SUPPORTING STATEMENT
DoD-Defense Industrial Base (DIB) Cybersecurity (CS) Activities
Point of Contact Information Collection
(Refer to OMB Form 83-I INST)

A. JUSTIFICATION:

1. Need for the information collection

Describe the information collection activity under review. Explain precisely why it is necessary; i.e., why the Department of Defense needs the information required by the proposed collection.

This updated information collection reinstates and changes Defense Industrial Base Cybersecurity Activities Points of Contact (POC) Information. Under the voluntary threat information sharing program, the Government will collect points of contact (POC) information from all Defense Industrial Base (DIB) Cybersecurity (CS) program participants to facilitate communication between the Government and participating DIB companies. The eligible population for the voluntary program has expanded from 2,650 to 8,500 cleared defense contractors. DIB participants provide POC information for personnel responsible for the implementation and execution of the DIB CS program within their company. This information includes the name, company name and mailing address, work division/group, work email, and work telephone numbers of the Chief Executive Officer, Chief Information Officer, Chief Information Security Officer, General Counsel, and the Corporate or Facility Security Officer, or their equivalents, as well as those policy or technical staff personnel that will interact with the Government in executing the DIB CS program (e.g., typically 3-10 company designated points of contact.)

2. Use of the information

Be specific in describing how, by whom, and for what purpose the information is to be used. Unless this is a new collection, describe how the information has been used in the past. Identify all formats used to collect the information in this paragraph. Identify any legal or administrative requirements that mandate the collection, and include the title page and relevant portions thereof in your proposal package.

Information is necessary for the Government to interact with the DIB participants implementing the DIB CS program in their companies. This includes facilitating the Government response to voluntary cyber incident threat reporting by DIB participants, or inviting DIB participants to periodic working groups or teleconferences to address the cyber threat.

a. Relevant Statutes/Regulations

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 cybersecurity purposes, supports and implements national and DoD-specific guidance and authority.

(1) Cybersecurity (CS)

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. 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

Does the information collection involve the use of technological collection techniques; e.g., electronic response submission?

DIB participants will voluntarily provide POC information to the DIB CS program via email, telephone, fax, in person or web portal.

4. Non-duplication

Is there information already available which can be used, or modified for use, for the purposes of this collection?

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

5. Burden on Small Business

If any of the respondents are small businesses or other small entities, discuss efforts taken to minimize the burden imposed by this collection; i.e., developing separate or simplified requirements, etc.

POC information will be collected by the Government on a one-time basis and the information will be updated by the DIB participants as 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 or meetings.

6. Less Frequent Collection

What would be the consequences if the collection were conducted less frequently? If there are technical or legal obstacles to reducing the burden in this manner, explain.

Keeping an accurate database on POC information for DIB participants must be done routinely on a continuing basis. As personnel change positions in a company or new technical POCs are identified, this information is needed by the Government. Less frequent collection may result in information possibly being misrouted or sent to the wrong individual(s) within DIB participating company.

7. Paperwork Reduction Act Guidelines

Explain any special circumstances that require the collection to be conducted in a manner inconsistent with the guidelines delineated in 5 CFR 1320.5(d)(2).

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

8. Consultation and Public Comments

a. Identify the date and page number of publication in the Federal Register of the Agency's 60-day notice, required by 5 CFR 1320.8(d), soliciting comments on the information collection prior to submission to OMB. Include a summary of any public comments received as a result of the 60-day Federal Register Notice, and address actions taken in response to those comments. If no comments were received, so state.

Date of Federal Register publication– TBD. Public comments- TBD.

b. Describe efforts made to consult with persons outside the sponsoring Agency regarding availability of requested information, frequency of collection, clarity of instructions,

etc. Consultation with respondents, or their representatives, should occur at least every 3 years, even if the information collection does not change. If there are circumstances that mitigate against consultation, explain. This item does not refer to consultants, per se. Rather, it addresses the act of consulting with others to determine continued viability of collection elements, procedures, etc.

Information will be solicited and collected on a one-time basis and DIB participants will provide changes to the Government as POCs change.

9. Gifts or Payment

Explain any decision to provide payment or gifts to respondents, other than remuneration of contractors or grantees.

The Government will provide no payment or gifts to respondents

10. Confidentiality

Describe the extent of confidentiality inherent in the information collection. Address such things as protection provided against disclosure of information containing personal or organizational identifiers, disposal of completed forms or surveys, etc.

When an assurance of confidentiality is provided, the respondent is being asked to submit proprietary, trade secret, or confidential information to the agency. In turn the agency is assuring the respondent that it has instituted procedures to protect the confidentiality of the information to the extent permitted by law. Some laws governing confidentiality carry large penalties for the agency if the information is not protected properly. In addition, collections including an assurance of confidentiality must be supported by an authority established in statute or regulation.

Specifically address any assurance of confidentiality provided to respondents. Explain the basis for this assurance as provided in statute, regulation, or Agency policy.

Provide the Privacy Act System of Records Notice (SORN) ID number and title and address whether or not a Privacy Impact Assessment has been accomplished. Include a copy of the SORN and the PIA in the information collection package.

a. The Privacy Impact Assessment for the DIB CS Activities is posted at: http://cio-nii.defense.gov/docs/DIB%20CS-IA%20PIA_FINAL_signed_30jun2011_VMSS_GGMR_RC.pdf

b. The SORN, DCIO 01, entitled “Defense Industrial Base (DIB) Cybersecurity Records” is attached

11. Sensitive Questions

Provide thorough justification for any questions of a sensitive nature, such as those pertaining to sexual behavior or attitudes, religious beliefs, race and/or ethnicity, or other matters usually considered private such as the collection of the SSN. Does the question violate the Privacy Act (Reference (w)), as implemented by DoD 5400.11-R (Reference (k))? What explanation of the necessity for collecting this data will be provided the respondents prior to their responding?

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 program. The Government will make full use of the exemptions of the Freedom of Information Act to protect against disclosure of attribution or proprietary information provided by a DIB participant.

12 Respondent Burden, and its Labor Costs

a. Estimation of Respondent Burden

Explain how the burden estimate reported in Item 13 of the OMB Form 83-I was determined. While not required, consultation with a sample of the potential respondents is desirable. Remember, however, that your sample must be of fewer than 10 potential respondents or the sample effort itself must be approved by OMB. If the collection consists of more than a single instrument of collection; i.e., form, survey, questionnaire, etc., provide burden estimates for each instrument, and aggregate the total burden in Item 13, of OMB Form 83-I.

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	850	935	20	312
2	850	935	20	312
3	850	935	20	312

* While the number of DoD contractors impacted is 8,500, DoD estimates that no more than 10% of the total eligible population of cleared defense contractors will apply to the voluntary DIB Cybersecurity Activities program resulting in 850 cleared defense contractors impacted annually. An additional 10% of the population or 85 contractors may provide updated points of contact for the program, as required.

b. Labor Cost of Respondent Burden

Provide an estimate of annualized cost to respondents of only the burden hours imposed by the collection. Do not include capital, start-up, contracting out, or operations and maintenance costs. Respondent cost other than burden hour costs should be shown in Item 13 of the Supporting Statement.

Annual Burden on Respondents

Year	Total Number of Responses	Minutes/ Response	Labor Cost/Hr	Total Cost
1	935	20	$38.41*	$11,984
2	935	20	$38.41*	$11,984
3	935	20	$38.41*	$11,984

* Mean hourly wage according to the Bureau of Labor Statistics for a Computer Systems Analyst, Occupational Employment and Wages, January 2014.

The table above is the total annualized cost to respondents imposed by the collection information pertaining to cyber threat information sharing. The cost for a DIB participant is estimated at $38.41 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 $13.00.

13 Respondent Costs Other Than Burden Hour Costs.

Provide an estimate of annualized costs to respondents, other than the burden hour costs addressed in Item 12, resulting from the collection of information. This item expands upon the entries in Item 14 of OMB Form 83-I. Break this item into two components:

a. Total capital and start-up costs annualized over the expected useful life of the item(s). Capital and start-up costs include the purchase of computers and software; testing equipment; and record storage facilities.

There are no other costs other than burden hour costs.

b. Total operation and maintenance costs take into account those costs associated with generating, maintaining, and disclosing or providing the information. O&M costs include such activities as contracting out for services and operational expenses, e.g., postage and printing.

There are no O&M costs to the Respondent.

14. Cost to the Federal Government

Annualize the costs incurred by the Federal Government in collecting and processing the information collected, and explain the methods used in determining these estimates. Include such elements as quantification of hours, operational expenses; i.e., equipment, overhead, printing, support staff, postage, contracting out for services, etc., and any other expense that would not have been incurred without this information collection. These costs, along with those estimated in items 12 and 13, may be aggregated in a single table.

Annual Labor Cost to Government

Year	Total Number of Responses	Labor Hrs /Response	Labor Cost/Hr	Total Cost
1	935	1	$28.6*	$26,741
2	935	1	$28.6*	$26,741
3	935	1	$28.6*	$26,741

*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 $26,741.

15. Reasons for Change in Burden

Briefly explain the reason for change in burden, if any, as indicated in Item 13 of OMB Form 83-I. Remember that any proposal which starts from a current OMB inventory of "0" hours must be a Program Change, e.g., reinstatement of a previously approved collection for which approval has expired or a new collection. (See OMB Form 83-I for explanation of program change or program adjustment.)

This requirement is not applicable to the DIB CS program.

16. Publication of Results

If the results of the information collection will be published for statistical use, outline plans for tabulation, statistical analyses, and publication. Provide a timeline for the entire project including the beginning and ending dates of the actual collecting of information, estimated completion date of the report, its publication date, as well as any other scheduled actions.

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

If you are requesting approval to omit display of the expiration date of OMB approval on the instrument of collection, provide justification for this request.

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"

Use this item to explain any provision of Item 19.a of OMB Form 83-I to which you cannot certify. You should also have identified these items at the bottom of Item 19.a. Unless you can demonstrate that these exceptions are necessary to satisfy statutory requirements, or other substantial need, OMB will not approve the collection of information.

DoD is not requesting exceptions.

B. COLLECTIONS OF INFORMATION EMPLOYING STATISTICAL METHODS:

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