SUPPORTING STATEMENT – PART A

DoD's Defense Industrial Base (DIB) Cybersecurity (CS) Activities Cyber Incident Reporting – OMB Control Number 0704-0489

A. JUSTIFICATION

1. Need for the Information Collection

List all authorities. DoD is working to establish a focal point for receiving cyber incident reports from defense contractors by using a single online format for both mandatory reporting requirements and voluntary requirements. Mandatory reporting requirements are addressed in a separate information collection under Office of Management and Budget (OMB) Control Number 0704-0479 entitled "Defense Federal Acquisition Regulation Supplement (DFARS) Business Systems-Definition and Administration; DFARS 234, Earned Value Management Systems" authorizing the collection of mandatory cyber incident reporting in accordance with 10 U.S.C. 393: "Reporting on Penetrations of Networks and Information Systems of Certain Contractors," 10 U.S.C. 391: "Reporting on Cyber Incidents with Respect to Networks and Information Systems of Operationally Critical Contractors and Certain Other Contractors, and 50 U.S.C. 3330: "Reports to the Intelligence Community on Penetrations of Networks and Information Systems of Certain Contractors.

This information collection (OMB Control Number 0704-0489) supports the voluntary sharing of cyber incident information from DoD contractors in accordance with 32 Code of Federal Regulations (CFR) part 236, "Department of Defense (DoD)-Defense Industrial Base (DIB) Cybersecurity (CS) Activities," which authorizes the DIB CS program. Sharing cyber incident information is critical to DoD's understanding of cyber threats against DoD information, programs and warfighting capabilities systems. This information helps DoD to inform and mitigate adversary actions that may affect DoD information resident on or transiting unclassified defense contractor networks. 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.

The information collection requests data from the reporting companies to enable DoD to better understand the technical details of or related to a cyber incident, including its potential adverse effect on the company's unclassified information system and the effect, if any, on DoD information residing on or transiting the company's information system; or a company's ability to provide operationally critical support to DoD. The collection includes a request for a company point of contact if DoD has questions regarding the shared information.

2. Use of the Information

When a defense contractor discovers a cyber incident or information related to malicious cyber activity that affects a covered contractor information system or the covered defense information residing therein or that affects the contractor's ability to provide operationally critical support, the contractor shall conduct a review for evidence of compromise of covered defense information. This review shall also include analyzing covered contractor information systems(s) that were part of the cyber incident, as well as other information systems on the contractor's network(s) that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the contractor's ability to provide operationally critical support. The information collection is based on the DoD contractor's internal assessment and determination that cyber incident information should be shared with DoD.

Defense contractors are encouraged to share information including cyber threat indicators that they believe may be of value in alerting the Government and others, as appropriate, to adversary activity so that we can develop mitigation strategies and proactively counter threat actor activity. Cyber incidents that are not compromises of covered defense information or do not adversely affect the contractor's ability to perform operationally critical support, may be of interest to the DIB and DoD for situational awareness purposes.

Once the defense contractor determines that a cyber incident report is needed, they submit a cyber incident report using the Incident Collection Format (ICF) that can be accessed via the web portal (http://dibnet.dod.mil). DoD is working to establish this portal as the single reporting site for cyber incident information, whether mandatory or voluntary. A defense contractor selects the "Report a Cyber Incident" icon. Since access to the ICF requires a valid DoD-approved medium assurance certificate, the defense contractor will be prompted for their DoD-approved medium assurance certificate. The contractor is then directed to a Privacy Act Statement web page that clearly states all cyber incident reports are stored in accordance with the Defense Industrial Base (DIB) Cybersecurity Activities System of Record Notice (SORN). Contractors are then allowed to access the ICF and input data. Once a defense contractor completes the ICF, they are given a preview of the ICF to ensure that all the information they are providing is correct. After verifying the information is correct, the defense

contractor will then click the "submit" button. A reporting submission ID number is provided when the report is submitted. DoD uses this number to track the report and actions related to the report.

The reporting is analyzed by cyber threat experts at the DoD Cyber Crime Center (DC3) and they, in turn, develop written products that include analysis of the threat, mitigations, and indicators of adversary activity. These anonymized products are shared with authorized DoD personnel, other Federal agencies and designated points of contact in defense companies participating in the DIB Cybersecurity program. The products developed by DC3 do not contain company attribution, proprietary or personal information, but are vital to improving network security within the Government and the defense industrial base..

3. Use of Information Technology

100% of cyber incident reports submitted by DoD contractors is collected electronically.

4. Non-duplication

The information provided by respondents includes timely and detailed reporting on cyber incidents that affect DoD programs and missions, that is not otherwise available or 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

DoD contractors only report when they have determined that a cyber incident has affected a covered contractor information system or the covered defense information residing therein or that affects the contractor's ability to provide operationally critical support. Defense contractors are also encouraged to report information to promote sharing of cyber threat indicators that they believe may be of value in alerting the Government to adversary activity to promote developing mitigation strategies and proactively countering threat actor activity. The omission of this cyber incident reporting would greatly reduce the Government's and DoD contractor's knowledge of adversary activity, as well as their ability to enhance the cybersecurity and safeguarding of critical

information systems. The reporting standards are in accordance with statutory requirements mandating defense contractors to report cyber incidents.

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

- Part A: PUBLIC NOTICE

As required by 5 CFR 1320.8(d), the notice of information collection was published on 28 April 2016 in the Federal Register at 81 FR 25390 soliciting comments. No public comments were received.

A 30-Day Federal Register Notice for this collection published on 22 September 2016 in the Federal Register at 81 FR 65347.

- Part B: CONSULTATION

DoD is working to establish a single focal point for receiving all cyber incident reporting affecting DoD contractor unclassified networks. DoD contractors submit cyber incident reports using the http://dibnet.dod.mil web portal. DoD is working internally to enable component to leverage this portal to satisfy all contract cyber incident reporting requirements. DoD has also provided status updates to Congressional staffs on implementing the information collection mandated under U.S.C. Title 10 391 and 393.

9. Gifts or Payment

The Government will provide no payment or gifts to respondents.

10. Confidentiality

The Privacy Act Statement (PAS) for this information collection is posted on the web portal (http://dibnet.dod.mil). When a DoD contractor accesses the web portal, and clicks on the "Report a Cyber Incident" icon they will see the screen containing the PAS prior to accessing the ICF.

Due to cost and time restrictions for updating the web portal, the PAS, Agency Disclosure Notice, OMB Control Number and Expiration data are not currently included on the attached instrument collection screenshots. We are in the process of updating the web portal and have included an additional word

document with our package submission to OMB that illustrates what will be posted once it is completed.

The related SORN identifier number for this collection is DCIO 01, entitled "Defense Industrial Base (DIB) Cybersecurity (CS) Activities Records." The SORN is available and posted at: http://www.gpo.gov/fdsys/pkg/FR-2015-05-21/pdf/2015-12324.pdf.

The Privacy Impact Assessment for the Defense Industrial Base (DIB) Cybersecurity Activities has been completed, and is titled "Defense Industrial Base (DIB) Cybersecurity Activities Updated 2015." It can be found at http://dodcio.defense.gov/Portals/0/Documents/DIB_2015.pdf

Since the publication of the SORN, the Records retention and disposition schedule was approved by the National Archives and Records Administration. The records retention and disposition schedule can be found at https://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-defense/office-of-the-secretary-of-defense/rg-0330/daa-0330-2015-0005_sf115.pdf.

The Records Schedule Numbers included are DAA-0330-2015-0005-0001, "Defense Industrial Base (DIB) Cyber Security/Information Assurance System Database," which directs that DIB participant master files be destroyed 3 years after the participating company withdraws from the program, closes or goes out of business; DAA-0330-2015-0005-0002, "Cybersecurity Assessment," which states files be destroyed 10 years after cut off; and DAA-0330-2015-0005-0003, "Cyber Incident Response and Analysis," which also states the files be destroyed 10 years after cut off.

11. Sensitive Questions

Sensitive private information is not collected. A Privacy Impact Assessment addresses the processes in place to protect information provided by DoD contractors reporting cyber incident.

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	Hours/ Response Time (Amount of time needed to complete the collection instrument)	Respondent Burden Hours (Total Annual Responses multiplied by Response Time) Please compute these into hours)
Incident Collection Format	8,500	5	42,500	2 hrs	85,000 hrs
Total	8,500	5	42,500	2 hrs	85,000 hrs

b. Labor Cost of Respondent Burden

Labor Cost of Respondent Burden					
	Number of Responses	Response Time per Response	Respondent Hourly Wage	Labor Burden per Response (Response Time multiplied by Respondent Hourly Wage)	Total Labor Burden (Number of Responses multiplied by Response Time multiplied by Respondent Hourly Wage)
Incident Collection Format	42,500	2 hrs	$43.36*	$86.72	$3,685,600.00
Total	42,500	2 hrs	$43.36	$86.72	$3,685,600.00

***** 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

DoD-approved medium assurance is required in order to access the ICF via the web portal (http://dibnet.dod.mil). The total annualized costs to all respondents other than the labor burden costs addressed in item 12, is $1,487,500.00 (which is the number of respondents multiplied by cost of DoD-approved medium assurance certificate). This cost is an estimate based on the need for DoD contractors submitting a cyber incident report to have or obtain a DoD-approved medium assurance certificate. The total cost for a DoD-approved medium assurance certificate is approximately $175.00. The company 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. This information collection is not CAC-enabled. It is not cost effective, nor practical for DoD to authorize CACs for all DoD contractors affected by this information collection. The DoD-approved medium assurance certificate utilized to submit the ICF provides the necessary security standard for DoD contractors to report cyber incidents.

14. Cost to the Federal Government

Labor Cost to the Federal Government		
	Incident Collection Format (ICF)	Total
Number of Responses	42,500	42,500
Processing Time Per Response (in hours)	2 hrs	2 hrs
Hourly Wage of Worker(s) Processing Responses	$41.81*	$41.81
Cost to Process Each Response (Processing Time Per Response multiplied by Hourly Wage of Worker(s) Processing Responses)	$83.62	$83.62
Total Cost to Process Responses (Cost to Process	$3,553,850.00	$3,553,850.00

Each Response multiplied by Number of Responses)		

***** Mean hourly wage according to Base General Schedule Pay Scale, GS-14, Step 1. 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
$2,648,000	$0	$0	$1,114,000	$0	$1,338,000*****	$5,100,000

***** "Other" costs include expenses required to lease workspaces, furnish the workspaces with utilities (power, lighting, communications), and perform regular periodic maintenance (repair and/or replace) on workspaces, furnishings, or equipment.

Total Cost to the Federal Government		
Operational and Maintenance Costs	Labor Cost to the Federal Government	Total Cost (O&M Costs + Labor Cost)
$5,100,000.00	$3,553,850.00	$8,653,850.00

15. Reasons for Change in Burden

This information collection is an extension of existing collection requirements. This collection (0704-0489) impacts an estimated 8,500 DoD contractors who are voluntarily reporting cyber incident information on average 5 responses per year at 2 hours per response. A change in burden estimates has occurred from the previous 60-Day collection and the previous OMB approved collection. This change is based on lessons learned for contractor cyber incident reporting, and reflects that statutory requirements mandating cyber incident reporting are covered under OMB control number 0704-0479, "Defense Federal Acquisition Regulation Supplement (DFARS) Business Systems-Definition and Administration; DFARS 234, Earned Value Management Systems."

16. Publication of Results

The results are not published; however, the analysis of the reported information is used to develop written products that include analysis of the threat, mitigations, and indicators of adversary activity. These products are shared with authorized DoD personnel, other Federal agencies and designated points of contact in defense companies participating in the DIB Cybersecurity program. The products developed do not contain company attribution, proprietary or personal information, but are vital to improving network security within the Government and the defense industrial base. These are ongoing activities.

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 to certification for paperwork reduction submissions.