BILLING C

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: Final rule.

SUMMARY: The DoD is finalizing revisions to the eligibility criteria for the voluntary Defense Industrial Base (DIB) Cybersecurity (CS) Program. These revisions will allow all defense contractors who own or operate an unclassified information system that processes, stores, or transmits covered defense information to benefit from bilateral information sharing. DoD is also finalizing changes to definitions and some technical corrections for readability.

DATES: This rule is effective on [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

FOR FURTHER INFORMATION CONTACT:

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

SUPPLEMENTARY INFORMATION:

Discussion of Comments and Changes

The proposed rule was published in the Federal Register (88 FR 27832-27839) on May 3, 2023. Four submissions were received and are summarized below.

A commenter suggested DoD should redefine terms and should change the regulations for the program. However, the commenter did not provide any additional detail which would allow DoD to consider possible changes.

A commenter suggested DoD use this opportunity to run a targeted marketing campaign to assist small businesses with explaining a medium assurance certificate's purpose and procuring the hardware in advance of needing it.

After consideration, DoD is modifying the requirement for industry to obtain a medium assurance certificate. Medium assurance certificates can be used to validate digital identity and facilitate the exchange of encrypted information. However, it is not the only technical solution available to support identity proofing requirements. So, DoD is revising paragraph (e) in § 236.4, and separately in Department of Defense Instruction (DoDI) 8582.01, "Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information," to require registration with Procurement Integrated Enterprise Environment (PIEE)[1] when submitting mandatory cyber incident reports. This change will reduce the burden of having to procure a medium assurance certificate which costs approximately $175 annually. All DoD contracts contain Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.232-7003 (48 CFR 252.232-7003), which specifies requirements for electronic submission of payment requests. In order to access the electronic systems associated with electronic payments the contractor must also complete the required identity proofing and registration process with PIEE.

Multiple commenters provided input on the accuracy of the burden estimates. One commentor recommended allowing one report to cover multiple contracts to reduce the administrative reporting burden on all parties and enhance consistency across DoD data. Another commentor noted that many firms will lack in-depth familiarity with existing policy, compliance requirements, and other details of the DIB CS Program and, as such, the estimate of 30 minutes for new entrants to familiarize themselves with the rule is an underestimate.

[1] https://piee.eb.mil/.

As DoD is modifying the requirement for industry to obtain a medium assurance certificate with this final rule, the Department believes the burden to companies participating in the DIB CS Program is being reduced. In response to concerns about submitting a nearly identical report for multiple contracts, DoD would like to clarify that a contractor may submit one report for an event that impacts multiple contracts. Finally, DoD would like to clarify the estimate of 30 minutes to review changes to this final rule and choose whether to apply to the voluntary DIB CS Program does not include time for contractors to develop in-depth familiarity with existing policies and compliance requirements. It is expected DoD contractors will invest time to familiarize themselves with contractually mandated requirements in addition to this estimate.

A commenter highlighted the revision to the DIB CS Program omits a key component of the Critical Infrastructure Protection Act (CIPA) of 2001, and the revisions to the DIB CS Program will exclude operationally critical support (OCS) contractors from its provisions unless such contractors have covered defense information (CDI) resident in their information systems (IS). The commenter recommended including contractors performing under contracts that are designated as providing OCS, regardless of whether those IS contain CDI.

In accordance with 10 U.S.C. 391, the DoD must include mechanisms for Department personnel to, if requested, assist operationally critical contractors in detecting and mitigating penetrations. Pursuant to section 1642(b) of the National Defense Authorization Act for Fiscal Year 2019 DoD has authority to engage with the DIB that is complementary to, but distinct from, the DIB Cybersecurity Activities that implement the requirements levied upon the Department in 10 U.S.C. 391 and 393. To meet the requirements specified in 10 U.S.C. 391, the DIB CS program will refer ineligible applicants to other U.S. Government Departments and Agencies sharing cybersecurity equities to ensure Federal unity of effort.

A commenter posed several questions about the role of third-party service providers seeking to understand if a third-party service provider may submit reports on behalf of a client,

and if a third-party service provider must own or operate covered contractor information systems.

Currently, a contractor may authorize a third-party service provider to report incidents on behalf of the contractor. If that contractor and the third-party service provider are interested in participating in the DIB CS Program, an amendment to the DIB CS Program Framework Agreement is available to authorize the third-party service provider access to DIB CS resources. This agreement details whether the third-party service provider will provide on-site or off-site support; clarifies the respective roles of the contractor and the third-party service provider regarding accessing the government-furnished information on the DIB CS web portal and voluntary reporting of cyber incidents and indicators to the Government. The Framework Agreement and all Program amendments are made available through https://dibnet.dod.mil to an eligible company after the company has been verified by the DoD. The third-party service provider does not need to own or operate a covered defense system.

Two commenters reiterated the need for training and best practices but did not indicate if they are familiar with DoD's current training programs or if they believe the programs are adequate.

DoD notes the DIB CS Program offers training and best practices through in-person and virtual meetings and provides information about digital resources on https://dibnet.dod.mil.

One commenter stated a link or a copy of the "standardized" Government Framework Agreement on the website will help contractors better understand their ability to meet the requirement before submitting an application – potentially saving all parties time and resources. DoD notes factsheets and informational materials are publicly available on https://dibnet.dod.mil. The Framework Agreement between the Government and a DIB participant is made available after the company applies to the program and DoD verifies the company meets the eligibility requirements set forth in § 236.7.

A commenter suggested access and information for cleared companies should remain as it is today and recommended an "impact statement" to information released to uncleared firms to help contextualize the information and the reason for disseminating it.

The Privacy Impact Assessment (PIA) for DoD's DIB CS Activities provides procedures on how the Government handles personally identifiable information (PII), as well as other forms of sensitive contractor information (*e.g.*, contractor attributional/proprietary). The PIA is publicly available at https://dodcio.defense.gov/Portals/0/Documents/DIB_PIA.pdf and no changes to the PIA are being proposed. The Security Classification Guide (SCG)[2] is the tool used by DoD Personnel to identify and safeguard national security information when derivatively classifying information. All information will be designated and handled in accordance with the DIB CS Activities SCG, the NISPOM Program as defined in 32 CFR part 117 and the Controlled Unclassified Information (CUI) Program as defined in 32 CFR part 2002.

A commenter asked about a future opportunity to map the level of access to DIB CS resources to a company's certification(s) level or assessment scoring.

DoD notes all companies currently participating in the DIB CS Program are eligible to receive Government Furnished Information (GFI) under the voluntary DIB CS Program and cybersecurity information is shared to the greatest extent possible in accordance with the Program's SCG. Information about a company's certification level or assessment score is controlled information and not available to the DIB CS Program at this time.

A commenter recommended providing consistent controls and data access channels to help companies synthesize and apply the threat information to their market.

The DIB CS Program marks all documents in accordance with the SCG[3] and DIBNet remains the primary channel for disseminating threat products. DoD has recently relaunched DIBNet to provide an API-based data access channel to complement the ability for a DIB CS

[2] DIB CS Activities Security Classification Guide is available via https://www.DTIC.mil.

Participant to download PDF, TXT, and CSV based products which should allow a participating company to analyze threat information unique to their market.

A commenter recommended adding headers to § 236.4 for paragraph (f), (g), (j), and (o) to increase uniformity.

DoD has added headers to § 236.4 for paragraphs (f), (g), and (o). Paragraph (j) has a header, and an administrative correction will be made to correct the format of paragraph (n).

A commenter asked if the rights and responsibilities for submittals under the DIB CS Program have changed with respect to Freedom of Information Act (FOIA).

The rights and responsibilities for submittals under the DIB CS Program have not changed with respect to Freedom of Information Act (FOIA). The Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency (OATSD(PCLT)) maintains a DoD FOIA Handbook available at https://open.defense.gov/Transparency/FOIA/FOIAHandbook.aspx.

Background and Authority

The DIB means the DoD, 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 DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.[4] This program supports and complements DoD-specific authorities at 10 U.S.C. 2224 and the Federal Information Security Management Act (FISMA 2002) as amended by the

[4] https://www.ecfr.gov/current/title-48/chapter-2/subchapter-H/part-252/subpart-252.2/section-252.204-7012.

Federal Information Security Modernization Act, 2014. Cyber threat information sharing activities under this final 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),[5] "Critical Infrastructure Security and Resilience"). This program is aligned with the requirements of the Controlled Unclassified Information (CUI) program established in Executive Order 13556. 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.

[5] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

In May 2012, DoD published an interim final rule establishing the voluntary DIB CS Program and the bilateral information sharing model still used today.[6] 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 CDC is defined as a private entity granted clearance by DoD to access, receive, or 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.[7] 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[8] 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 requirement that CDCs be able to safeguard classified information to participate in the program. The rule also removed the mandatory program eligibility requirement to have or acquire a Communications Security (COMSEC) account[9] 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.[10]

Discussion of the Final Rule

---

[6] 77 FR 27615, May 11, 2012 (https://www.govinfo.gov/content/pkg/FR-2012-05-11/pdf/2012-10651.pdf).
[7] 78 FR 62430, October 22, 2013 (https://www.govinfo.gov/content/pkg/FR-2013-10-22/pdf/2013-24256.pdf).
[8] 80 FR 59581, October 2, 2015 (https://www.govinfo.gov/content/pkg/FR-2015-10-02/pdf/2015-24296.pdf).
[9] The National Security Agency administers COMSEC accounts.
[10] 81 FR 68312, October 4, 2016 (https://www.govinfo.gov/content/pkg/FR-2016-10-04/pdf/2016-23968.pdf).

With this rule, the Department is expanding 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. The current eligibility requirements, based on the October 2016 rule, requires a company to be a cleared defense contractor[11] who:

- Has DoD-approved medium assurance certificates;[12]
- Has an existing facility clearance[13] to at least the Secret level; and
- Can execute the standardized Framework Agreement[14] 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 more than 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. The steady increase in DIB applicants indicates an increasing desire amongst defense contractors to participate in a cyber threat information sharing program.

---

[11] 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.

[12] 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/]

[13] 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/]

[14] 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 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. 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 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 information 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 finalizing the following changes.

Section 236.2 Definitions:

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

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

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

Other Finalized Changes

DoD is amending § 236.4 (Mandatory cyber incident reporting procedures), in response to public comments received about the burden associated with medium assurance certificates. The amendment will require contractors to obtain PIEE account in conjunction with mandatory cyber incident reporting. This change will align the identity proofing processes used by DoD for the majority of DIB companies and will eliminate the cost associated with procuring medium assurance certificates. DoD will continue to accept medium assurance certificates to fulfil identity proofing requirements.

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 and is eligible 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),[15] to be eligible to participate in the DIB CS Program. In addition, references to 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 § 236.7 is the recognition that the information shared between DoD and DIB CS Program participants pursuant to the DIB CS Program includes CUI,[16] which 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

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

(https://dpcld.defense.gov/Portals/49/Documents/Privacy/SORNs/OSDJS/DCIO-01.pdf). No changes to the PIA or SORN are being made in conjunction with this final rule.

Expected Impact of the Final Rule

Comments were received on the cost of a DoD-approved medium assurance certificates and the accuracy of estimates relating to familiarization costs and attending meetings. DoD is removing the requirement for the DIB to have a DoD-approved medium assurance certificate to report cyber incidents. The requirement is being replaced with the requirement to register in PIEE which has established procedures to perform digital identity proofing. The basis for the cost estimate for a company to familiarize themselves with changes to this rule and determine if they would like to apply to the DIB CS Program does not include time for a company to perform an in-depth review of preexisting contractually mandated requirements. The basis for the cost estimate to participate in meetings uses the assumption a company sends the equivalent of an Information Security Analyst with the mean wage estimate published by the Bureau of Labor Statistics. If the company elects to send more senior representatives the cost will be higher. The economic analysis is being finalized without changes.

Costs

DoD believes the cost impact of the changes to this final 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 itself 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 $217,840 ($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 ($108.92 x 1/3 hours = $36.31 x 8,800 events = $319,498.67).

There is an estimated annual burden projected at $1,089.20 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 = $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 $3,485.44 ($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,[17] 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, by Year 9, 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 $72,647.20 = (620 +800 x $51.16).

	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9
DIB CS Participants	1780	2580	3380	4180	4980	5780	6580	7380	8000
New Applications	780	800	800	800	800	800	800	800	620
Updates	178	258	338	418	498	578	658	738	800
Annual Cost	$49,011.28	$54,127.28	$58,220.08	$62,312.88	$66,405.68	$70,498.48	$74,591.28	$78,684.08	$72,647.20

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

[17] 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.

This program benefits the Department by increasing the overall security of the DIB through 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 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 unique 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 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.

Regulatory Compliance Analysis

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

Executive Order 12866 directs 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 final 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 final rule has not been designated a major rule, as defined by 5 U.S.C. 804(2). This final 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 certified that this final 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 final 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, and in fact can avoid expending resources to obtain threat intelligence from private sources if the company elects to participate in services offered by the DoD that directly integrate threat intelligence.

Participation in the DIB CS Program is voluntary. Program application and participation costs are described in the cost analysis section of this final 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 is the result. This final 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)

Section 236.2 of this rule contains information collection requirements. As required by the Paperwork Reduction Act (44 U.S.C. Chapter 35), DoD submitted information collection requests to the Office of Management and Budget for review and approval. In response to DoD's invitation in the proposed rule to comment on any potential paperwork burden associated with this rule, there were no comments from the public. This final rule contains the following information collection requirements under the Paperwork Reduction Act (PRA) of 1995.

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

The System of Records Notice associated with these information collections (DCIO 01, "Defense Industrial Base (DIB) Cybersecurity (CS) Activities Records") published on May 17, 2019. The Federal Register citation for the SORN is 84 FR 22477.

The Privacy Impact Assessment for the Defense Industrial Base (DIB) Cybersecurity (CS) Activities is posted at: https://dodcio.defense.gov/Portals/0/Documents/DIB_PIA.pdf.

F. Executive Order 13132, "Federalism"

Executive Order 13132 establishes certain requirements that an agency must meet when it promulgates a final rule that imposes substantial direct requirement costs on State and local governments, preempts State law, or otherwise has federalism implications. This final 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 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 final 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 amends 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 is revised to read as follows:

Authority: 10 U.S.C. 391, 393, and 2224; 44 U.S.C. 3506 and 3554; 50 U.S.C. 3330.

2. Revise the heading of 32 CFR part 236 to read as set forth above.

3. Revise and republish §236.1 to read as follows:

§236.1 Purpose.

Cyber threats to contractor 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. This part requires all DoD contractors to rapidly report cyber incidents involving covered defense information on their covered contractor information systems or cyber incidents affecting the contractor's ability to provide operationally critical support. The part also permits eligible DoD contractors to participate in the voluntary DIB CS Program to share cyber threat information and cybersecurity best practices with DIB CS Program participants. The DIB CS Program enhances and supplements DIB CS Program participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems.

4. Amend §236.2 by:

a. Removing the definition of "Access to media".

b. Removing the definition of "DIB participant" and adding the definition "DIB CS Program participant" in its place.

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

The addition reads as follows:

§236.2 Definitions.

* * * * *

DIB CS Program 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]

5. Amend §236.3 by:

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

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

6. Amend §236.4 by:

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

b. Revising paragraphs (e) through (g).

c. Removing the words “paragraph (e)” and adding in their place the words “paragraph (i)” in paragraph (k).

d. Revising paragraph (m)(4).

e. Adding a heading for paragraph (o).

f. Revising paragraph (p).

The revisions and additions read as follows:

§236.4 Mandatory cyber incident reporting procedures.

* * * * *

(e) *Procurement Integrated Enterprise Environment (PIEE) account requirement.* To report cyber incidents in accordance with this section, the contractor or subcontractor shall have a PIEE account to access https://dibnet.dod.mil. For information on obtaining a PIEE account, see https://piee.eb.mil/.

(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.

(g) *Voluntary information sharing*. Contractors are encouraged to report information to promote sharing of cyber threat indicators that they believe are valuable in alerting the Government and others, as appropriate, in order to better counter threat actor activity. Cyber incidents that are not compromises of covered defense information or do not adversely affect the contractor's ability to perform operationally critical support may be of interest to the DIB and DoD for situational awareness purposes.

* * * * *

(m) * * *

(4) For national security purposes, including cyber situational awareness and defense purposes (including sharing non-attributional cyber threat information with defense contractors participating in the DIB CS Program authorized by this part); or

* * * * *

(o) *Contractor activities*. * * *

(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. Revise and republish §236.5 to 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.

(b) Under the voluntary activities of the DIB CS Program, the Government and each DIB CS Program participant will execute a 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, cybersecurity information.

(c) Each such FA between the Government and a DIB CS Program 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 CS Program participants.

(d) DoD’s DIB CS Program Management 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.

(e) The Government will maintain a website or other internet-based capability to provide potential DIB CS Program participants with information about eligibility and participation in the program, to enable online application or registration for participation, and to support the execution of necessary agreements with the Government.

(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.

(g) The Government shall share GFI DIB CS Program participant or designated SP in accordance with this part.

(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.

(j) Except as authorized in this part or in writing by the Government, DIB CS Program participants may:

(1) Use GFI only on U.S. based covered contractor information systems, or U.S. based networks or information systems used to provide operationally critical support; and

(2) Share GFI only within their company or organization, on a need-to-know basis, with distribution restricted to U.S. citizens.

(k) In individual cases DIB CS Program participants may request, and the Government may authorize, disclosure and use of GFI under applicable terms and conditions when the DIB CS Program participant can demonstrate that appropriate information handling and protection mechanisms are in place and has determined that it requires the ability:

(1) To share the GFI with a non-U.S. citizen; or

(2) To use the GFI on a non-U.S. based covered contractor information system; or

(3) To use the GFI on a non-U.S. based network or information system in order to better protect a contractor's ability to provide operationally critical support.

(l) DIB CS Program 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).

(m) DIB CS Program 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.

(n) If the DIB CS Program participant utilizes a SP for information system security services, the DIB CS Program participant may share GFI with that SP under the following conditions and as authorized in writing by the Government:

(1) The DIB CS Program 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 CS Program 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 CS Program 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 CS Program participant) under which the SP is subject to all applicable requirements of this part and of any supplemental terms and conditions in the DIB CS

Program participant's FA with the Government, and which authorizes the SP to use the GFI only as authorized by the Government.

(o) The DIB CS Program participant may not sell, lease, license, or otherwise incorporate the GFI into its products or services, except that this does not prohibit a DIB CS Program participant from being appropriately designated an SP in accordance with paragraph (n) of this section.

8. Revise and republish §236.6 to read as follows:

§236.6 General provisions of DoD's DIB CS Program.

(a) Confidentiality of information that is exchanged under the DIB CS Program will be protected to the maximum extent authorized by law, regulation, and policy. DoD and DIB CS Program participants each bear responsibility for their own actions under the voluntary DIB CS Program.

(b) All DIB CS Program participants may participate in the Department of Homeland Security's Enhanced Cybersecurity Services (ECS) program (*https://www.cisa.gov/resources-tools/programs/enhanced-cybersecurity-services-ecs*).

(c) Participation in the voluntary DIB CS Program does not obligate the DIB CS Program participant to utilize the GFI in, or otherwise to implement any changes to, its information systems. Any action taken by the DIB CS Program participant based on the GFI or other participation in this program is taken on the DIB CS Program participant's own volition and at its own risk and expense.

(d) A DIB CS Program participant's participation in the voluntary DIB CS 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 CS Program participant, its information systems, or its products or services.

(e) The DIB CS Program participant and the Government may each unilaterally limit or discontinue participation in the voluntary DIB CS Program at any time. Termination shall not relieve the DIB CS Program 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.

(f) Upon termination of the FA, change of status as a defense contractor, and/or change of Facility Security Clearance (FCL) status below Secret, GFI must be returned to the Government or destroyed pursuant to direction of, and at the discretion of, the Government.

(g) Participation in these activities does not abrogate the Government's, or the DIB CS Program 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. However, participation in the voluntary activities of the DIB CS Program does not eliminate the requirement for DIB CS Program participants to report cyber incidents in accordance with § 236.4.

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.

(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: March 1, 2024.

Patricia L. Toppings,

OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2024-04752 Filed: 3/11/2024 8:45 am; Publication Date: 3/12/2024]