SUPPORTING STATEMENT – PART A

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

A. JUSTIFICATION

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

- While POC information regarding DIB CS participants may possibly be found on the web in various forums, the information may be unreliable, missing, or out-of-date. The only way to have accurate POC information is to have direct input from the DIB CS participants.

5. Burden on Small Business

- 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. The Government will make every attempt to minimize the burden on DIB 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 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

- Information is collected consistent with 5 CFR 1320.5(d)(2). No special circumstances are required.

8. Consultation and Public Comments

- As required by 5 CFR 1320.8(d), the notice of information collection was published on 29 April 2016 in the Federal Register at 81 FR 25655 soliciting comments. No public comments were received.

- The DIB CS program office communicates with the company POCs on a quarterly basis, primarily through email. While we rely on the companies to provide updates as their points of contact change, the quarterly outreach allows us to validate the accuracy of the information. When the DIB CS program discovers any inaccurate POC information, it notifies the DIB CS participant by email to update their POC information via the web portal (http://dibnet.dod.mil).

- A 30-Day Federal Register Notice for the collection published on September 28, 2016. The 30-Day FRN citation is 81 FR 66642

9. Gifts or Payment

- The Government will provide no payment or gifts to respondents.

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://dpcld.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 on12 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

- Sensitive private information is not collected. A Privacy Impact Assessment addresses the processes in place to protect information provided by a DIB CS participant in the event of an inadvertent disclosure of personally identifiable information (PII) by DIB CS participants as part of the DIB CS program. The Government will make full use of the exemptions of the Freedom of Information Act to protect against unauthorized public disclosure of attribution, proprietary, or other non-public information provided by a DIB CS participant. However, the Government cannot guarantee that information provided will never be subject to release, if the information cannot qualify for any FOIA exemptions.

12. Respondent Burden, and its Labor Costs

   a. Estimation of Respondent Burden

	Estimation of Respondent Burden Hours				
	Number of Respondents	Number of Responses per Respondent	Number of Total Annual Responses	Response Time/Minutes (Amount of time needed to complete the collection instrument)	Respondent Burden Hours (Total Annual Responses multiplied by Response Time) Please compute these into hours)
http://dibnet.dod.mil	935	1	935	20 mins	312
Total	935	1	935	20 mins	312

   b. Labor Cost of Respondent Burden

	Labor Cost of Respondent Burden				
	Number of Responses	Minutes/Response Time per Response	Respondent Hourly Wage	Labor Burden per Response (Response Time multiplied by Respondent	Total Labor Burden (Number of Respondents multiplied by Response Time multiplied by

				Hourly Wage)	Respondent Hourly Wage)
http://dibnet.dod.mil	935	20 mins	$43.36	$14.45	$13,513.87
Total	935	20 mins	$43.36*****	$14.45	$13,513.87

* Mean hourly wage according to the Bureau of Labor Statistics for a Computer Systems Analyst, Occupational Employment and Wages, May 2015. For additional information on the mean hourly wage, please visit http://www.bls.gov/oes/current/oes151121.htm.

13. Respondent Costs Other Than Burden Hour Costs

- There are no other costs other than burden hour costs. There are no O&M costs to the respondent.

14. Cost to the Federal Government

Labor Cost to the Federal Government		
	http://dibnet.dod.mil	Total
Number of Responses	935	935
Processing Time Per Response (in hours)	1	1
Hourly Wage of Worker(s) Processing Responses	$23.25*****	$23.25
Cost to Process Each Response (Processing Time Per Response multiplied by Hourly Wage of Worker(s) Processing Responses)	$23.25	$23.25
Total Cost to Process Responses (Cost to Process Each Response multiplied by Number of Responses	$21,738.75	$21,738.75

* Mean hourly wage according to Base General Schedule Pay Scale, GS-9, Step 5. For more information on the hourly wage scale, please visit http://www.federaljobs.net/salarybase.htm#2016_HOURLY_RATE_SCHEDULE.

Operational and Maintenance Costs						
Equipment	Printing	Postage	Software Purchases	Licensing Costs	Other	Total
$0	$0	$0	$0	$0	$0	$0

Total Cost to the Federal Government		
Operational and Maintenance Costs	Labor Cost to the Federal Government	Total Cost (O&M Costs + Labor Cost)
$0	$21,738.75	$21,738.75

15. Reasons for Change in Burden

- This collection is an existing requirement under OMB control number 0704-0490. The burden is all the same except for the annual cost burden, which has increased since the last submission. The reason for this increase is due to the hourly labor rate increasing over the past 3 years.

16. Publication of Results

- The results will not be published. The use and protection of the information would occur under the conditions prescribed in the Interim Federal Rule for the protection of attribution and proprietary information.

17. Non-Display of OMB Expiration Date

- DoD is not requesting approval to omit display of the expiration date of OMB approval on the instrument of collection.

18. Exceptions to "Certification for Paperwork Reduction Submissions"

- DoD is not requesting an exception to the certification for paperwork reduction submissions.