

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

- None

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 participants provide POC information to DoD during the application process to join the program. This information includes the names, company name and mailing address, work division/group, work email, and work telephone numbers of company-identified POCs. DIB CS program POCs include the Chief Executive Officer, Chief Information Officer, Chief Information Security Officer, General Counsel, Corporate or Facility Security Officer, and the Chief Privacy Officer, 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 (e.g., typically 3-10 company designated POCs.) After joining the program, DIB CS program participants 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," which authorizes the voluntary DIB CS information sharing program. In addition, the Federal Information Security Modernization Act (FISMA) of 2014 authorizes DoD to oversee agency information security policies and practices, for systems that are operated by DoD, a contractor of the Department, or another entity on behalf of DoD that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on DoD's mission. Activities under this information collection also support DoD's critical infrastructure protection responsibilities, as the sector specific agency for the DIB sector (see Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience," available at

<https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

2. Use of the Information

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.

DIB participants voluntarily provide POC information to the DIB CS program via the web portal (<http://dibnet.dod.mil>). On occasion, DIB CS 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. 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 in order to proceed with the application. The privacy notice will be updated once this information collection has been approved since the web portal is maintained by a DoD contractor. DoD must pay for web portal updates, including changes to the privacy page. To minimize the cost to DoD, we will make all the necessary updates to the Privacy Information page once the collection has been approved.

The company is then required to complete the point of contact fields that are provided (i.e., Company Name, Company Representative, CEO, CIO, CISO, and any additional POCs). The online application process does not allow the applicant to submit the information unless they certify that the information provided is accurate by “checking” the certification box. Once all the contact information has been entered, the company clicks on the “submit” button that automatically registers an email notice to the DIB CS Program office that their application has been submitted.

At any point, if a company wants to update the POC information, they access the portal using their 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. Viewing of this data is also restricted to the designated company representatives and the DIB CS program office systems administrators.

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 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 Thursday, July 25, 2019. The 60-Day FRN citation is 84 FRN 35857.

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

A 30-Day Federal Register Notice for the collection published on Monday, September 30, 2019. The 30-Day FRN citation is 84 FRN 51526.

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 (<http://dibnet.dod.mil>). This Privacy Act Statement references the SORN, DCIO 01, "Defense Industrial Base (DIB) Cybersecurity (CS) Activities Records" that is available and posted at:

<http://dpcl.d.defense.gov/Privacy/SORNsIndex/DODComponentArticleView/tabid/7489/Article/570553/dcio-01.aspx>

The publically releasable Privacy Impact Assessment for the Defense Industrial Base (DIB) Cybersecurity Activities has been completed and posted at:
http://dodcio.defense.gov/Portals/0/Documents/PIA_DIB%20CS%20program_Aug%202015_corrected.pdf?ver=2016-09-22-113831-737r

Records retention and disposition schedule was approved by the National Archives and Records Administration on 12 August 2015. 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)

<http://dibnet.dod.mil>

- a) Number of Respondents: 935
- b) Number of Responses Per Respondent: 1
- c) Number of Total Annual Responses: 935
- d) Response Time: 20 mins
- e) Respondent Burden Hours: 312 hours

2) Total Submission Burden (Summation or average based on collection)

- a) Total Number of Respondents: 935
- b) Total Number of Annual Responses: 935
- c) Total Respondent Burden Hours: 312 hours

Part B: LABOR COST OF RESPONDENT BURDEN.

1) Collection Instrument(s)

<http://dibnet.dod.mil>

- a) Number of Total Annual Responses: 935
- b) Response Time: 20 mins
- c) Respondent Hourly Wage: \$43.36
- d) Labor Burden per Response: \$14.45
- e) Total Labor Burden: \$13,513.87

2) Overall Labor Burden

- a) Total Number of Annual Responses: 935
- b) Total Labor Burden: \$13,513.87

The Respondent hourly wage was determined by using the [Department of Labor Wage Website] (<http://www.dol.gov/dol/topic/wages/index.htm>)

13. Respondent Costs Other Than Burden Hour Costs

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. Cost to the Federal Government

Part A: LABOR COST TO THE FEDERAL GOVERNMENT

1) Collection Instrument(s)

<http://dibnet.dod.mil>

- a) Number of Total Annual Responses: 935
- b) Processing Time per Response: 1 hours
- c) Hourly Wage of Worker(s) Processing Responses : \$23.25
- d) Cost to Process Each Response: \$23.25
- e) Total Cost to Process Responses: \$21,738.75

2) Overall Labor Burden to the Federal Government

- a) Total Number of Annual Responses: 935
- b) Total Labor Burden: \$21,738.75

Part B: OPERATIONAL AND MAINTENANCE COSTS

1) Cost Categories

- a) Equipment: \$0
- b) Printing: \$0
- c) Postage: \$0
- d) Software Purchases: \$0
- e) Licensing Costs: \$0
- f) Other: \$0

2) Total Operational and Maintenance Cost: \$0

Part C: TOTAL COST TO THE FEDERAL GOVERNMENT

1) Total Labor Cost to the Federal Government: \$21,738.75

2) Total Operational and Maintenance Costs: \$0

3) Total Cost to the Federal Government: \$21,738.75

15. Reasons for Change in Burden

There has been no change in burden since the last approval.

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" (1 sentence)

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