BILLIN

DEPARTMENT OF DEFENSE

Office of the Secretary

32 CFR Part 236

[Docket ID: DOD–2019-OS-0112]

RIN 0790–AK86

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

AGENCY: Office of the DoD Chief Information Officer, Department of Defense (DoD).

ACTION: Proposed rule.

SUMMARY: The DoD is proposing revisions to the eligibility criteria for the voluntary Defense Industrial Base (DIB) Cybersecurity (CS) Program. These revisions will allow a broader community of defense contractors to benefit from bilateral information sharing as when this proposed rule is finalized all defense contractors who are subject to mandatory cyber incident reporting will be able to participate. DoD is also proposing changes to definitions and some technical corrections for readability.

DATES: Comments must be received by [INSERT DATE 45 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Please submit comments on this proposed rule, identified by 32 CFR part 236, Docket ID: DOD-2019-OS-0112 and/or by Regulatory Information Number (RIN) 0790-AK86, by any of the following methods:

- Federal Rulemaking Portal: https://www.regulations.gov. Follow the instructions for submitting comments.
- Mail: Department of Defense, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Regulatory Directorate, 4800 Mark Center Drive, Mailbox #24, Suite 08D09, Alexandria, VA 22350-1700.

Instructions: The general policy for comments is to make these submissions available for public viewing as they are received without change, including any personal identifiers or contact information provided by the commenter.

FOR FURTHER INFORMATION CONTACT:

- Stacy Bostjanick, Chief Defense Industrial Base Cybersecurity, Office: 703-604-3167.
- DIB CS Program Management Office: OSD.DIBCSIA@mail.mil.

  Instructions: DO NOT submit comments to this email address.

SUPPLEMENTARY INFORMATION:

Background and Authority

The 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. The DIB Cybersecurity Program is a voluntary program to enhance and supplement participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems. The program encourages greater threat information sharing to complement mandatory aspects of DoD's DIB cybersecurity activities which are contractually mandated through Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.[1] This program supports and complements DoD-specific authorities at 10 U.S.C. 2224 and the Federal Information Security Management Act (FISMA) (44 U.S.C. 3541 et seq). Cyber threat information sharing activities under this proposed rule also fulfill important elements of DoD's critical infrastructure protection responsibilities, as the sector risk management agency for the DIB (see Presidential Policy Directive 21 (PPD-21),[2] "Critical Infrastructure Security and

[1] https://www.ecfr.gov/current/title-48/chapter-2/subchapter-H/part-252/subpart-252.2/section-252.204-7012.
[2] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Resilience"). Expanding eligibility requirements for the DIB CS Program will augment DoD's information sharing activities with the DIB.

Currently, the DIB CS Program has the following objectives:

- Establish a voluntary, mutually acceptable framework to protect information from unauthorized access.
- Protect the confidentiality of information exchanged to the maximum extent authorized by law.
- Create a trusted environment to maximize network defense and remediation efforts by:
    1. Sharing cyber threat information and incident reports.
    2. Providing mitigation/remediation strategies and malware analysis.

This program is part of DoD's larger portfolio of work to protect DoD information handled by the DIB by understanding and sharing information, building security partnerships, implementing long-term risk management programs, and maximizing efficient use of resources. It supports two-way information sharing and maintains meaningful relationships and frequent dialogue across the diverse array of eligible defense contractors. For eligible defense contractors, the program maintains a capability for companies to access classified government cyber threat information providing additional context to better understand the cyber threats targeting their networks and information systems.

In May 2012, DoD published an interim final rule establishing the voluntary DIB CS Program and the bilateral information sharing model still used today.[3] The 2012 rule established a voluntary cyber threat information sharing program for cleared defense contractors (CDC) with the ability to safeguard classified information, estimated at 2,650 in 2012. Under the rule cleared defense contractor is defined as a private entity granted clearance by DoD to access, receive, or

[3] 77 FR 27615, May 11, 2012 (https://www.govinfo.gov/content/pkg/FR-2012-05-11/pdf/2012-10651.pdf).

store classified information for the purpose of bidding for a contract or conducting activities in support of any program of DoD. The 2012 rule stated DoD would maintain a website to facilitate the following aspects of program participation: 1) sharing information regarding eligibility and participation in the program with potential participants, 2) applying to the program online, and 3) executing the necessary agreements with the Government. DoD has established this capability as an online portal referred to as "DIBNet," located at https://dibnet.dod.mil. A final rule responding to public comments was published in October 2013.[4] In October 2015, responding to new statutory requirements for cyber incident reporting for DoD contractors, subcontractors, and those providing operationally critical support, DoD published another interim final rule[5] to expand eligibility to all cleared defense contractors (estimated at 8,500 in 2015 and 12,000 in 2022), subject to program eligibility requirements. The 2015 rule removed the safeguarding requirement to participate in the program. The rule also removed the mandatory program eligibility requirement to have or acquire a Communications Security (COMSEC) account[6] and obtain access to DoD's secure voice and data transmission systems, although participants still have to fulfill these requirements to receive classified cyber threat information electronically. A final rule responding to public comments was published in October 2016.[7]

Discussion of the Proposed Rule

With this rule, the Department proposes to expand eligibility requirements to allow greater program participation and increase the benefits of bilateral information sharing, which helps protect DoD controlled unclassified information from cyberattack, as well as to better align the voluntary DIB CS Program with DoD's mandatory cyber incident reporting requirements.

---

[4] 78 FR 62430, October 22, 2013 (https://www.govinfo.gov/content/pkg/FR-2013-10-22/pdf/2013-24256.pdf).
[5] 80 FR 59581, October 2, 2015 (https://www.govinfo.gov/content/pkg/FR-2015-10-02/pdf/2015-24296.pdf).
[6] The National Security Agency administers COMSEC accounts.
[7] 81 FR 68312, October 4, 2016 (https://www.govinfo.gov/content/pkg/FR-2016-10-04/pdf/2016-23968.pdf).

The current eligibility requirements, based on the October 2016 rule, requires a company to be a cleared defense contractor[8] who:

- Has DoD-approved medium assurance certificates;[9]
- Has an existing facility clearance[10] to at least the Secret level;
- Can execute the standardized Framework Agreement[11] provided to interested contractors after the Department has verified the DIB company is eligible.

The program has experienced steady growth, with the annual number of applications tripling since 2016 (80 total applications received in 2016, 266 total applications received in 2022). It has also seen a steady increase in the percentage of defense contractors who are interested in participating but do not meet current eligibility requirements. The percentage of applications received from ineligible defense contractors has risen at an average rate of 5% per year since 2016; 10% of applications received in 2016 were from ineligible defense contractors, while 45% of applicants in 2022 were ineligible. This steady increase in ineligible applicants indicates an increasing desire amongst defense contractors to participate in a cyber threat information sharing program.

In addition, the Department has actively engaged defense associations, universities, and companies in the DIB, as well as participated in many public forums discussing cyber threats and the way forward. The overwhelming feedback was for the Department to facilitate engagement with the broader community of defense contractors beyond just the cleared defense community.

---

[8] 32 CFR 236.2 defines cleared defense contractor to mean a subset of contractors cleared under the National Industrial Security Program (NISP) who have classified contracts with the DoD.

[9] The DoD has established the External Certification Authority (ECA) program to support the issuance of DoD-approved certificates to industry partners and other external entities and organizations. The ECA program is designed to provide the mechanism for these entities to securely communicate with the DoD and authenticate to DoD Information Systems. [https://public.cyber.mil/eca/]

[10] Entities (including companies and academic institutions) engaged in providing goods or services to the U.S. Government involving access to or creation of classified information may be granted a Facility Clearance (FCL). The Defense Counterintelligence and Security Agency (DCSA) processes, issues, and monitors the continued eligibility of entities for an FCL. [https://www.dcsa.mil/mc/isd/fc/]

[11] Applicants to the DIB CS Program submit an application from https://dibnet.dod.mil. Once a company has been verified, the Framework Agreement is made available for review.

In general, smaller defense contractors have fewer resources to devote to cybersecurity, which may provide a vector for adversaries to access information critical to national security. In addition, the Department is working on providing more tailored threat information to support the needs of a broader community of defense contractors with varying cybersecurity capabilities. The gap in eligibility in the current program, feedback from interested but ineligible contractors, a vulnerable DoD supply chain, and a pervasive cyber threat have prompted DoD to propose revising the eligibility requirements of the DIB CS Program to allow participation by non-cleared defense contractors.

The maximum number of defense contractors estimated to be subject to mandatory cyber incident reporting under DFARS clause 252.204-7012 is 80,000. The presence of the clause in a contract does not establish that covered defense information is shared. DoD is working on reporting mechanisms to better assess contractors managing covered defense information. The population of defense contractors in possession of covered defense information and subject to mandatory incident reporting requirements far exceeds the population of defense contractors currently eligible to participate in the voluntary DIB CS Program. With the proposed changes to the eligibility criteria, an estimated additional 68,000 defense contractors will be eligible to participate in the voluntary DIB CS Program. Based on prior participation statistics, it is estimated that about 10% of the eligible contractors (12,000 + 68,000 = 80,000) will actually apply to join the voluntary DIB CS Program (80,000 x 0.10 = 8,000).

Currently, the DIB CS Program has approximately 1,000 cleared defense contractors participating in the program. Program participants have access to technical exchange meetings, a collaborative web platform (DIBNet-U), and threat products and services through the DoD Cyber Crime Center (DC3). DC3 implements the program's operations by sharing cyber threat information and intelligence with the DIB, and offering a variety of products, tools, services, and events. DC3 serves as the single clearinghouse for unclassified Mandatory Incident Reports (MIRs) and voluntary threat information sharing reports.

Changes to Definitions

In addition to the program eligibility changes described above, DoD is also proposing the following changes.

§236.2 Definitions:

1. Access to media – This definition is being removed as it is no longer used in the rule text.

3. DIB CS Program participant – This definition has been revised to align with the revised eligibility requirements set forth in this proposed rule.

4. Government furnished information (GFI) – This definition was revised to adopt the convention of referring to the DIB CS Program with a capital 'P'.

Other Proposed Changes

DoD is amending § 236.5 (DoD's DIB CS program) in order to align the program description with the revised eligibility requirements. As a result, references to cleared defense contractors have been replaced with contractors that own or operate a covered contractor information system. Security clearance information is only collected, when applicable, if a company elects to participate in classified information sharing. In addition, the language stating participation is typically three to ten company-designated points of contact (POC) has been removed, to avoid confusion regarding the number of POCs, as some larger companies may wish to nominate a larger number of POCs and smaller companies may wish to nominate fewer.

DoD is amending § 236.7 (DoD's DIB CS program requirements) to remove the requirement that a company have an existing active facility clearance (FCL) to at least the Secret level granted under 32 CFR part 117, National Industrial Security Program Operating Manual (NISPOM),[12] to be eligible to participate in the DIB CS Program. In addition, references to

[12] https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117.

cleared defense contractors have been replaced with contractors that own or operate a covered contractor information system.

A foundational element of the activities described in this part is the recognition that the information shared between DoD and DIB CS Program participants pursuant to the DIB CS Program includes extremely sensitive information that requires protection. For additional information regarding the Government's safeguarding of information received from contractors that requires protection, see the Privacy Impact Assessment (PIA) for the DIB Cybersecurity Activities located at: https://dodcio.defense.gov/Portals/0/Documents/DIB_PIA.pdf. 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. In addition, personnel information is covered by Office of the Secretary of Defense (OSD) System of Records Notice (SORN) DCIO 01 (https://dpcld.defense.gov/Portals/49/Documents/Privacy/SORNs/OSDJS/DCIO-01.pdf). No changes to the PIA or SORN are being proposed in conjunction with this proposed rule.

Expected Impact of the Proposed Rule

Costs

DoD believes the cost impact of the proposed changes to this proposed rule is not significant, as the changes primarily expand the availability of the established DIB CS Program to additional defense contractors. The newly eligible population of defense contractors may incur costs to familiarize themselves with the rule and those who elect to participate in the program will incur costs related to program participation. The Government will continue to incur costs related to operating the program. The DIB CS Program conducts outreach activities to defense contractors through press releases, participation in defense-oriented conferences,

speaking engagements, and through digital media. The program will leverage pre-established channels to message changes to the program and engage with the eligible population of defense contractors. Based on the program growth experienced that during the last phase of program expansion the program is forecasting annual growth at just over 1% of the eligible population. At a growth rate of 1% per year it will take the program approximately 10 years to achieve the estimated 10% participation rate of the eligible DIB.

Costs to DIB Participants

In order to join the DIB CS Program there is an initial labor burden for a defense contractor to familiarize themselves with the rule and subsequently apply to the program and provide POC information. In total, if it takes each contractor 30 minutes to read and familiarize him/herself with the rule, it will take contractors 4,000 hours to familiarize themselves with the rule (8,000 participants x .5 = 4,000 hours). At an hourly wage of $108.92, the total cost incurred by contractors for rule familiarization will amount to $108,920 dollars ($108.92 x .5 hours = $54.46 x 4,000 hours = $217,840). The hourly labor cost is based on the mean wage estimate from the Bureau of Labor Statistics for an Information Security Analysts, Occupational Employment and Wages, May 2021 and is covered under information collection 0704-0490. This hourly wage is adjusted upward by 100% to account for overhead and benefits, which implies a value of $108.92 per hour.

The estimated annual burden for a company to apply to the program or for a participating company to update POC information is $36.31, with a total annual cost to all participants of $319,498.67 at peak program participation. This calculation is based on 8,000 participants submitting an average of one application per year and 10% of the population (800 participants) submitting an update each year, with 20 minutes of labor per submission, at a cost of $108.92 per hour ($36.31 ($108.92 x 1/3 hours) x 8,800 events = $319,498.67).

There is an estimated annual burden projected at $544.60 for defense contractors voluntarily sharing cyber threat information. This is based on a defense contractor electing to

submit an average of five informational reports per year with two hours of labor per voluntary submission, at a cost of $108.92 per hour ($108.92 x 2 hours each = $217.84 x 5 reports = $1,089.20). It is estimated that 1% of the newly eligible population will elect to join the DIB CS Program annually, which currently has approximately 1,000 participants, with program growth plateauing at 10% of the population by Year 9. The table below shows the costs to industry to voluntarily sharing cyber threat information over a 9-year period. If, in the first year of the program expanding there are 980 participants and 800 new participants join the program, there will be a total of 1,780 participants. Assuming each participant responds five times, this totals 8,900 annual responses times $217.84 per response and will equal $1,938,776 in total annual cost to participants, which is covered in information collection 0704-0489.

	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9
DIB CS Participants	1,780	2,580	3,380	4,180	4,980	5,780	6,580	7,380	8,000
Voluntary Reports Received	8,900	12,900	16,900	20,900	24,900	28,900	32,900	36,900	40,000
Annual Cost	$1,938,776	$2,810,136	$3,681,496	$4,552,856	$5,424,216	$6,295,576	$7,166,936	$8,038,296	$8,713,600

In addition, DIB CS Program participants may choose to attend meetings in conjunction with the DIB CS Program. All new participants are invited to attend an orientation session and all existing participants are invited to attend meetings on a quarterly basis. If a defense contractor chooses to send an employee to a day-long meeting each quarter, the defense contractor would incur a cost of $1,742 ($108.92 x 8 hours = $871.36 x 4 meetings = $3,485.44).

Costs to the Government

The DoD has identified general areas of costs related to the operation of this program. First, DoD incurs costs to implement this program operationally by responding to inquiries, processing application submissions and collecting, sharing, and managing POC information for program administration and management purposes. Second, DoD incurs costs to collect, analyze, and disseminate threat information.

DoD responds to an average of 2,000 questions each year and these responses are estimated to take 20 minutes per response. If it takes 20 minutes to respond to each question, it will take 667 hours to respond to questions. At an hourly wage of $51.16,[13] it will cost the DoD $34,107 dollars to respond to questions ($51.16 x (.333 x 2,000) = $34,107). Costs to the government are incurred when a company applies to the DIB CS Program to validate and store POC information and to perform follow-up activities with a company when the information is outdated. The processing time for these activities is estimated to be one hour per company. If 8,000 companies participate in the program and 10% of the companies update information with the program annually the labor cost to the government is expected to be $450,208 = (8,800 x $51.16).

In addition, there is a cost incurred by the DoD to receive cyber threat information submitted by defense contractors to have it analyzed by cyber threat experts at DC3. By year 9 of the expanded program, it is estimated DC3 will receive 40,000 responses per year, based on the estimate that each participating company elects to submit 5 informational reports (8,000 participants x 5 reports). Each product takes approximately two hours to create and incurs an hourly labor cost of $51.16 per hour. This equals $102.32 (2 hours x 51.16) per response. The labor cost to the government is forecasted to be $4,092,800 annually after 9 years of growth. In addition to processing cyber threat information, the DoD incurs operational and maintenance costs for the system receiving and storing cyber threat information. This system costs the DoD $5,100,000 annually to maintain (covered under information collection 0704-0489).

Benefits

This program benefits the Department by increasing awareness and improving assessments of cyber incidents that may affect mission critical capabilities and services. It continues to be an important element of the Department's comprehensive effort to defend DoD

[13] This is based upon the 2022 General Schedule (GS) pay scale for a GS-9 Step 5 and is adjusted upward by 100% to adjust for overhead and benefits.

information, protect U.S. national interests against cyber-attacks, and support military operations and contingency plans worldwide. Once a defense contractor joins the program, they are encouraged to share information, including cyber threat indicators, that they believe may be of value in alerting the Government and others, as appropriate, of adversary activity to enable the development of mitigation strategies and proactively counter threat actor activity. DC3 develops written products that include analysis of the threat, mitigations, and indicators of adversary activity. Even cyber incidents that are not compromises of covered defense information may be of interest to DoD for situational awareness purposes. This information is disseminated as anonymized threat products that are shared with authorized DoD personnel, other Federal agencies, and company-designated POCs participating in the DIB CS Program. With the revisions to the eligibility criteria, the Department will be able to reduce the impact of cyber threat activity on DIB networks and information systems and, in turn, preserve its technological advantage and protect DoD information and warfighting capabilities. The mitigation of the cyber threat targeting defense contractors reinforces the nation's national security and economic vitality.

For DIB participants, this program provides valuable cyber threat information they cannot obtain from anywhere else and technical assistance through analyst-to-analyst exchanges, mitigation and remediation strategies, and cybersecurity best practices in a collaborative environment. The shared unclassified and classified cyber threat information is used to bolster a company's cybersecurity posture and mitigate the growing cyber threat. The program's tailored support for small, mid-size, and large companies with varying cybersecurity maturity levels is an asset for participants. The program remains a key element of DoD's cybersecurity efforts by providing services to help protect DIB CS Program participants and the sensitive DoD information they handle.

Alternatives

Alternative #1

Maintain status quo with the ongoing voluntary cybersecurity program for cleared defense contractors.

Reason for not Selecting Alternative #1

This option is not selected as it does not allow DoD to increase bilateral information sharing to bolster DIB cybersecurity and safeguard DoD information transiting on DIB networks. In addition, the population of defense contractors with mandatory reporting requirements would continue to exceed those eligible to participate in the DIB CS Program. Companies that submit mandatory reports but are not eligible for the DIB CS Program would continue to be excluded from receiving cyber threat information and technical assistance.

Alternative #2

DoD posts generic cyber threat information and cybersecurity best practices on a publicly accessible website without directly engaging participating companies.

Reason for not Selecting Alternative #2

This alternative was not selected as companies already have access to open-source cyber threat information and best practices from multiple sources in the public sector. This alternative does not afford access by defense contractors to government-furnished cyber threat information, specifically tailored for the DIB. In addition, this alternative does not enable defense contractor interaction with DC3.

Alternative #3

Revise eligibility requirements to permit all defense contractors who own or operate a covered contractor information system (approximately 80,000 defense contractors) to participate in the DIB CS Program. Using the 10% estimation used for past program participation, the program is forecasted to grow to approximately 8,000 defense contractors.

Reason for Selecting Alternative #3

The revised eligibility criteria allow DoD to perform outreach to a broader DIB community. Being able to share pertinent cyber threat information with the DIB will increase both the DoD

and defense contractors' knowledge of the cyber threat landscape. Giving DoD the ability to have greater visibility over issues affecting unclassified networks will allow DoD to share pertinent alerts and threat information with a larger number of DIB organizations. DoD believes that revising the eligibility criteria to apply to contractors that own or operate covered contractor information systems is an important step in managing DoD's operational risk because it will allow additional companies to begin receiving cyber threat information to inform and harden their cybersecurity posture. DIB organizations that do not meet the current eligibility requirements to be in a DoD-sponsored cyber threat information sharing program have expressed interest in this change as noted previously by the growing percentage of ineligible applicants.

Regulatory Compliance Analysis

A. Executive Order 12866, "**Regulatory Planning and Review" and Executive Order 13563, "Improving Regulation and Regulatory Review"**

Executive Order 12866 direct agencies to assess all costs, benefits, and available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health, safety effects, distributive 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 proposed rule has been designated "significant," under Executive Order 12866.

B. Congressional Review Act (5 U.S.C. 801 et seq.)

Pursuant to the Congressional Review Act, this proposed rule has not been designated a major rule, as defined by 5 U.S.C. 804(2). This proposed rule will not have an economic effect above the $100 million threshold defined in 5 U.S.C. 804(2) or spur a major increase in costs or prices for consumers, individual industries, Federal, State, or local government agencies, or geographic regions; or have 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.

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

The Office of the DoD Chief Information Officer certifies that this proposed rule 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. This proposed rule will have a significant positive impact on small entities that will become eligible to participate in and receive benefits through the DIB CS Program. For DIB participants, this program provides cyber threat information and technical assistance through analyst-to-analyst exchanges, mitigation and remediation strategies, and cybersecurity best practices in a collaborative environment. The shared threat information is used to bolster a company's cybersecurity posture and mitigate the growing cyber threat. The program's tailored support for small, mid-size, and large companies with varying cybersecurity maturity levels is an asset for participants.

Participation in the DIB CS Program is voluntary. Program application and participation costs are described in the cost analysis section of this proposed rule. These costs are voluntarily incurred and associated with the labor and resource costs to complete the required program paperwork, including execution of the Framework Agreement, to submit information to the Government, and to receive information from the Government. The costs associated with applying to the DIB CS Program are associated exclusively with labor costs and estimated to be $18.15 per company. None of the program's offering come at an additional fee to DIB participants and additional costs related to participation are estimated based on the time investment (labor hours) required to obtain the benefits as described in the cost analysis of this preamble. Therefore, the Regulatory Flexibility Act, as amended, does not require us to prepare a regulatory flexibility analysis.

D. Sec. 202, Public Law 104-4, "Unfunded Mandates Reform Act"

Section 202 of the Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1532) requires agencies to assess anticipated costs and benefits before issuing any rule whose mandates require spending in any one year of $100 million in 1995 dollars, updated annually for inflation. When the Federal

Government passes legislation requiring a State, local, or tribal government to perform certain actions or offer certain programs but does not include any funds for the actions or programs in the law, an unfunded mandate results. This proposed rule will not mandate any requirements for State, local, or tribal governments, and will not mandate private sector incurred costs above the $100 million threshold defined in 2 U.S.C. 1532.

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

This proposed rule contains the following information collection requirements under the Paperwork Reduction Act (PRA) of 1995.

- 0704-0489, "DoD's Defense Industrial Base (DIB) Cybersecurity (CS) Activities Cyber Incident Reporting,"
- 0704-0490, "DoD's Defense Industrial Base (DIB) Cybersecurity (CS) Points of Contact (POC) Information."

With the revisions in eligibility criteria, DoD expects the burden associated with both collections to increase as additional defense contractors join the DIB CS Program and additional cyber threat information is reported. DOD is requesting comments on both collections as part of this proposed rule. Additional information regarding these collections of information – including all background materials -- can be found at https:/www.reginfo.gov/public/do/PRAMain by using the search function to enter either the title of the collection or the Office of Management and Budget (OMB) Control Number.

Comments are invited on: (a) whether the proposed collections of information are 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 for both information collections; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden on respondents, including the use of automated collection

techniques or other forms of information technology. Specific information on both collections is below.

DoD's Defense Industrial Base (DIB) Cybersecurity (CS) Activities Cyber Incident Reporting – OMB Control Number 0704-0489

Title: DoD's Defense Industrial Base (DIB) Cybersecurity (CS) Activities Cyber Incident Reporting

Type of Request: Revision.

Number of Participants: Number of DoD contractors eligible to participate in the voluntary program is 80,000. DoD estimates that approximately 1% of the newly eligible population will elect to join the program each year with program growth plateauing at approximately 10% of the population by Year 9. Based on this estimate, after the first three years of the program expansion, 2,400 defense contractors will join the existing 980 participating companies resulting in 3,380 defense contractors submitting voluntary cyber threat information reports.

Projected Responses Per Participant: Five reports per participant.

Annual Total Responses: 16,900.

Average Burden Per Response: Two hours.

Annual Total Burden Hours: 33,800 hours for all voluntary submissions.

Needs and Uses: DoD designated DC3 as the single focal point for receiving all cyber incident reporting affecting the unclassified networks of DoD contractors from industry and other government agencies. DoD collects cyber incident and threat reports using the Defense Industrial Base Network (DIBNet) portal (https://dibnet.dod.mil). Cyber threat reports are analyzed by experts at DC3 and they, in turn, develop written products that include analysis of the threat, mitigations, and indicators of adversary activity. These anonymized products are shared with authorized DoD personnel, authorized personnel from other Federal agencies, and authorized POCs from the DIB CS Program.

Affected Public: Business or other for-profit and not-for-profit institutions.

Frequency: On occasion.

Respondent's Obligation: Voluntary.

DoD's Defense Industrial Base (DIB) Cybersecurity (CS) Points of Contact (POC) Information -- OMB Control Number 0704-0490

Title: DoD's Defense Industrial Base (DIB) Cybersecurity (CS) Activities Points of Contact (POC) Information.

Type of Request: Revision.

Number of Participants: DoD contractors impacted is 80,000. DoD estimates that approximately 1% of the newly eligible population (800 defense contractors) will elect to join the program each year with program growth plateauing at approximately 10% of the population by Year 9. Each year, approximately 10% of participating companies will report changes to company contacts. If 10% of the pre-existing companies (2,580 in year 2) submit updates to the POC information and 800 new companies join, by year 3 this would result in 1,058 annual updates.

Projected Responses Per Participant: Initial collection is one per company with updates on a case-by-case basis.

Annual Total Responses: 1,058.

Average Burden Per Response: 20 minutes.

Annual Total Burden Hours: 353 hours for all participants.

Needs and Uses: Defense contractors complete a program application and sign the DIB CS Program Framework to initiate participation. The Government will collect business POC information from all DIB CS Program participants on a one-time basis, with updates as necessary, to facilitate communications and the sharing of share unclassified and classified cyber threat information.

Affected Public: Business or other for-profit and not-for-profit institutions.

Frequency: On occasion.

Respondent's Obligation: Voluntary.

F. Executive Order 13132, "Federalism"

Executive Order 13132 establishes certain requirements that an agency must meet when it promulgates a proposed rule (and subsequent final rule) that imposes substantial direct requirement costs on State and local governments, preempts State law, or otherwise has federalism implications. This proposed rule will not have a substantial effect on State and local governments.

G. Executive Order 13175, "Consultation and Coordination with Indian Tribal Governments"

Executive Order 13175 establishes certain requirements that an agency must meet when it promulgates a proposed rule (and subsequent final rule) that imposes substantial direct compliance costs on one or more Indian tribes, preempts tribal law, or effects the distribution of power and responsibilities between the Federal Government and Indian tribes. This proposed rule will not have a substantial effect on Indian tribal governments.

List of Subjects in 32 CFR Part 236

Government contracts, Security measures.

Accordingly, DoD proposes to amend 32 CFR part 236 as follows:

PART 236—DEPARTMENT OF DEFENSE (DoD) DEFENSE INDUSTRIAL BASE (DIB) CYBERSECURITY (CS) ACTIVITIES

1. The authority citation for 32 CFR part 236 continues 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. Revise the heading of 32 CFR part 236 to read as set forth above.

§236.1 [Amended]

3. Amend §236.1 by:

a. Removing "eligible DIB participants" and adding in its place "eligible DoD contractors".

b. Removing "DIB CS program" and adding in its place "DIB CS Program" wherever it appears.

c. Removing “DIB CS participants” and adding in its place “DIB CS Program participants”.

d. Removing “DIB participants’ capabilities” and adding in its place “DIB CS Program participants’ capabilities”.

§236.2 [Amended]

4. Amend §236.2 by:

a. Removing the definition of “Access to media”.

b. In the definition of “DIB participant”:

i. Removing “DIB participant” and adding in its place “DIB CS Program participant”.

ii. Removing “DIB CS program” and adding in its place “DIB CS Program”.

c. Removing “DIB CS program” in the definition of “Government furnished information (GFI)” and adding in its place “DIB CS Program”.

§236.3 [Amended]

5. Amend §236.3 by:

a. Removing “program” and adding in its place “Program participants” in paragraph (b)(1).

b. Removing “DIB CS program” and adding in its place “DIB CS Program” in paragraph (c).

6. Amend §236.4 by:

a. Removing “*http*” and adding in its place “*https*” in paragraphs (b)(2), (c), and (d).

b. Removing “http://iase.disa.mil/pki/eca/Pages/index.aspx” and adding in its place “https://public.cyber.mil/eca/” in paragraph (e).

c. Revising paragraph (f).

d. Adding a comma after “as appropriate” in the first sentence in paragraph (g).

e. Removing “paragraph (e)” and adding in its place “paragraph (i)” in paragraph (k).

f.. In paragraph (m)(4):

i. Removing “DIB contractors” and adding in its place “defense contractors”.

ii. Removing “DIB CS program” and adding in its place “DIB CS Program”.

g. Revising paragraph (p).

The revisions read as follows:

§236.4 Mandatory cyber incident reporting procedures.

* * * * *

(f) *Third-party service provider support*. If the contractor utilizes a third-party service provider (SP) for information system security services, the contractor may authorize the SP to report cyber incidents on behalf of the contractor.

* * * * *

(p) *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). The Government will notify the non-Government source or submitter (*e.g.*, contractor or DIB CS Program participant) of the information in accordance with the procedures in 32 CFR 286.10.

* * * * *

7. Amend §236.5 by:

a. Revising section heading and paragraph (a).

b. In paragraph (b):

i. Removing “DIB CS program” and adding in its place “DIB CS Program”.

ii. Removing “DIB participant” and adding in its place “DIB CS Program participant”.

c. In paragraph (c):

i. Removing “DIB participant” and adding in its place “DIB CS Program participant”.

ii. Removing “individual DIB participants” and adding in its place “individual DIB CS Program participants.”

d. In paragraph (d):

i. Removing “DoD's DIB CS Program Office” and adding in its place “DoD’s DIB CS Program Management Office”.

ii. Removing “DoD DIB” and adding in its place “DoD-DIB”.

iii. Removing “DIB CS program” and adding in its place “DIB CS Program”.

e. Removing “DIB participants” and adding in its place “DIB CS Program participants” in paragraph (e).

f. Redesignating paragraphs (f) through (n) as paragraphs (g) through (o).

g. Adding new paragraph (f).

h. In newly redesignated paragraph (g):

i. Removing the heading.

ii. Removing “DIB participants” and adding in its place “DIB CS Program participants”.

i. Revising newly redesignated paragraphs (h) and (i).

j. Removing “DIB participants” and adding in its place “DIB CS Program participants” in newly redesignated paragraph (j) introductory text.

k. In newly redesignated paragraph (k):

i. Removing “DIB participants” and adding in its place “DIB CS Program participants”.

ii. Removing “DIB participant” and adding in its place “DIB CS Program participant”.

l. Removing “DIB participants” and adding in its place “DIB CS Program participants” in newly redesignated paragraph (l).

m. Removing “DIB participants” and adding in its place “DIB CS Program participants” in newly redesignated paragraph (m).

n. In newly redesignated paragraph (n):

i. Removing “DIB participant” and adding in its place “DIB CS Program participant” wherever it appears.

ii. Removing “DIB participant’s FA” and adding in its place “DIB CS Program participant’s FA”.

o. In newly redesignated paragraph (o):

i. Removing “DIB participant” and adding in its place “DIB CS Program participant” wherever it appears.

ii. Removing “paragraph (m) of this section” and adding in its place “paragraph (n) of this section.”

The revisions and addition read as follows:

§236.5 DoD's DIB CS Program.

(a) All defense contractors that meet the requirements set forth in §236.7 are eligible to join the DIB CS Program as a DIB CS Program participant. Defense contractors meeting the additional eligibility requirements in §236.7 can elect to access and receive classified information electronically.

* * * * *

(f) As participants of the DIB CS Program, defense contractors are encouraged to share cyber threat indicators and information that they believe are valuable in alerting the Government and other DIB CS Program participants to better counter threat actor activity. Cyber activity that is not covered under §236.4 may be of interest to DIB CS Program participants and DoD.

* * * * *

(h) Prior to receiving GFI, each DIB CS Program participant shall provide the requisite points of contact information, to include U.S. citizenship and security clearance information, as applicable, for the designated personnel within their company in order to facilitate the DoD-DIB interaction in the DIB CS 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 CS Program participant for this program.

(i) GFI will be issued via both unclassified and classified means. DIB CS Program participants handling and safeguarding of classified information shall be in compliance with 32 CFR part 117. The Government shall specify transmission and distribution procedures for all GFI, and shall inform DIB CS Program participants of any revisions to previously specified transmission or procedures.

* * * * *

§236.6 [Amended]

8. Amend §236.6 by:

a. Removing “program” and adding in its place “Program” in the section heading.

b. In paragraph (a):

i. Removing “DIB CS program” and adding in its place “DIB CS Program” wherever it appears.

ii. Removing “DIB participants” and adding in its place “DIB CS Program participants”.

c. In paragraph (b):

i. Removing “DIB CS participants” and adding in its place “DIB CS Program participants”.

ii. Removing “http://www.dhs.gov/enhanced-cybersecurity-services” and adding in its place “https://www.cisa.gov/enhanced-cybersecurity-services-ecs”.

d. In paragraph (c):

i. Removing “DIB CS program” and adding in its place “DIB CS Program”.

ii. Removing “obligate the DIB participant” and adding in its place “obligate the DIB CS Program participant”.

iii. Removing “taken by the DIB participant” and adding in its place “taken by the DIB CS Program participant”.

iv. Removing “taken on the DIB participant’s” and adding in its place “taken on the DIB CS Program participant’s”.

e. In paragraph (d):

i. Removing “DIB participant’s participation” and adding in its place “DIB CS Program participant’s participation”.

ii. Removing “DIB CS program” and adding in its place “DIB CS Program”.

iii. Removing “approval of the DIB participant” and adding in its place “approval of the DIB CS Program participant”.

f. In paragraph (e):

i. Removing “DIB participant” and adding in its place “DIB CS Program participant” wherever it appears.

ii. Removing “DIB CS program” and adding in its place “DIB CS Program”.

g. Adding “change of status as a defense contractor,” after “Upon termination of the FA,” in paragraph (f).

h. In paragraph (g):

i. Removing “DIB participants’ rights” and adding in its place “DIB CS Program participants’ rights”.

ii. Removing “DIB CS program” and adding in its place “DIB CS Program”.

iii. Removing “the requirement for DIB participants” and adding in its place “the requirement for DIB CS Program participants”.

9. Revise §236.7 to read as follows:

§236.7 DoD's DIB CS Program requirements.

(a) To participate in the DIB CS Program, a contractor must own or operate a covered contractor information system and shall execute the standardized FA with the Government (available during the application process), which implements the requirements set forth in §§ 236.5 and 236.6 and this section.

(b) In order for DIB CS Program participants to receive classified cyber threat information electronically, the company must be a cleared defense contractor and must:

(1) Have an existing active facility clearance level (FCL) to at least the Secret level in accordance with 32 CFR part 117;

(2) Have or acquire a Communication Security (COMSEC) account in accordance with 32 CFR part 117, which provides procedures and requirements for COMSEC activities;

(3) Have or acquire approved safeguarding for at least Secret information, and continue to qualify under 32 CFR part 117 for retention of its FCL and approved safeguarding; and

(4) Obtain access to DoD's secure voice and data transmission systems supporting the voluntary DIB CS Program.

Dated: April 25, 2023.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2023-09021 Filed: 5/2/2023 8:45 am; Publication Date: 5/3/2023]