SUPPORTING STATEMENT
DIB CS/IA Cyber Incident Reporting Information Collection
(Refer to OMB Form 83-I INST)

A. JUSTIFICATION:

1. Need for the information collection.

The information collected supports the execution of the voluntary DIB CS/IA program to enhance and supplement DIB participant's capabilities to safeguard Department of Defense (DoD) information that resides on, or transits, DIB unclassified information systems. The requested information supports the collaborative cyber threat information sharing and incident reporting partnership between DoD and the DIB. The Incident Collection Form (ICF) supports the operational implementation of DIB CS/IA incident reporting and response. The purpose for collecting POC information on the ICF is to provide sufficient contact information for the DC3/DCISE to follow-up with the company reporting an incident (e.g., a known or suspected compromise to DoD information that resides on, or transits, the company's unclassified information systems).

- Each DIB participant identifies personnel that are authorized to submit an ICF to DC3. Typically, the authorized personnel are comprised of technical staff and their network responders. These technical points of contact are key to rapid network defense of DIB networks, and therefore are authorized to collaborate with DoD on rapid mitigation/remediation strategies to incidents. These personnel are not, however, the company's senior corporate officials and staff that manage overall participation in the DIB CS/IA program for the company. Key corporate official POC information is collected during the application process.

2. Use of the information

In most cases, DIB participants report cyber incidents using a DIB CS/IA program standardized ICF, which is submitted to the DoD-DIB Collaborative Information Sharing Environment (DCISE) that is part of the DoD Cyber Crime Center (DC3). The DIB participant can download the ICF, complete it, and submit it via encrypted email or fax, or they can submit the data via an online web location. In some cases, a DIB participant may elect to report the incident without using the ICF through a variety of communications channels, including email, fax, or by phone.

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 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

DIB participants will provide their incident information using the following options:

(1) Download, complete and submit the ICF, via encrypted email using DoD-approved medium assurance certificates. (Fax can be used as an alternative)

(2) Complete and submit data with DoD-approved medium assurance certificates via an online web form.

The use of technology (e.g., forms software and online access) will decrease the respondent reporting burden. If respondents choose to use the electronic ICF, it will standardize data entry and allow respondents to make data entry selections by checking appropriate boxes, enabling digital signatures, and automate email delivery using software macros. The online web form provides similar, user-friendly conveniences.

4. Non-duplication

No. The information voluntarily provided by respondents includes timely and detailed reporting on cyber incidents that affect DoD programs and missions, which is not routinely provided to the Government.

5. Burden on Small Business

The Government strives to minimize the information collection burden imposed on small businesses and only requests the minimum amount of information necessary to establish the technical character of a cyber incident, and the minimum amount of information needed to validate a cyber intrusion damage assessment.

6. Less Frequent Collection

DIB participants complete and submit a DIB CS/IA cyber incident report on an “as needed” basis following unauthorized access to an unclassified DIB network that compromises DoD program information and missions.

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 the 60-day public comment period; however, OMB received comments from Tech America during their review. DoD provides the following response:

Tech America commented that our estimated annual burden was understated, specifically because the estimated number of respondents was too low. DoD has reviewed our estimates and conclude that the initial estimates overstated the annual burden for this information collection by overestimating the number of respondents. The initial estimate of 750 respondents was based on the potential for the program to accommodate up to 250 additional participants (i.e., respondents) each year, reaching up to 750 by the third year. However, 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 adjusting for anticipated future growth in the number of participants each year, DoD estimates that not more than 250 companies will respond to the information collection request for incident reporting each year (i.e., a downward adjustment from the initial estimate of 750). In addition, DoD’s review of the incident reporting trends continues to support the initial estimated number of reports projected per each respondent: 5. Thus, the revised estimated total number of annual projected responses is 1,250 reports (adjusted downward from the initial estimate of 3,750). Similarly, DoD's review supports the initial estimated average burden per response to be 7 hours.

In estimating this average burden, it is important to understand that the respondents are only asked to report information on those cyber incidents that they have already identified in the course of their normal cybersecurity activities, and more specifically only on those incidents that indicate a compromise or potential compromise of information related to DoD programs. DoD agrees that the respondents will need to review cyber incident information that they have already compiled and collected to determine which of those incidents meet the reporting criteria, share any qualifying incident reports under the DIB CS/IA program, and DoD concludes that the initial estimated average burden for this activity is accurate. Accordingly, the revised total annual estimated burden is 8,750 hours.

9. Gifts or Payment

The Government will provide no payment or gifts to respondents.

10. Confidentiality

a. 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

b. 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, as well as 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 disclosure of attribution or proprietary information provided by a DIB participant.

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:

(1) The total number of DIB participants. 250 annually.

(2) The annual number of responses provided to the Government (cyber incidents collected and reported--event-based reporting) by DIB participants. The total annual projected

number of responses (incidents reported), on average by each DIB participant (respondent) is projected to be five (5).

(3) The estimated amount of time required to report a cyber incident (for each participant to collect and report such information) to the Government is projected to be seven (7) man hours.

(4) These projections are based on current available data and best estimates. Additional data will become available through program implementation to validate future burden projections. The chart below reflects the estimated respondent burden:

Total Annual Hours

Year	Total Number of Respondents	Cyber Incidents/ Respondent	Labor Hrs/Response	Total Annual Hours
1	250	5	7	8,750

b. Labor Cost of Respondent Burden

Total Annual Cost Burden

Year	Total Number of Responses	Hours/ Response	Labor Cost/Hr	Total Cost
1	1,250	7	$39.06*	$341,775

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

The table above outlines the annualized cost to respondents imposed by the collection of cyber incident reporting. The total annual cost per DIB participant is $1,367 a year assuming 5 responses per DIB participant at 7 hours per response at $39.06 an hour.

13 Respondent Costs Other Than Burden Hour Costs.

a. DIB participants reporting cyber incidents must have or obtain DoD-approved medium assurance certificates. Generally, DIB participants will purchase medium assurance certificates from an approved commercial vendor. This is a start-up and recurring cost, however, certificates can be purchased for 1, 2 or 3 years, as needed. Each respondent is estimated to have seven certificates. The chart below depicts incident reporting start up costs for respondents. Figures assume an average of 7 certificates per DIB participants.

Year	Number of Respondents	Number of Certificates	Cost/Certificate	Annual Start Up Costs
1	250	7	$175	$306, 250

It will cost a company approximately $175 for each certificate. The start-up costs for one respondent with seven certificates is approximately $1,225. If a company provides more than seven points of contact, it will cost an additional $175 per person per certificate.

b. Certificates must be renewed annually, unless purchased for a 2 or 3-year period. The chart below represents costs to annually obtain/renew certificates as the DIB CS/IA Program.

The chart below reflects respondents' annual costs for obtaining/renewing certificates. It assumes that each respondent maintains an average of 7 certificates.

O&M Costs to Respondent

14. Cost to the Federal Government

Year	Number of Respondents	No. Certificates / Respondents	Cost/Certificate	Annual Start Up Costs
1	250	7	$175	$306, 250

The chart below reflects Government estimates that it will take six (6) hours to review and process the information in each report. The estimated times are as follows: 1 hour for logging and comparing to previous reporting, 3 hours for data querying, cross comparison and trend analysis, 1 hour for report writing, 1 hour for report review = 6 hrs total.

(1) For 250 Respondents, each having five incidents, requiring six hours of processing time by the Government, equates to an annual cost of $317,625. This figure does not include follow-up detailed analyses, cyber forensics, and support to cyber intrusion damage assessment.

Annual Cost to Government

Year	Number of Respondents	Number of Cyber Incidents	Labor Hrs/ Response	Labor Cost/Hr	Total Cost
1	250	1,250	6	$42.35	$317,625

* Mean hourly wage according to Base General Schedule Pay Scale, GS-14, Step 1.

15. Reasons for Change in Burden

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

16. Publication of Results

The Government expects that its components and other agencies will extract information from the information record to analyze patterns, capabilities, targets, operational methods, etc., for security and counterintelligence purposes. 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.