Supporting Statement

Safeguarding Unclassified Controlled Technical Information

A. Justification

1. Circumstances Requiring Collection of Information.
This is a request for establishment of a new information collection requirement to implement DoD's safeguarding of unclassified controlled technical information within industry. "Technical Information," means technical data or computer software of any kind that can be used, or adapted for use, in the design, production, manufacture, assembly, repair, overhaul, processing, engineering, development, operation, maintenance, adapting, testing, or reconstruction of goods or materiel; or any technology that advances the state of the art, or establishes a new art, in an area of significant military applicability in the United States. The information may be in tangible form, such as a blueprint, photograph, plan, instruction, or an operating manual, or may be intangible, such as a technical service or oral, auditory, or visual descriptions. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software. Controlled technical information must be marked in accordance with DoD instruction 5230.24 as provided by DoD to a non-DoD entity, or that is collected, developed, received, transmitted, used, or stored by a non-DoD entity in support of an official DoD activity (DTM-08-027-ASD(NII)).

2. Purpose of the Information.
DoD is proposing amendments to the Defense Federal Acquisition Regulation Supplement (DFARS) to implement safeguarding and cyber intrusion reporting of unclassified controlled technical information within industry. This case would make the following changes to the DFARS:

- Add a new DFARS Subpart 204.74, Safeguarding Unclassified Controlled Technical Information; and

Add new DFARS 252.204-7012 clause for Safeguarding of Unclassified Controlled Technical Information.
As stated at DFARS 252.204-7012(d), the contractor shall report to DoD via http://dibnet.dod.mil/ within 72 hours of discovery of any cyber incident. The information provided in the reporting process will be used by network analyst in their efforts to safeguard DoD unclassified controlled technical information.

3. Use of Information Technology.
Improved information technology will be used to the maximum extent practicable. Contractors will report incidents to DoD via the internet.

4. Efforts to Identify Duplication.
As a matter of policy, DoD reviews the Federal Acquisition Regulation (FAR) and DFARS to determine if adequate language already exists. This information collection implements a unique provision and does not duplicate any other requirement.

5. Methods to Minimize Burden to Small Business.
The burden applied to small businesses 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 properly protecting information from its adversaries. Furthermore, DoD would not know the content of the data exfiltrated, the impact of the data loss to its mission, and 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.
There are no special circumstances that require the collection to be conducted in any manner listed in 5 CFR 1320.5(d)(2).

8. Publication for Comments.
This information collection is consistent with the guidelines in 5 CFR 1320.5(d). Public comments were solicited via the notice

published in Federal Register 76 FR 38089, June 29, 2011. Several comments were received stating that the information collection was either burdensome or that the incident reporting rate and burden hours were grossly underestimated.

Since the burden estimates were estimated for the proposed rule, much more data has become available, in particular from voluntary reporting by defense industrial base companies to the Defense Cyber Crime Center. Data from this voluntary program suggests 5 reports per company per year with a 3.5 hour burden per response. Accordingly, DoD is revising its cost estimate upward to 5 reports per company per year with a 3.5 hour burden per response.

9. Payments or Gifts to Respondents.
No payment or gift will be provided to respondents.

10. Assurance of Confidentiality to Respondents.
The information collected will be disclosed only to the extent consistent with prudent business practice, current regulations, and statutory requirements. No assurance of confidentiality is provided to respondents.

11. Justification for Sensitive Questions.
No sensitive questions are involved.

12. Estimates of Information Collection Burden.
The final rule will require an enhanced level of information assurance protection, and reporting of information loss or cyber-intrusions by DoD contractors that use unclassified controlled technical information requiring special handling. The requirement would also be passed down through the supply chain.

It is assumed that most information passed down the supply chain will not require special handling. DoD estimates that of the current 8,000 cleared defense contractors only 6,555 would be handling unclassified controlled technical information.

The total estimated burden to the public is 114,713 hours ($4,176,682).

A.	Total annual responses	32,775
B.	Hours per response	3.5

C.	Total public burden hours	114,713
D.	Cost per hour	$37[1]
E.	Total annual estimate of public burden	$4,244,381

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 receiving, reviewing, analyzing the information submitted by the contractor. We estimate that the time associated with this task is 3 hours per response.

A.	Number of respondents	6,555
B.	Responses per respondent	5
C.	Total Annual responses	32,775
D.	Hours per response	3
E.	Total hours	98,325
F.	Cost per hour	$37[2]
G.	Total amount	$3,638,025

15. Program Changes or Adjustments.
This is a new information collection requirement.

16. Publication.
Results of this information will not be tabulated or published.

17. Display of Expiration Date.
DoD does not seek approval to not display the expiration dates for OMB approval of the information collection.

18. Exception to Certification Statement.
There are no exceptions to the certification accompanying this Paperwork Reduction Act submission.

B. Collections of Information Employing Statistical Methods:
Statistical methods will not be employed.

---

[1] *Based on 2012 GS–11 step 5 of $27.31 plus an overhead of 36.25 percent, rounded to the nearest dollar ($37.20 rounded to $37 per hour).*

[2] *Based on 2012 GS–11 step 5 of $27.31 plus an overhead of 36.25 percent, rounded to the nearest dollar ($37.20 rounded to $37 per hour).*