SUPPORTING STATEMENT - PART A

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

Summary of Changes from Previously Approved Collection:

- The burden has been adjusted to reflect expanded eligibility to the voluntary DIB CS Program. It is estimated that 10% of the eligible population will elect to join the voluntary DIB CS Program, resulting in 8,000 participating companies in addition to those already participating providing updated POC information. This has resulted in an increase in total respondent labor burden.

1. Need for the Information Collection

DoD's Defense Industrial Base (DIB) Cybersecurity (CS) Program enhances and supports DIB participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems. The operational implementation of this program requires DoD to collect, share, and manage point of contact (POC) information for program administration and management purposes. The Government will collect typical business POC information from all DIB CS Program participants to facilitate communication and share cyber threat information. To implement and execute this program within their companies, DIB CS Program participants provide POC information to DoD during the application process to join the program. After joining the program, DIB CS Program participants are asked to revalidate information annually and provide updated POC information to DoD when personnel changes occur.

The DIB CS Program implements statutory authorities to established programs and activities to protect sensitive DoD information, including when such information resides on, or transits information systems operated by contractors in support of DoD activities. Authorities include 32 Code of Federal Regulations (CFR) Part 236, "Department of Defense (DoD)-Defense Industrial Base (DIB) Cybersecurity (CS) Activities,"[1] which authorizes the voluntary DIB CS information sharing program. In addition, the DIB CS Program supports and complements DoD-specific authorities at 10 U.S.C. § 2224 and the Federal Information Security Management Act (FISMA) of 2014 (44 U.S.C. § 3554). FISMA requires all federal agencies to provide information security protections for information collected or maintained by, or on behalf of, the agency. Cyber threat information sharing activities under this rule fulfill important elements of DoD's critical infrastructure protection responsibilities, as the sector risk management agency for the DIB sector (see National Security Memorandum (NSM–22), "Critical Infrastructure Security and Resilience."[2]

2. Use of the Information

[1] 32 CFR Part 236: https://www.federalregister.gov/documents/2024/03/12/2024-04752/department-of-defense-dod-defense-industrial-base-dib-cybersecurity-cs-activities

[2] NSM 22: https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/

The DIB CS Program is focused on sharing cyber threat information and cybersecurity best practices with DIB CS Program participants. To implement this program and share cyber threat information, the DoD needs to collect POC information for management and administration of the DIB CS Program. The Government will collect business POC information from all DIB CS Program participants to facilitate emails, teleconferences, meetings, and other program activities. This information includes company information including company name, Unique Entity Identifier (UEI), Commercial and Government Entity (CAGE) code, North American Industry Classification System (NAICS) code, company size, street address, and main telephone number. Then the applicant is asked to "Certify" that "[Their] company handles (e.g. processes, stores, develops, or transits) DoD Controlled Unclassified Information (CUI)," which is an eligibility requirement for participation. Information requested for identified company POCs includes name, title, work phone, and email. DIB CS Program POCs include the Chief Executive Officer (CEO), Chief Information Officer (CIO), Chief Information Security Officer (CISO), and Corporate or Facility Security Officer (CSO/FSO), or their equivalents, as well as those administrative, policy, technical staff, and personnel designated to interact with the Government in executing the DIB CS Program. A U.S. Government POC is also requested but is not required.

DIB participants voluntarily provide POC information to the DIB CS Program via the web portal (https://dibnet.dod.mil). On occasion, DIB CS Program participants may provide updated POC information by email but will follow up with a formal update to the web portal. The web portal is the method by which we collect information. To initiate the application, a representative from a company selects the "Apply to Program" button. Since access to the application requires a valid DoD-approved medium assurance certificate, the applicant will be prompted with for their DoD-approved medium assurance certificate. They are then directed to a DoD Consent Banner that indicates they are accessing a U.S. Government information system and must be click the "Agree" button in order to continue. The next page is the DoD Privacy Notice that includes the Authorities, Use, and Disclosure, and Freedom of Information Request (FOIA) disclaimers, which must be agreed to by the Company by clicking the "Agree" button to proceed with the application. The applicant is then required to complete several of the point of contact fields that are provided (i.e., company information, Company Representative, CEO, CIO, CISO, and any additional POCs). The online application does not allow the applicant to submit the information unless they certify that the information provided is accurate by "checking" the "Certify Application" box, as well as attesting that their company handles DoD CUI earlier in the application. Once all the contact information has been entered, the applicant clicks on the "Submit" button that automatically sends an email notice to the DIB CS Program office inbox that their application has been submitted.

If a company representative ever wants to update the POC information, they simply access the portal using their established DoD-approved medium assurance certificate. Only the designated company representative and the DIB CS Program system administrators have permission to update the company POC information.

3. Use of Information Technology

100% of the POC information provided by DIB companies is collected electronically.

4. Non-Duplication

The information obtained through this collection is unique and is not already available for use or adaptation from another cleared source.

5. Burden on Small Businesses

This information collection does not impose a significant economic impact on a substantial number of small businesses or entities.

6. Less Frequent Collection

POC information will be collected by the Government during the application process (e.g., a one-time collection) and the information will be updated by the DIB CS Program participants as personnel changes occur. After joining the program, it is the responsibility of the DIB company to maintain current POC information with the DoD to ensure timely cyber threat information sharing and incident reporting.

7. Paperwork Reduction Act Guidelines

This collection of information does not require collection to be conducted in a manner inconsistent with the guidelines delineated in 5 CFR 1320.5(d)(2).

8. Consultation and Public Comments

Part A: PUBLIC NOTICE

A 60-Day Federal Register Notice (FRN) for the collection published on Friday, August 2, 2024. The 60-Day FRN citation is 89 FR 63183.

No comments were received during the 60-Day Comment Period.

A 30-Day Federal Register Notice for the collection published on Friday, November 22, 2024. The 30-Day FRN citation is 89 FR 91375.

Part B: CONSULTATION

No additional consultation apart from soliciting public comments through the Federal Register was conducted for this submission.

9. Gifts or Payment

No payments or gifts are being offered to respondents as an incentive to participate in the collection.

10. Confidentiality

Companies submitting POC information are required to review and accept a standard Privacy Act Statement after they click on the “Apply to DIB CS Program” icon on when accessing the web portal.

The associated SORN (Defense Industrial Base (DIB) Cybersecurity (CS) Activities Records, DCIO 01) is posted at:
https://dpcld.defense.gov/Portals/49/Documents/Privacy/SORNs/OSDJS/DCIO-01.pdf

The Privacy Impact Assessment for the Defense Industrial Base (DIB) Cybersecurity Activities has been completed, entitled “Defense Industrial Base (DIB) Cybersecurity Activities Updated 2024” and is posted at https://dodcio.defense.gov/Portals/0/Documents/DIB_PIA.pdf

The Records Schedule Number is DAA-0330-2015-0005-0001. The master file consisting of DIB Participant information is temporary, and to be destroyed 3 years after the participating company withdraws from the program, closes, or goes out of business.

11. Sensitive Questions

No questions considered sensitive are being asked in this collection.

12. Respondent Burden and its Labor Costs

Part A: ESTIMATION OF RESPONDENT BURDEN

1) Collection Instrument(s)
   DIBNet Point of Contact Information
   a) Number of Respondents: 8,800
   b) Number of Responses Per Respondent: 1
   c) Number of Total Annual Responses: 8,800
   d) Response Time: 20 minutes
   e) Respondent Burden Hours: 2,933.33 hours

2) Total Submission Burden
   a) Total Number of Respondents: 8,800
   b) Total Number of Annual Responses: 8,800
   c) Total Respondent Burden Hours: 2,933 hours

Part B: LABOR COST OF RESPONDENT BURDEN.

1) Collection Instrument(s)
   DIBNet Point of Contact Information
   a) Number of Total Annual Responses: 8,800
   b) Response Time: 20 minutes
   c) Respondent Hourly Wage: $119.94

    d) Labor Burden per Response: $39.98
    e) Total Labor Burden: $351,824

2) Overall Labor Burden
    a) Total Number of Annual Responses: 8,800
    b) Total Labor Burden: $351,824

The Respondent hourly wage was determined by using the mean wage estimate from the Bureau of Labor Statistics for an Information Security Analyst under Occupational Employment and Wages.[3] This hourly wage is adjusted upward by 100% to account for overhead and benefits, which implies a value of $119.94 per hour.

13. <u>Respondent Costs Other Than Burden Hour Costs</u>

There are no annualized costs to respondents other than the labor burden costs addressed in Section 12 of this document to complete this collection.

14. <u>Cost to the Federal Government</u>

Part A: LABOR COST TO THE FEDERAL GOVERNMENT

1) Collection Instrument(s)

   DIBNet Point of Contact Information
    a) Number of Total Annual Responses: 8,800
    b) Processing Time per Response: 1 hour
    c) Hourly Wage of Worker(s) Processing Responses: $55.76
    d) Cost to Process Each Response: $55.76
    e) Total Cost to Process Responses: $490,688

2) Overall Labor Burden to the Federal Government
    a) Total Number of Annual Responses: 8,800
    b) Total Labor Burden*:* $490,688

The hourly rate for Federal Government personnel was determined by using the OPM Salary Table 2024-GS - Base General Schedule Pay Scale, GS-9, Step 5[4] and is adjusted upward by 100% to adjust for overhead and benefits. This hourly wage is adjusted upward by 100% to account for overhead and benefits, which implies a value of $55.76 per hour.

Part B: OPERATIONAL AND MAINTENANCE COSTS

1) Cost Categories
    a) Equipment: $0
    b) Printing: $0
    c) Postage: $0

[3] BLS Information Security Analyst: https://www.bls.gov/oes/current/oes151212.htm

[4] 2024-GS OPM Salary Table: https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/salary-tables/24Tables/html/GS_h.aspx

d) Software Purchases: $0
e) Licensing Costs: $0
f) Other: $36,244 (Responding to questions from respondents)

2) Total Operational and Maintenance Cost: $36,244*

*Note: Operational and maintenance costs associated with the web portal (https://dibnet.dod.mil) are captured in information collection Control Number 0704-0489 entitled “DoD's Defense Industrial Base (DIB) Cybersecurity (CS) Activities Cyber Incident Reporting.”

Part C: TOTAL COST TO THE FEDERAL GOVERNMENT

1) Total Labor Cost to the Federal Government: $490,688

2) Total Operational and Maintenance Costs: $36,244

3) Total Cost to the Federal Government: $526,932

15. Reasons for Change in Burden

The burden has been adjusted to reflect expanded eligibility to the voluntary DIB CS Program. It is estimated that 10% of the eligible population will elect to join the voluntary DIB CS Program, resulting in 8,000 participating companies and that 10% of companies already participating will provide updated POC information each year, resulting in 8,800 updates per year.[5] Additionally, the latest figures from OPM and BLS were reflected in the labor rates.

16. Publication of Results

The results of this information collection will not be published.

17. Non-Display of OMB Expiration Date

We are not seeking approval to omit the display of the expiration date of the OMB approval on the collection instrument.

18. Exceptions to “Certification for Paperwork Reduction Submissions”

We are not requesting any exemptions to the provisions stated in 5 CFR 1320.9.

[5] 32 CFR Part 236: https://www.federalregister.gov/d/2024-04752/p-60