SUPPORTING STATEMENT
DIB CS/IA Point of Contact Information Collection
(Refer to OMB Form 83-I INST)

A. JUSTIFICATION:

1. Need for the information collection

The DIB CS/IA 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 information for program administration and management purposes. The Government will collect typical business points of contact (POC) information from all Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) program participants to facilitate communication, pass security clearances, share unclassified and classified cyber threat information, and report DIB cyber incidents to DoD. To implement and execute this program within their companies, DIB 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 POCs include the Chief Executive Officer, Chief Information Officer, Chief Information Security Officer, General Counsel, and the Corporate or Facility Security Officer, the Chief Privacy Officer, or their equivalents, as well as those administrative, policy, technical staff, or personnel designated to report incidents, who will interact with the Government in executing the DIB CS/IA program (e.g., typically 3-10 company designated points of contact.) After joining the program, DIB companies provide updated POC information to DoD when personnel changes occur.

2. Use of the information

The DIB CS/IA Program is focused on sharing information assurance and cyber security related information. The operational implementation of this program requires DoD to collect, share and manage point of contact for program administration and management purposes. The Government will collect typical business POC information from all DIB CS/IA program participants to facilitate emails, teleconferences, meetings, and other program activities.

The DIB CS/IA Program works with cleared defense contractors. For the administration and management of the program, there are two instances in which DoD requires validation of an individual's citizenship and security clearance.

- First, confirmation of a valid and current security clearance, including level of clearance, is required in order for the government to share classified threat information, or hold classified meetings. Through the routine government processes to pass clearances, an individual's name, social security number, citizenship, and security clearance are provided to appropriate government, or contractor, security offices. To receive classified threat information, DIB participant points of contact have security clearances on file with

DoD CIO Security Office and DC3. For classified meetings, security clearances are passed by both government and contractor attendees to the appropriate security offices, depending on the location of the meeting.

- The information provided for the passing of security clearances, is not collected on the online application, nor is it collected in support of a network intrusion incident report. Rather, this information is part of routine government processes to pass clearances.
- Secondly, during the application process to join the program DoD also must ensure compliance with the security-based elements of the program's eligibility requirements.
- As background, during the planning stages to open the program, DoD CIO discussed with Defense Security Service (DSS) and the Security and Counterintelligence directorates in the Under Secretary of Defense for Intelligence the potential for unknown actors to attempt to spoof identities to appear to be legitimate applicants. To ensure the continued security of the program, DSS provided DoD CIO access to the DSS Industrial Security Facilities Database (ISFD), which lists information on each cleared defense contractor company, in accordance with the National Industrial Security Program (NISP). Each cleared defense contractor has official Company and Facility Security Officers (CSO/FSO) point of contact information on record in the ISFD.
- During the application process, the applicant is required to "certify that the information provided is accurate to the best of their knowledge" and that they "understand DoD will confirm the accuracy of the information." The online application process does not allow the applicant to submit the information unless the certification box is checked.
- To confirm the accuracy of the information provided by the applicant, DoD will use the ISFD to contact the company CSO/FSO of the applicant to confirm that the applicant is: 1) a current employee of the company, 2) is a U.S. citizen, and 3) that the POC information provided in the application by the applicant is correct. DoD intends to contact company CSO/FSO using the contact information DSS has on record for the company. DoD confirmation of the information is not tracked on the POC forms.
  - If the CSO/FSO confirms that the data provided is accurate, the applicant receives notice that they may continue in the application process.
  - If the CSO/FSO confirms that the data provided is inaccurate, the applicant receives notice that the information provided was not confirmed by the company's CSO/FSO of record.

a. <u>Relevant Statutes/Regulations</u>

The following statutes and policy guidance identifies cyber threat information sharing as an urgent national-level priority and supports the collection of information from the DIB. This guidance includes the collection, management and sharing of information for cyber security purposes, supports and implements national and DoD-specific guidance and authority.

(1) Information Assurance (IA)

DoD is required by statute to establish programs and activities to protect DoD information and DoD information systems, including information and information systems operated and maintained by contractors or others in support of DoD activities. Section 2224 of Title 10, U.S. Code (U.S.C.), requires DoD to establish a Defense IA Program to protect and defend DoD information, information systems, and information networks that are critical to the Department during day-to-day operations and operations in times of crisis. (10 U.S.C. § 2224(a)) The program must provide continuously for the availability, integrity, authentication, confidentiality, non-repudiation, and rapid restitution of information and information systems that are essential elements of the Defense information infrastructure. (10 U.S.C. § 2224(b)) The program strategy also must include vulnerability and threat assessments for defense and supporting non-defense information infrastructures, joint activities with elements of the national information infrastructure, and coordination with representatives of those national critical infrastructure systems that are essential to DoD operations. (10 U.S.C. § 2224(c)) The program must provide for coordination, as appropriate, with the heads of any relevant federal agency and with representatives of those national critical information infrastructure systems that are essential to the operations of the Department regarding information assurance measures necessary to the protection of these systems. (10 U.S.C. § 2224(d))

The Defense IA Program also must ensure compliance with Federal IA requirements provided in the Federal Information Security Management Act (FISMA), 44 U.S.C. § 3541 et seq. FISMA requires all federal agencies to provide information security protections for information collected or maintained by, or on behalf of, the agency. Information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency must be in accordance with 44 U.S.C. § 3544(a)(1)(A). Agencies are expressly required to develop, document, and implement programs to provide information security for information and information systems that support the operations and assets of the agency, including those provided by another agency, contractor, or other source in accordance with 44 U.S.C. § 3544(b).

3. Use of Information Technology

Yes, technological collection techniques are an option for DIB companies to share their POC information. DIB participants voluntarily provide POC information to the DIB CS/IA program via email, telephone, fax, in person or web portal.

4. Non-duplication

While POC information regarding DIB 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 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 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 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 in the Federal Register on May 11, 2012, page 27615 soliciting comments. No public comments were received during this 60-day public comment period; however, OMB received comments from Tech America during their review of the collection. DoD provides the below response:

Tech America commented that our estimated annual burden was understated, specifically because the estimated number of respondents was too low. More specifically, DoD estimated 250 respondents, and Tech America suggested that 750 respondents would be more accurate, in part because a related information collection review for the DIB CS/IA Cyber Incident Reporting, OMB Control Number 0704-0489, had estimated that the program may grow by up to 250 additional participants each year, reaching up to 750 in the third year. DoD agrees that the number of the respondents for the DIB CS/IA program should be consistent for both the POC information, and the cyber incident reporting. DoD has reviewed our estimates for both of these information collections, and conclude that the estimates for the POC information collection are more accurate, while the initial estimates for cyber incident reporting overstated the annual burden by overestimating the number of respondents. By May 2013, approximately the end of the first year of the DIB CS/IA program operations under the interim rule published in May 2012, there were nearly 80 participants. Based on this information, and adjusted for anticipated future growth in the number of participants each year, DoD estimates that not more than 250 companies will respond to the initial information collection request for POC information each year (this estimate will also be applied to the cyber incident reporting information collection review). As noted in your comments, the estimated 1.1 responses per respondent and average burden of 20 minutes per response, appears to be a reasonable and accurate estimate, thus resulting in a total estimated annual burden of 92 hours for this POC information collection. Information will be collected during the application process to join the program. After joining the program, it is the responsibility of the DIB participants to provide changes to the Government as personnel changes occur.

9. Gifts or Payment

The Government will provide no payment or gifts to respondents

10. Confidentiality

The publically releasable version of the Privacy Impact Assessment for the DIB CS/IA Activities has been completed and posted at: http://dodcio.defense.gov/Portals/0/Documents/DIB%20CS-IA%20PIA_FINAL_signed_30jun2011_VMSS_GGMR_RC.pdf

a. SORN system identifier and name: DCIO 01, entitled "Defense Industrial Base (DIB) Cyber Security/Information Assurance Records." The SORN is attached.

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 participant and in the event of an inadvertent disclosure of PII by DIB participants as part of the DIB CS/IA 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 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

The estimated annual respondent burden report in Item 13 of OMB Form 83-I is a function of the annual number of responses provided to the Government by DIB participants and the estimated amount of time required for each response (for each participant to collect and report such information) to the Government. The projections below are rounded to the nearest hour and are based on current available data and best estimates. Additional data will become available through program implementation to validate future burden projections. The following chart specifies the annual number of respondents showing tiered Growth:

Estimation of Respondent Burden

Year	Number of Respondents	Number of Responses*	Minutes/ Response	Annual Hours
1	250	275	20	92
2	250	275	20	92
3	250	275	20	92

* Number of responses includes one response per DIB participant plus an additional 10% per year included for updates, as required.

b. Labor Cost of Respondent Burden

Annual Burden on Respondents

Year	Total Number of Responses	Minutes/ Response	Labor Cost/Hr	Total Cost
1	275	20	$36.41*	$3,337
2	275	20	$36.41*	$3,337
3	275	20	$36.41*	$3,337

* Mean hourly wage according to the Bureau of Labor Statistics for a Computer Systems Analyst, Occupational Employment and Wages, May 2010.

The table above is the total annualized cost to respondents imposed by the collection of cyber incident reporting. The cost for a DIB participant is estimated at $36.41 per hour. The time required to complete the incident reporting form is approximately twenty minutes. Therefore, the annual cost for a DIB participant to submit the required POC information could be as low as $12.00.

13 Respondent Costs Other Than Burden Hour Costs.

a. There are no other costs other than burden hour costs.

b. There are no O&M costs to the Respondent.

14. Cost to the Federal Government

Annual Labor Cost to Government

Year	Total Number of Responses	Labor Hrs /Response	Labor Cost/Hr	Total Cost
1	275	1	$28.55*	$7,851
2	275	1	$28.55*	$7,851
3	275	1	$28.55*	$7,851

*Mean hourly wage according to Base General Schedule Pay Scale, GS-9, Step 5.

The Government estimates that it will take one (1) hour to review and process the POC information reported from each DIB participant with a projected an annual labor cost to the Government of $7,851.

15. Reasons for Change in Burden

This is a reinstatement of a previously approved public information collection.

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 exceptions.

B. COLLECTIONS OF INFORMATION EMPLOYING STATISTICAL METHODS:

The information collection under the program does not employ statistical methods.