SUPPORTING STATEMENT - PART A

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

Summary of Changes from Previously Approved Collection

- Actual figures from calendar years 2021, 2022, and 2023 were used to calculate annual cost averages.
- Current BLS and OPM wage rates were applied.
- An alternate authentication method (Procurement Integrated Enterprise Environment "PIEE") is noted.

1. Need for the Information Collection

DoD designated the DoD Cyber Crime Center (DC3) as the single 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 0704-0478 entitled "Safeguarding Covered Defense Information, Cyber Incident Reporting, and Cloud Computing" 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 threat 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 risk management agency for the DIB sector (see National Security Memorandum (NSM–22), "Critical Infrastructure Security and Resilience."[1]

The information collection requests data from the companies participating in the DIB CS Program to enable DoD and the DIB to better understand the technical details of a cyber threat. Eligible DoD contractors participate in the voluntary DIB CS Program to share cyber threat information and cybersecurity best practices with DIB CS Program participants. The DIB CS Program enhances and supplements DIB CS Program participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems.

2. Use of the Information

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. The information collection is based on the DoD contractor's internal assessment and determination that cyber information should be shared with DoD. Once the defense contractor determines that a report will be valuable to the community, 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 a Cyber Incident" button. The defense contractor will then be prompted for their DoD-approved medium assurance certificate to gain access to the ICF. Another means of authentication is through the Defense Logistics Agency (DLA) Procurement Integrated Enterprise Environment (PIEE) dashboard, which is automatically available to all users with a "Vendor" role.[2] 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 content to ensure that all the information they are providing is correct. After verifying the information is correct, the defense contractor will then click the "Certify" and then "Submit" button. When a user submits a report, the system generates a reporting submission ID number, and the user may download a copy of their report. DoD and DC3 use 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 authorized points of contact in defense companies participating in the DIB CS Program. The

[1] NSM 22: https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/

[2] PIEE Role Matrix: https://pieetraining.eb.mil/wbt/xhtml/wbt/portal/overview/PIEERoleList.xhtml

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

As a voluntary activity, this information collection does not impose a significant economic impact on a substantial number of small businesses or entities.

6. Less Frequent Collection

Defense contractors are 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.

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 Friday, August 2, 2024. The 60-Day FRN citation is 89 FR 63179.

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

A 30-Day Federal Register Notice for the collection published on Friday, November 22, 2024. The 30-Day FRN citation is 89 FR 92667.

No comments were received during the 30-Day Comment Period.

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 Privacy Act Statement 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 Privacy Act Statement 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://dpcld.defense.gov/Portals/49/Documents/Privacy/SORNs/OSDJS/DCIO-01.pdf

The Privacy Impact Assessment for the Defense Industrial Base (DIB) Cybersecurity Activities has been completed, entitled "Defense Industrial Base (DIB) Cybersecurity Activities Updated 2024" and is posted at https://dodcio.defense.gov/Portals/0/Documents/DIB_PIA.pdf

The Records Schedule Number is: DAA-0330-2015-0005, and 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

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 (https://dibnet.dod.mil)
   a) Number of Respondents: 111
   b) Number of Responses Per Respondent: 5
   c) Number of Total Annual Responses: 555
   d) Response Time: 2 hours
   e) Respondent Burden Hours: 1,100 hours

2) Total Submission Burden (Summation or average based on collection)
   a) Total Number of Respondents: 111

b) Total Number of Annual Responses: 555
c) Total Respondent Burden Hours: 1,100 hours

Part B: LABOR COST OF RESPONDENT BURDEN

1) Collection Instrument
   DIBNet (https://dibnet.dod.mil)
   a) Number of Total Annual Responses: 555
   b) Response Time: 2 Hours
   c) Respondent Hourly Wage: $119.94
   d) Labor Burden per Response: $239.88
   e) Total Labor Burden: $133,133.40

2) Overall Labor Burden
   a) Total Number of Annual Responses: 555
   f) Total Labor Burden: $113,113,40

The Respondent hourly wage was determined by using the mean wage estimate from the Bureau of Labor Statistics for an Information Security Analysts, Occupational Employment and Wages.[3] This hourly wage is adjusted upward by 100% to account for overhead and benefits, which implies a value of $119.94 per hour.

13. Respondent Costs Other Than Burden Hour Costs

A DoD-approved medium assurance certificate or a PIEE account with "Vendor" role is required to access the Incident Collection Format (ICF). Although the scope of the voluntary DIB CS Program has expanded from roughly 8,500 eligible contractors to 80,000,[4] all covered defense contractors participating in the DIB CS Program will have DoD-approved medium assurance certificates as part of their compliance with the requirements in DFARS Clause 252.204-7012.

The total annualized costs to all respondents, other than the labor burden costs addressed in item 12, ranges between $0 (for those with PIEE access) and $19,425 (number of respondents multiplied by the cost of a DoD-approved medium assurance certificate). The cost of access to DoD contractors with a PIEE account will be $0, but the cost of a DoD-approved medium assurance certificate is approximately $175 per year. The medium assurance certificate is a start-up and recurring cost, and certificates can be purchased for one, two or three years, as needed.

14. Cost to the Federal Government

Part A: LABOR COST TO THE FEDERAL GOVERNMENT

1) Collection Instrument(s)

[3] BLS Information Security Analyst: https://www.bls.gov/oes/current/oes151212.htm
[4] 32 CFR Part 236: https://www.federalregister.gov/documents/2024/03/12/2024-04752/department-of-defense-dod-defense-industrial-base-dib-cybersecurity-cs-activities

DIBNet

a) Number of Total Annual Responses: 555
b) Processing Time per Response: 2 hours
c) Hourly Wage of Worker(s) Processing Responses: $55.76
d) Cost to Process Each Response: $111.52
e) Total Cost to Process Responses: $61,893,60

2) Overall Labor Burden to the Federal Government
   a) Total Number of Annual Responses: 555
   b) Total Labor Burden: $61,893,60

The hourly rate for Federal Government personnel was determined by using the OPM Salary Table 2024-GS - Base General Schedule Pay Scale, GS-9, Step 5[5] and is adjusted upward by 100% to adjust for overhead and benefits.

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: $61,893,60

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

3) Total Cost to the Federal Government: $5,161,893.60

15. Reasons for Change in Burden

Actual submission figures from CY 2021, 2022, and 2023 were used to recalculate annual averages and Bureau of Labor Statistics salary figures were also updated with most recent data.

16. Publication of Results

The results of this information collection will not be published.

[5] 2024-GS OPM Salary Table: https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/salary-tables/24Tables/html/GS_h.aspx

17. Non-Display of OMB Expiration Date

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.