Supporting Statement
Cyber Incident Reporting by DoD Contractors
(Refer to OMB Form 83-I INST)

A. Justification

1. Circumstances Requiring Collection of Information.

This updated information collection reinstates and changes the previously approved information collect requirements under 0704-0489 "Defense Industrial Base Cyber Security/Information Assurance (DIB CS/IA) Cyber Incident Reporting.

DoD is revising 32 CFR Part 236 to implement mandatory cyber incident reporting on unclassified networks or information systems by DoD contractors or those contractors designated as providing operationally critical support. 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 941 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 13, *Reports to Department of Defense on Penetrations of Networks and Information Systems of Certain Contractors,* requires all cleared defense contractors to report cyber incidents to DoD to include a description of the technique used, a summary of information potentially compromised and a sample of malicious software, if discovered and isolated by the contractor. Additionally, Section 1632 of the NDAA for FY15, *Reporting on Cyber Incidents with Respect to Networks and Information Systems of Operationally Critical Contractors,* requires contractors designated as operationally critical contractors by DoD to report cyber incidents to include an assessment of the effect of the cyber incident on the ability of the contractor to meet the DoD contractual requirements, the technique used, a summary of information compromised, and a sample of malicious software, if discovered and isolated by the contractor. Under these mandatory statutory reporting requirements, DoD contractors are required to report cyber incidents to DoD.

2. Purpose of the Information.

DoD is proposing a revision to 32 CFR Part 236 to mandate reporting of cyber incidents on unclassified networks or information systems by DoD contractors or those contractors designated as providing operationally critical support. Mandatory cyber incident reporting requirements apply to all forms of contracts or other agreements between DoD and DIB companies (e.g., procurement contracts, cooperative agreements, other transaction agreements). When the reports are submitted, the DoD Cyber Crime Center (DC3) will analyze the reported information for cyber threats and vulnerabilities in order to develop response measures as well as improve U.S. Government and DIB understanding of advanced cyber threat activity. DoD may work with a DIB company on a more detailed, digital forensics analysis or damage assessment, which may include sharing of additional electronic media/files or information regarding the incident or the affected systems, networks, or information to evaluate the impact of the incident on DoD information.

3. Use of Information Technology.

DoD contractors will provide their cyber incident information using the following options:

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

(2) Complete a document version of the questions and submit responses via encrypted email using DoD-approved medium assurance certificates. (Fax can be used as an alternative).

The use of technology (e.g., forms software and online access) will decrease the reporting burden on respondents. The online ICF standardizes data entry and allows respondents to make data entry selections by checking appropriate boxes. The ICF also provides help text and other features to streamline data entry.

4. **Efforts to Identify Duplication**.
This collection request applies to non-contract arrangements between DoD and DIB companies (e.g., cooperative agreements, other transaction agreements) and is therefore not duplicative of other requirements.

5. **Methods to Minimize Burden to Small Business**.
The burden applied to small businesses to evaluate the effect of the cyber incident on DoD information and/or its mission is the minimum consistent with applicable laws, Executive orders, regulations, and prudent business practices.

6. **Consequences to DoD**.
The consequence of not collecting this data is that DoD is not able to protect sensitive information from its adversaries. Furthermore, DoD would not know the content of the data exfiltrated, the impact of the data loss to its mission, or how to develop appropriate countermeasures. DoD specialists who are most knowledgeable of the requirements and the need for the information reviewed the information collection frequency. This reporting requirement is needed to assess the impact of loss and to improve protection by better understanding the methods of loss.

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

8. **Publication for Comments**.
This information collection will be published in the Federal Register soliciting public comments.

9. **Payments or Gifts to Respondents**.
The Government will provide no payment or gifts to respondents.

10. **Assurance of Confidentiality to Respondents**.
The protection against disclosure of information containing personal or organizational identifiers is found in the publically releasable version of the Privacy Impact Assessment (PIA) for the DIB CS Activities.

The Privacy Act Statement of Records Notice (SORN) system identifier, DCIO 01, Defense Industrial Base (DIB) Cybersecurity Records, is attached.

11. **Justification for Sensitive Questions**.
A PIA addresses the processes in place to protect information provided by a DoD contractor, as well as the event of an inadvertent disclosure of PII by DoD contractors under mandatory incident reporting. 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 DoD contractor.

12. **Estimates of Information Collection Burden**.
The revised 32 CFR Part 236 rule will require additional reporting of cyber incidents by DoD contractors on unclassified networks or information systems for by DoD contractors.

DoD estimates that there are currently 10,000 cleared defense contractors and that all 10,000 may be required to report cyber incidents as a result of these changes to 32 CFR.

The total estimated burden to the public is 250,000 hours ($10,350,000).

A.	Number of respondents	10,000
B.	Responses per respondents	5
C.	Total annual responses	50,000
D.	Hours per response	5
D.	Total public burden hours	250,000
F.	Cost per hour	$41.40[1]
G.	Total annual estimate of public burden	$10,350,000

13. **Annual Cost Burden to Respondents**.
DoD does not estimate any burden hours apart from the hours estimated in items 12 and 14.

14. **Annual Cost Burden to Federal Government**.
The time estimates are based on the length it will take to log and compare to previous reporting, data querying, cross comparison and trend analysis, report writing, and report review. We estimate the time associated with this task is 6 hours per response.

A.	Number of Respondents	10,000
B.	Number of Cyber Incidents	5
C.	Hours per response	6
D.	Cost per hour	$41.40
E.	Total Cost	$12,240,000

15. **Program Changes or Adjustments**.
This information collection updates existing collection approvals by increasing the number of DoD contractors that may report cyber incidents to 10,000.

[1] Mean hourly wage to Base General Schedule Pay Scale 2015, GS-14, Step 1

16. **Publication**.
The use and protection of the information will conform to the conditions prescribed in the revised 32 CFR Part 236 for the protection of attribution and proprietary information. Results of this information will not be tabulated or published.

17. **Display of Expiration Date**.
DoD is not requesting approval to omit display of the expiration date of OMB approval on the instrument of collection.

18. **Exception to Certification Statement**
DoD is not requesting exception to satisfy the statutory requirements.

19. Collections of Information Employing Statistical Methods:
The information collection under the program does not employ statistical methods.