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

- Change in total number of responses: 935 cleared defense contractors to 7,590 defense contractors that process, store, develop, or transmit DoD controlled unclassified information
- Changes in respondent burden hours: 312 hours to 2,530 hours
- Labor cost to the federal government: $22,580.25 to $188,080.20

1. Need for the Information Collection

DoD's Defense Industrial Base (DIB) Cybersecurity (CS) Program enhances and supports DIB CS 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 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 names and mailing address, work divisions/groups, work email addresses, and work telephone numbers of company-identified POCs. DIB CS Program POCs include the Chief Executive Officer (CEO), Chief Information Officer (CIO), Chief Information Security Officer (CISO), 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 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)'s 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 process 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 policy 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 participants. DoD needs to collect POC information to implement, manage, and administer the Program, and to share cyber threat information with participants. The Government will collect business POC information from all DIB CS participants to facilitate emails, teleconferences, meetings, and other Program activities.

The DIB CS Program uses a web portal (https://dibnet.dod.mil) to gather POC information from DoD contractors when they elect to participate in the Program. Companies select the "Apply Now!" button to start the application process. Applicants will then be prompted to sign into the application with a valid DoD-approved medium assurance certificate. They are then directed to a DoD Information System Standard Notice and Consent banner that indicates they are accessing a U.S. Government information system and must be click the "I Agree" button in order to continue. The next page is the DoD Privacy Statement that includes the Authorities, Purpose, Routine Use(s), Disclosure, Privacy Impact Assessment (PIA), Freedom of Information Request (FOIA) disclaimers, and an Agency Disclosure Notice, which must be agreed to by the company by clicking the "I Agree" button in order to proceed with the application.

Applicants are then required to complete the POC fields that are provided (i.e., Company Name, Company Representative, CEO, CIO, CISO, and any additional POCs). The online application process does not allow applicants to submit the information unless they certify that the information provided is accurate by checking the "Certify Application" box. After entering all contact information, applicants click on the "Submit Application" button that automatically sends an email to the DIB CS Program Office that an application has been submitted.

If companies want to update their POC information, they can access the portal using their DoD-approved medium assurance certificates. Only designated company representatives and the DIB CS Program system administrators may view or update company POC information.

3. Use of Information Technology

100% of the POC information provided by DIB CS participants 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

POC information will be collected by the Government during the application process (e.g., a one-time collection) and updated by DIB CS participants as personnel changes occur. The Government will make every attempt to minimize the burden on DIB CS participants by verifying POC information whenever possible/feasible during telephone calls, email exchanges, meetings, or other Program activities.

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 companies' responsibility 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, May 29, 2020. The 60-Day FRN citation is (85) FRN (32366).

A 30-Day Federal Register Notice for the collection published on Thursday, August 27, 2020. The 30-Day FRN citation is (85) FRN (52967).

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 Now!" button on the web portal (https://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://dpcld.defense.gov/Privacy/SORNsIndex/DODComponentArticleView/tabid/7489/Article/570553/dcio-01.aspx . An updated, draft copy of the SORN (DCIO 01, Defense Industrial Base (DIB) Cybersecurity (CS) Activities Records), has been provided with this package for OMB's review.

The publically releasable "Privacy Impact Assessment for the Defense Industrial Base (DIB) Cybersecurity Activities" can be found using the link provided below. An updated, draft copy of the PIA, Defense Industrial Base (DIB) Cybersecurity Activities, has been provided with this package for OMB's review.
https://dodcio.defense.gov/Portals/0/Documents/DIB%20CS%20PIA%20for%20Public%20Release_July2017.pdf?ver=2017-08-07-115131-963

Records retention and disposition schedule was approved by the National Archives and Records Administration on 12 August 2015. The Disposition Authority Number is DAA-0330-2015-0005-0001. The master file consisting of DIB CS participant information is temporary, and will be destroyed 3 years after participating companies withdraw from the Program, close, or go 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
   [Defense Industrial Base (DIB) Cybersecurity (CS) Program Company Application Process*]
   a) Number of Respondents: 7,590
   b) Number of Responses Per Respondent: 1
   c) Number of Total Annual Responses: 7,590
   d) Response Time: 20 minutes
   e) Respondent Burden Hours: 2,530 hours
   *https://dibnet.dod.mil/portal/intranet/

2) Total Submission Burden
   a) Total Number of Respondents: 7,590
   b) Total Number of Annual Responses: 7,590
   c) Total Respondent Burden Hours: 2,530 hours

Part B: LABOR COST OF RESPONDENT BURDEN

3) Collection Instrument
   [Defense Industrial Base (DIB) Cybersecurity (CS) Program Company Application Process*]
   a) Number of Total Annual Responses: 7,590
   b) Response Time: 20 minutes
   c) Respondent Hourly Wage: $46.23
   d) Labor Burden per Response $15.25
   e) Total Labor Burden: $115,792.28

*https://dibnet.dod.mil/portal/intranet/

4) Overall Labor Burden
    a) Total Number of Annual Responses: 7,590
    b) Total Labor Burden: $115,792.28

The Respondent hourly wage was determined by using the [Department of Labor Wage Website] (http://www.bls.gov/oes/current/oes151121.html)

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
   [Defense Industrial Base (DIB) Cybersecurity (CS) Program Company Application Process*]
    a) Number of Total Annual Responses: 7,590
    b) Processing Time per Response: 1 hour
    c) Hourly Wage of Worker(s) Processing Responses : $24.78/hour
    d) Cost to Process Each Response: $24.78/hour
    e) Total Cost to Process Responses: $188,080.20
   *https://dibnet.dod.mil/portal/intranet/

2) Overall Labor Burden to the Federal Government
    a) Total Number of Annual Responses: 7,590
    b) Total Labor Burden: $188,080.20

The Respondent hourly wage was determined by using the [OPM Wage Website - Base General Schedule Pay Scale, GS-9, Step 5] (https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/salary-tables/20Tables/html/GS_h.aspx).

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: $188,080.20

2) Total Operational and Maintenance Costs: $0

3) Total Cost to the Federal Government: $188,080.20

15. Reasons for Change in Burden

The burden has increased since the previous approval due to DoD making revisions to 32 CFR part 236 which would expand the eligibility criteria in the DIB CS Program. The expanded eligibility criteria would allow a broader community of defense contractors to participate in the Program expanding from 8,500 cleared defense contractors to defense contractors to 69,000 defense contractors who process, store, develop, or transmit DoD CUI. These changes will increase the number of respondents within this document from 935 to 7,590.

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.