SUPPORTING STATEMENT - PART A

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

1. Need for the Information Collection

DoD designated the DoD Cyber Crime Center (DC3) as the single focal point for receiving all cyber incident reporting affecting the unclassified networks of DoD contractors from industry and other government agencies. DoD collects cyber incident reports using the Defense Industrial Base Network (DIBNet) portal (https://dibnet.dod.mil). 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 System” 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 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. 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 conducts a review for evidence of compromise of covered defense information. This review also includes 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 (https://dibnet.dod.mil).

DoD established this portal as the single reporting site for cyber incident information, whether mandatory or voluntary. A defense contractor selects the "Report" icon. The defense contractor will then be prompted for their DoD-approved medium assurance certificate to gain access to the ICF. The contractor is then directed to a Privacy Act Statement (PAS) 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 report is analyzed by cyber threat experts at 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 CS 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 DIB.

3. Use of Information Technology

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

4. Non-duplication

The information obtained through this collection is unique and is not already available for use or adaptation from another cleared source.

5. Burden on Small Businesses

This information collection does not impose a significant economic impact on a substantial number of small businesses or entities.

6. Less Frequent Collection

DoD contractors only report when they have determined that a cyber-incident has affected a covered defense 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 develop mitigation strategies and proactively counter 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

This collection of information does not require collection to be conducted in a manner inconsistent with the guidelines delineated in 5 CFR 1320.5(d)(2).

8. Consultation and Public Comments

Part A: PUBLIC NOTICE

A 60-Day Federal Register Notice (FRN) for the collection published on Monday, July 8, 2019. The 60-Day FRN citation is 84 FRN 32429.

No comments were received during the 60-Day Comment Period.

A 30-Day Federal Register Notice for the collection published on Monday, September 30, 2019. The 30-Day FRN citation is 84 FRN 51527.

Part B: CONSULTATION

No additional consultation apart from soliciting public comments through the Federal Register was conducted for this submission.

9. Gifts or Payment

No payments or gifts are being offered to respondents as an incentive to participate in the collection.

10. Confidentiality

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

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: https://www.govinfo.gov/content/pkg/FR-2015-05-21/pdf/2015-12324.pdf

The Privacy Impact Assessment for the Defense Industrial Base (DIB) Cybersecurity Activities has been completed, entitled "Defense Industrial Base (DIB) Cybersecurity Activities Updated 2015" and is posted 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. (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).

11. Sensitive Questions

No questions considered sensitive are being asked in this collection.

12. Respondent Burden and its Labor Costs

Part A: ESTIMATION OF RESPONDENT BURDEN

1) Collection Instrument
   DIBNet
   a) Number of Respondents: 8,500

b) Number of Responses Per Respondent: 5
c) Number of Total Annual Responses: 42,500
d) Response Time: 2 hours
e) Respondent Burden Hours: 85,000 hours

2) Total Submission Burden (Summation or average based on collection)
   a) Total Number of Respondents: 8,500
   b) Total Number of Annual Responses: 42,500
   c) Total Respondent Burden Hours: 85,000 hours

Part B: LABOR COST OF RESPONDENT BURDEN

1) Collection Instrument
   DIBNet
   a) Number of Total Annual Responses: 42,500
   b) Response Time: 2 Hours
   c) Respondent Hourly Wage: $45.01
   d) Labor Burden per Response: $90.02
   e) Total Labor Burden: $3,825,850

2) Overall Labor Burden
   a) Total Number of Annual Responses: 42,500
   b) Total Labor Burden: $3,825,850

The Respondent hourly wage was determined by using the [Department of Labor Wage Website] ([http://www.dol.gov/dol/topic/wages/index.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 (https://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 (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 DoD-approved 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

Part A: LABOR COST TO THE FEDERAL GOVERNMENT

1) Collection Instrument(s)
   DIBNet
   a) Number of Total Annual Responses: 42,500
   b) Processing Time per Response: 2 hours
   c) Hourly Wage of Worker(s) Processing Responses: $43.42
   d) Cost to Process Each Response: $86.84
   e) Total Cost to Process Responses: $3,690,700

2) Overall Labor Burden to the Federal Government
   a) Total Number of Annual Responses: 42,500
   b) Total Labor Burden *(P: add all "e's" in this section):* $3,690,700

Part B: OPERATIONAL AND MAINTENANCE COSTS

1) Cost Categories
   a) Equipment: $2,648,000
   b) Printing: $0
   c) Postage: $0
   d) Software Purchases: $1,114,000
   e) Licensing Costs: $0
   f) Other: $1,338,000

2) Total Operational and Maintenance Cost: $5,100,000

Part C: TOTAL COST TO THE FEDERAL GOVERNMENT

1) Total Labor Cost to the Federal Government: $3,690,700

2) Total Operational and Maintenance Costs: $5,100,000

3) Total Cost to the Federal Government: $8,790,700

15. <u>Reasons for Change in Burden</u>

There has been no change in burden since the last approval.

16. <u>Publication of Results</u>

The results of this information collection will not be published.

17. <u>Non-Display of OMB Expiration Date</u>

We are not seeking approval to omit the display of the expiration date of the OMB approval on the collection instrument.

18. Exceptions to "Certification for Paperwork Reduction Submissions"

We are not requesting any exemptions to the provisions stated in 5 CFR 1320.9.