rule on October 2, 2015 (80 FR 59581). Twenty-eight comments were received and reviewed by DoD in the development of this final rule. A discussion of the comments received and changes made to the rule as a result of those comments follows:

Comment: One respondent recommended that the rule be clarified to confirm the requirements in the rule are prospective to be implemented in new agreements or in modifying an existing agreement.

Response: There should be no confusion regarding the prospective effect and effective date of the rule, nor is there basis to infer or interpret the rule as being intended to apply retroactively or otherwise to mandate the modification of pre-existing agreements; however, DoD agrees that the rule enables the option to modify such pre-existing agreements where deemed appropriate. No change is made to the rule.

Comment: One respondent expressed concern about being unable to locate the text of Section 941 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2013 in the U.S. Code.

Response: Section 941 of NDAA for FY13 has been codified at 10 U.S.C. § 393 and all citations to this law have been updated accordingly.

Comment: One respondent recommended regularly conducting and releasing PIAs.

Response: DoD updates PIAs in accordance with DoD regulations and policy. DoD revised the PIA and published it in October 2015 (see http://dodcio.defense.gov/IntheNews/PrivacyImpactAssessments.aspx). No change is made to the rule.

Comment: Two respondents recommended publishing a report on the program's privacy implications and addressing personal information in internal contractor systems and that DoD address special procedures and protections for personal information.

Response: DIB CS program activities are in compliance with DoD and national policies for collecting, handling, safeguarding, and sharing sensitive information in accordance with DoD Directive 5400.11, "DoD Privacy Program" and 5400.11- Regulation, "Department of Defense Privacy Program," which prescribes uniform procedures for implementation of and compliance with the DoD Privacy Program. Also, as noted in the immediately preceding response, the PIA for this program is also publicly available at http://dodcio.defense.gov/IntheNews/PrivacyImpactAssessments.aspx. In addition, DoD submits a privacy and civil liberties assessment of the DIB CS voluntary program for the annual Privacy and Civil Liberties Assessment Report required by E.O. 13636. No change is made to the rule.

Comment: One respondent stated that contractors are faced with multiple and sometimes conflicting reporting requirements for reporting cyber incidents from across the Government and even within DoD, and asserts that these reporting requirements should be clearly set forth in agreements with the Government. The respondent did not specifically identify any other cyber incident reporting requirements that might conflict with this rule.

Response: This rule consolidates and streamlines mandatory cyber incident reporting requirements and procedures originating from multiple separate statutory bases (e.g., 10 U.S.C. 391 and 393, and 50 U.S.C. 3330(e))—however, reporting under these procedures in no way abrogates the contractor's responsibility to meet other cyber incident reporting requirements that may be applicable based on other contract requirements, or other U.S. Government statutory or regulatory requirements (see §236.4(p)). DoD is working to streamline reporting procedures

within the Department, including by designating the DoD Cyber Crime Center (DC3) as the single DoD focal point for receiving cyber incident reporting affecting unclassified networks of DoD contractors. No change is made to the rule.

Comment: One respondent recommended that Congress repeal the requirement to establish procedures for mandatory cyber incident reporting.

Response: This rule implements mandatory statutory requirements for mandatory cyber incident reporting set forth in 10 U.S.C. 391 and 393 (§236.4(b) – (d)). No change is made to the rule.

Comment: Two respondents questioned the Department's use of specific terms and definitions in the rule. One respondent stated that "a violation of security policy of a system" that is a subset of the definition of "compromise" is very broad and could result in over reporting and overwhelming DoD's resources. Another respondent recommended that the scope of the rule should be narrowed to only information that relates to a "successful penetration."

Response: The rule leverages established definitions from the Committee on National Security Systems Instruction No. 4009, "National Information (IA) Assurance Glossary," (https://www.ncsc.gov/nittf/docs/CNSSI-4009_National_Information_Assurance.pdf). The term "successful penetration" is not in the CNSS glossary. However, the rule uses the established terms "cyber incident" and "compromise" from the CNSS glossary, which are widely accepted and understood Government definitions. Adhering to this definition will not overwhelm DoD resources. No change is made to the rule.

Comment: One respondent stated that the four categories of covered defense information are unclear and will hamper timely reporting.

Response: The definition of covered defense information has been clarified to more closely align with, and leverage, the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html (§236.2).

Comment: One respondent stated the scope of a cyber incident "affecting the contractor's ability to provide operationally critical support" is so vague that it may result in over reporting.

Response: DoD designates the supplies or services that qualify as operationally critical support, and is developing procedures to ensure that contractors are notified when they are providing supplies or services designated as operationally critical support. If the contractor is unclear as to what specific supplies or services being provided have been designated as operationally critical, the contractor should request clarification from the DoD point of contact (e.g., contracting officer or agreements officer) for the agreement(s) governing the activity in question. No change is made to the rule.

Comment: One respondent stated that it is not clear why the rule now distinguishes information "created by or for DoD" from information "not created by DoD."

Response: The distinction regarding whether information has been created by or for DoD originates from that distinction being an element of the underlying statutes that are implemented in this rule (e.g., 10 U.S.C. 391 and 393). The distinction is made in a variety of contexts—generally to reinforce the underlying reason for requiring the contractor to share information with DoD (e.g., as it relates to a potential compromise of information created by or for DoD in support of a DoD program), and to minimize the requirement to share or provide access to information that is not related to DoD programs or activities (e.g., except as necessary for forensics analysis regarding an incident in which DoD information may have been compromised). No change is made to the rule.

Comment: One respondent requested clarification of the purpose of, "Applicability and Order of Precedence," and the meaning of the phrase "applicable laws and regulations" in §236.4 of this rule.

Response: Section 236.4(a) mandates that the cyber incident reporting requirements of this rule be incorporated into all relevant types of agreements between DoD, but recognizes that in some cases an individual agreement may have terms or conditions that may be inconsistent with this rule, and allows the terms of the agreement to take precedence over the requirements of this rule only when the terms of the agreement "are authorized to have been included in the agreement in accordance with applicable laws and regulations." The laws and regulations that are applicable to any individual agreement will depend on the nature and context of the agreement. For example, in the context of procurement contracts, the requirements of this rule are implemented through Defense Federal Acquisition Regulation Supplement (DFARS) Subpart 204.73, "Safeguarding Covered Defense Information and Cyber Incident Reporting," and its associated clauses (e.g., DFARS 252.204-7009, and -7012). However, the FAR and DFARS also permit deviations from otherwise prescribed contract requirements under certain conditions, but not including cases when the deviation would be "precluded by law, executive order, or regulation" (see FAR 1.402). No change is made to the rule.

Comment: One respondent recommended that the phrase "all applicable agreements" in §236.4(a) be clarified to identify the agreements that DoD intends to be covered by the rule.

Response: Section 236.4(a) has been revised to clarify that the rule applies to "all forms of agreements (e.g., contracts, grants, cooperative agreements, other transaction agreements, technology investment agreements, and any other type of legal instrument or agreement)." For

example, these requirements are implemented for DoD procurement contracts through DFARS Subpart 204.73 and its associated clauses (e.g., DFARS 252.204-7009, and -7012).

Comment: One respondent raised issue about the practicality of the 72 hour reporting requirement.

Response: Timeliness in reporting cyber incidents is a key element in cybersecurity and provides the clearest understanding of the cyber threat targeting DoD information and the ability of companies to provide operationally critical support. The 72 hour reporting standard has been a part of the DIB CS program since it was first established as a pilot activity in 2008, and throughout its evolution into a permanent program and ultimate codification in the CFR in 2012. Based on this history, the 72 hour period has proven to be an effective balance of the need for timely reporting while recognizing the challenges inherent in the initial phases of investigating a cyber incident. Contractors should report available information within the 72 hour period and provide updates if more information becomes available. No change is made to the rule.

Comment: One respondent questioned the reporting by subcontractors and how DoD intends to enforce flow down of the clause and does DoD consider Internet Service Providers (ISPs) to fall in the category of subcontractors.

Response: Section 236.4(d) of the rule has been revised to clarify that contractors must flow down the reporting requirements to "subcontractors that are providing operationally critical support or for which subcontract performance will involve a covered contractor information system." Whether these requirements would be required to flow down to an ISP would depend on whether the particular service(s) being provided would meet the flowdown criteria, and the implementation of these requirements for any specific type of agreement (e.g., for procurement contracts governed by the DFARS) may provide additional guidance regarding flowdown. The

contractor should consult with the DoD point of contact for the relevant agreement (e.g., contracting officer or agreements officer) when it is uncertain if the requirements should flow down. Section 236.4(d) has been revised.

Comment: One respondent recommended that the rule establish what information a contractor must share with the Government under mandatory reporting.

Response: Contractors are required to report in accordance with §236.4(b). A list of the reporting fields can be found at http://dibnet.dod.mil. These reporting fields include the statutory requirements set forth in 10 U.S.C. 391 and 393, including but not limited to an assessment of the impact of the cyber incident, description of the technique or method used, summary of information compromised. No change is made to the rule.

Comment: One respondent commented that the rule does not provide any mechanism for a contractor to raise concerns about, object to, or limit the data being provided due to its sensitivity.

Response: This rule implements mandatory information sharing requirements of 10 U.S.C. 391 and 393 by requiring DoD contractors to report key information regarding cyber incidents, and to provide access to equipment or information enabling DoD to conduct forensic analysis to determine if or how DoD information was impacted in a cyber incident. The rule's implementation of these requirements is tailored to minimize the sharing of unnecessary information (whether sensitive or not), including by carefully tailoring the information required in the initial incident reports (§236.4(c)), by expressly limiting the scope of the requirement to provide DoD with access to additional information to only such information that is "necessary to conduct a forensic analysis," and by affirmatively requiring the Government to safeguard any contractor attributional/proprietary information that has been shared (or derived from

information that has been shared) against any unauthorized access or use. In the event that the contractor believes that there is information that meets the criteria for mandatory reporting, but the contractor desires not to share that information due to its sensitivity, then the contractor should immediately raise that issue to the DoD point of contact (e.g., contracting officer or agreements officer) for the agreement(s) governing the activity in question, and if necessary, follow the dispute resolution procedures that are applicable to the agreement(s). No change is made to the rule.

Comment: One respondent asked how DoD will safeguard any contractor data provided as part of media once in DoD's possession, and what are the recourses for contractors in the event of a breach of those safeguards.

Response: DoD uses a wide variety of mechanisms to safeguard all forms of sensitive information, including information received from contractors, to ensure that information is accessed, used, and shared only with authorized persons for authorized purposes. For example, the DIB CS PIA addresses how PII and other sensitive information will be protected. No change is made to the rule.

Comment: One respondent stated that the rule lacks sufficient protections for contractor sensitive information that is provided to government support contractors, and the rule should provide such protections consistent with 10 U.S.C. 2320(f)(2) and DFARS 252.227-7025, "Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends."

Response: Responsibilities of government support contractors to protect sensitive information received from other contractors under this rule are addressed in §236.4(m)(5) and are largely consistent with, although not identical to, the statutory provision and DFARS Clause

cited by the commenter. In addition, the support contractor providing support for DoD's activities under this rule may also qualify as a "covered Government support contractor" under the cited DFARS clause, and thereby would already be subject to the cited DFARS clause. No change is made to the rule.

Comment: One respondent stated the information shared with the Government should only be used for cybersecurity purposes.

Response: 10 U.S.C. 391 and 393 provide specific authorization for sharing information received in cyber incident reports for a range of important activities that include, but are not limited to, cybersecurity activities (see §236.4(m)(1)-(5)). Limiting the sharing of information to cybersecurity purposes only would be inconsistent with the statutory framework and would unnecessarily limit the use of information for critical activities such as law enforcement, counterintelligence, and national security. No change is made to the rule.

Comment: One respondent stated the rule provides no limitations on DoD's ability to share information with third-party contractors. It also imposes a confidentiality obligation upon receiving contractors but does not address measures needed to mitigate any potential conflicts of interest stemming from third-party access.

Response: Section 236.4(m)(5) authorizes sharing with government support contractors that are "directly supporting" Government activities under this rule, and applies a comprehensive set of use and non-disclosure restrictions and responsibilities for those government support contractors to safeguard the information they receive, including prohibiting the support contractor from using the information for any other purpose, making the reporting contractor a third-party beneficiary of the non-disclosure agreement with direct remedies for any breach of the restrictions by the support contractor. No change is made to the rule.

Comment: One respondent recommended the proposed rule should establish requirements for companies to remove PII before sharing with the Government and for the Government to remove upon receipt.

Response: The DIB CS program has implemented procedures to minimize the collection and sharing of PII. Companies are always asked to remove unnecessary PII, and only share information if it is relevant to a cyber incident (e.g., for forensics or cyber intrusion damage assessment). The PIA for DoD's DIB CS Activities provides procedures on how the Government handles PII, as well as other forms of sensitive contractor information (e.g., contractor attributional/proprietary). The PIA was updated and published in October 2015 (http://dodcio.defense.gov/IntheNews/PrivacyImpactAssessments.aspx). No change is made to the rule.

Comment: One respondent stated the rule places burden on the contractor to mark information as, "contractor attributional/proprietary," but if it is not marked and subsequently submitted in response to request for images at the time of the cyber incident, Government must ensure, in absence of marking, obligation to protect information as contractor/attributional/proprietary.

Response: The rule requires that, to the maximum extent practicable, the contractor shall identify and mark attributional/proprietary information, but it does not condition the Government's safeguarding of such information on that identification or marking. The Government has established procedures for receiving, evaluating, anonymizing, safeguarding and sharing of such reported information in connection with cyber incidents involving contractor information and information systems. The DIB CS PIA provides more details regarding processes for handling PII and other sensitive information. No change is made to the rule.

Comment: One respondent stated that the rule should include provisions for liability protection.

Response: Liability protections established by 10 U.S.C. 391 and 393 became effective after the publication of the interim rule. The regulatory implementation of these new statutory elements will be addressed through future rulemaking activities to ensure the opportunity for public comment.

Comment: One respondent recommended expanding the number of commercial service providers under the Enhanced Cybersecurity Service (ECS) program, as part of the DIB CS program.

Response: The ECS program is managed by the Department of Homeland Security (DHS). Recommendations regarding ECS should be forwarded to DHS at ECS_Program@hq.dhs.gov. No change is made to the rule.

Comment: One respondent cautioned against expanding the types of companies eligible for the DIB CS program until addressing all relevant operational, privacy, and security concerns. This expansion could encompass companies who provide services and products to the general public and current defense contractors who are not currently eligible to participate in the program.

Response: DoD has established eligibility requirements (§236.7) for participation in the DIB CS program and thus any future expansion or revision of this eligibility criteria will be accomplished in accordance with federal rulemaking requirements to allow for public review and comment. No change is made to the rule.

Comment: One respondent expressed concern about the burden of cost due to increased participation in the DIB CS program.

Response: The burden of cost for companies participating in the DIB CS program has been reduced. Under the revised rule, DoD removed the requirement for DIB CS participants to obtain access to DoD's secure voice and transmission systems supporting the program. All companies participating in the DIB CS program are still required to have a DoD-approved medium assurance certificate to enable encrypted unclassified information sharing between the Government and DIB CS participants. The cost of a DoD-approved medium assurance certificate has not changed and is approximately $175. No change is made to the rule.

REGULATORY PROCEDURES

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

Executive Orders 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distribute impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This rule has been designated a "significant regulatory action," although not economically significant, under section 3(f) of Executive Order 12866. Accordingly, the rule has been reviewed by the Office of Management and Budget (OMB).

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

It has been determined that this rule 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.

2 U.S.C. Ch. 25, "Unfunded Mandates Reform Act"

It has been determined that this rule 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. Ch. 6)

It has been certified that this rule is not subject to the Regulatory Flexibility Act (5 U.S.C. Ch. 6) because it would not, if promulgated, have a significant economic impact on a substantial number of small entities. Therefore, the Regulatory Flexibility Act, as amended, does not require us to prepare a regulatory flexibility analysis.

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

This rule does contain reporting requirements under the Paperwork Reduction Act (PRA) of 1995. The collection requirements were published in the preamble of the interim final rule that was published on October 2, 2015 (80 FR 59581) for public comment. No comments were received for these collections. The Office of Management and Budget (OMB) Control Numbers are: 0704-0489, "DoD's Defense Industrial Base (DIB) Cybersecurity (CS) Activities Cyber Incident Reporting," and 0704-0490, "DoD's Defense Industrial Base (DIB) Cybersecurity (CS) Program Points of Contact (POC) Information."

Executive Order 13132, "Federalism"

It has been determined that this rule 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

Government contracts, Security measures.

Accordingly, the interim final rule published at 80 FR 59581 on October 2, 2015, is adopted as a final rule with the following changes:

PART 236--DEPARTMENT OF DEFENSE (DoD)'s DEFENSE INDUSTRIAL BASE (DIB) CYBERSECURITY (CS) ACTIVITIES

1. The authority citation is revised to read as follows:

Authority: 10 U.S.C. 391, 393, and 2224; 44 U.S.C. 3506 and 3544; 50 U.S.C. 3330.

2. Amend §236.1 by revising the last two sentences in the section to read as follows:

§236.1 Purpose.

* * * The part also permits eligible DIB participants to participate in the voluntary DIB CS program to share cyber threat information and cybersecurity best practices with DIB CS participants. The DIB CS program enhances and supplements DIB participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems.

3. Amend §236.2 by:

a. Revising the definition of “Covered contractor information system”.

b. Revising the definition of “Covered defense information”.

c. Revising the definition of “Cyber incident”.

d. Revising the definition of “DIB participant”.

e. Removing “DoD-DIB CS information sharing program” and adding in its place “DIB CS program” in the definition of “Government furnished information”.

f. Removing “Contractor” and adding in its place “contractor” in the definition of “Media”.

The revisions read as follows:

§236.2 Definitions.

* * * * *

Covered contractor information system means an unclassified information system that is owned or operated by or for a contractor and that processes, stores, or transmits covered defense information.

Covered defense information means unclassified controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html) that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies, and is:

(1) Marked or otherwise identified in an agreement and provided to the contractor by or on behalf of the DoD in support of the performance of the agreement; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the agreement.

* * * * *

DIB participant means a contractor that has met all of the eligibility requirements to participate in the voluntary DIB CS program as set forth in this part (see §236.7).

* * * * *

§236.3 [Amended]

4. Amend §236.3 by:

a. In paragraph (b)(1), removing "DoD-DIB CS information sharing program" and adding in its place "DIB CS program."

b. In paragraph (c), removing "DoD-DIB CS information sharing program" and adding in its place "DIB CS program."

§236.4 [Amended]

5. Amend §236.4 by:

a. In paragraph (a), removing "applicable agreements" and adding in its place "forms of agreements (e.g., contracts, grants, cooperative agreements, other transaction agreements, technology investment agreements, and any other type of legal instrument or agreement)."

b. In paragraph (d), removing ", as appropriate" and adding in its place "that are providing operationally critical support or for which subcontract performance will involve a covered contractor information system."

c. In paragraph (e), removing "http://iase.disa.mil/pki/eca/certificate.html" and adding in its place "http://iase.disa.mil/pki/eca/Pages/index.aspx."

d. In paragraph (m)(4), adding "non-attributional cyber threat information" after "sharing."

e. Redesignating paragraphs (n) through (p) as paragraphs (o) through (q).

f. Redesignating paragraph (m)(6) as paragraph (n).

6. Amend §236.5 by:

a. Revising the section heading.

b. In paragraph (a), removing “DoD-DIB CS information sharing program” and adding in its place “DIB CS program.”

c. In paragraph (b), removing “DoD-DIB CS information sharing program” and adding in its place “DIB CS program.”

d. Revising paragraph (d).

e. In paragraph (g), removing “DoD-DIB CS information sharing program” and adding in its place “DIB CS program.”

The revisions read as follows:

§236.5 DoD’s DIB CS program.

*** * * * ***

(d) DoD’s DIB CS Program Office is the overall point of contact for the program. The DC3 managed DoD DIB Collaborative Information Sharing Environment (DCISE) is the operational focal point for cyber threat information sharing and incident reporting under the DIB CS program.

*** * * * ***

7. Amend §236.6 by:

a. Revising the section heading.

b. In paragraph (a):

i. Removing “DoD-DIB CS information sharing program” and adding in its place “DIB CS program” in the first sentence.

ii. Removing “DoD-DIB CS information sharing program” and adding in its place “DIB CS program” in the second sentence.

c. In paragraph (c), removing “DoD-DIB CS information sharing program” and adding in its place “DIB CS program.”

d. In paragraph (d), removing “DoD-DIB CS information sharing program” and adding in its place “DIB CS program.”

e. In paragraph (e), removing “DoD-DIB CS information sharing program” and adding in its place “DIB CS program.”

f. In paragraph (g), removing “DoD-DIB CS information sharing program” and adding in its place “DIB CS program.”

The revisions read as follows:

§236.6 General provisions of DoD’s DIB CS program.

* * * * *

8. Amend §236.7 by:

a. Revising the section heading.

b. In paragraph (a) introductory text, removing “DoD-DIB CS information sharing program” and adding in its place “DIB CS program.”

c. In paragraph (a)(1), adding “to at least the Secret level” after “FCL.”

d. In paragraph (a)(2), removing “DoD-DIB CS information sharing program” and adding in its place “DIB CS program.”

e. In paragraph (a)(3)(iii), removing “DoD-DIB CS information sharing program” and adding in its place “DIB CS program.”

The revisions read as follows:

§236.7 DoD's DIB CS program requirements.

* * * * *

Dated: September 29, 2016.

Patricia L. Toppings,

OSD Federal Register, Liaison Officer, Department of Defense.

[FR Doc. 2016-23968 Filed: 10/3/2016 8:45 am; Publication Date: 10/4/2016]