SUPPORTING STATEMENT – PART A

OMB Control Number 0704-0478: Safeguarding Covered Defense Information, Cyber Incident Reporting, and Cloud Computing

Summary of Changes from Previously Approved Collection

The burden for this collection has changed from the previous collection, with a net decrease due to:

- A decrease in the number of estimated respondents under Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.239-7009, Representation of Use of Cloud Computing, from 34,684 to 16,108;
- An increase in the number of respondents estimated to report cyber incidents under DFARS clause 252.239-7010, Cloud Computing Services, from 10 to 32; and
- An increase in the number of respondents estimated to report cyber incidents under DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, from 200 to 580.

1. Need for the Information Collection

DoD revised the DFARS 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. Under the following mandatory statutory reporting requirements, DoD contractors are required to report cyber incidents to DoD:

a. *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.

b. *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.

2. Use of the Information

Offerors and contractors must report cyber incidents on unclassified networks or information systems, within cloud computing services, and when they affect contractors designated as providing operationally critical support, as required by statute.

a. DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, covers cyber incident reporting requirements for incidents that affect a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract.

b. DFARS provision 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls, requires an offeror that proposes to vary from any of the security controls of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 in effect at the time the solicitation is issued to submit to the contracting officer a written explanation of how the specified security control is not applicable or an alternative control or protective measure is used to achieve equivalent protection.

c. DFARS provision 252.239-7009, Representation of Use of Cloud Computing, requires contractors to report that they “anticipate” or “do not anticipate” utilizing cloud computing service in performance of the resultant contract. The representation will notify contracting officers of the applicability of the cloud computing requirements at DFARS clause 252.239-7010 of the contract.

d. DFARS clause 252.239-7010, Cloud Computing Services, requires reporting of cyber incidents that occur when DoD is purchasing cloud computing services.

These DFARS provisions and clauses facilitate mandatory cyber incident reporting requirements in accordance with statutory regulations. When reports are submitted, the DoD Cyber Crime Center will analyze the reported information for cyber threats and vulnerabilities in order to develop response measures as well as improve U.S. Government understanding of advanced cyber threat activity. In addition, the security requirements in NIST SP 800-171 are specifically tailored for use in protecting sensitive information residing in contractor information systems and generally reduce the burden placed on contractors by eliminating Federal-centric processes and requirements. The information provided will inform the Department in assessing the overall risk to DoD covered defense information on unclassified contractor systems and networks.

3. Use of Information Technology

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

i. Complete and submit data with DoD-approved medium assurance certificates via an online web form.

ii. Download, complete and submit the Incident Report, via encrypted email using DoD-approved medium assurance certificates. (Fax may be used as an alternative.)

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

c. The representation on use of cloud computing services may be submitted electronically, in accordance with solicitation specific instructions.

4. Non-duplication

As a matter of policy, DoD reviews the Federal Acquisition Regulation (FAR) and DFARS to determine if adequate language already exists. There are two other OMB Control Numbers associated with the cyber incident reporting program; however, this information collection reflects unique DFARS clauses/provisions and does not duplicate any other requirement. The two other OMB Control Numbers for the program are summarized as follows:

a. *0704-0489, DoD's Defense Industrial Base (DIB) Cyber Security (CS) Activities Cyber Incident Reporting*. This control number supports "voluntary" reporting of cyber incidents, while 0704-0478 supports reporting that is mandated under a DoD contract. Voluntary reporting could include grantees or members of industry who choose to voluntarily report incidents and does not address the burden for reporting required by a DoD contractual agreement. OMB 0704-0489 also covers the online collection medium, a Defense Industrial Base/Information Assurance Incident Collection format, which is a database used for both voluntary reporting and reporting that is contractually mandated. While this collection request (0704-0478) requires submission of information via the same Incident Report as voluntary collections under 0704-0489 "Defense Industrial Base Cyber Security/Information Assurance Cyber Incident Reporting," the reporting for each occurs in different circumstances and will not cause duplication.

b. *0704-0490, Defense Industrial Base Voluntary Cyber Security/Information Assurance Points of Contact (POC) Information*. This control number supports the application process in order to join the program. This collection is also supported by a Privacy Impact Assessment and a System of Records Notice (SORN) for the cyber incident reporting program.

5. Burden on 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. Less Frequent Collection

The consequence of not collecting this data is that DoD is not able to protect 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. 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

a. Public Notice

i. A 60-day notice for the collection was published in the *Federal Register* on June 21, 2022, at 87 FR 36831. One respondent provided comments as follows:

Comment: The renewal notice asked whether the proposed collection of information is necessary for the proper performance of the functions of DoD, including whether the information will have practical utility. The respondent stated that the information is absolutely necessary for the proper performance of the function of the DoD. The information does have practical utility to support DoD risk decisions about their supply chain.

Response: DoD acknowledges the comment.

Comment: The respondent commented on the accuracy of the estimate of the burden of the proposed information collection renewal. The call for inputs states that the average burden per response is 0.29 hours. It does not state how this number is calculated. When all the information has been gathered by the company, and its reporting has been determined to be required then the simple act of entering the information into the portal per incident may take on average around 30 minutes. In general, however, the totality of the effort required to be prepared to, capable of, and actually execute the information gathering processes required to support the reporting would raise the per report burden of response significantly. With over 80,000 companies subject to the regulation by the DoD's estimate and only 2,000 companies actually making reports, there seems to be a disconnect in reporting. Additionally, those companies on average are reporting more than once a month indicating a frequent report rate for companies that are reporting and a very large body of companies with a zero rate.

Response: The estimate of 0.29 hours represented a weighted average of the time required for a respondent to respond to the reporting requirements of the two clauses and two provisions covered by this information collection. The respondent is assuming that all of this

information collection is related to cyber incident reporting, but by far the largest response is not cyber incident-related but the DFARS 252.239-7009 Representation of Use of Cloud Computing. This is a simple representation (15 minutes/0.25 hours) that accounts for the vast majority (99%) of responses (34,684 of 34,974) and so dominates the overall response time, driving the average response time to 17 minutes/0.29 hours. The time estimated to submit a cyber-incident report is estimated at between 5 to 6 hours. DoD is revising its estimates for the overall information collection estimate based on the availability of more current information. The revised estimates reflect a reduction, by half, in the numbers of responses that indicate a positive representation that cloud computing is anticipated to be used under the proposed contract. The estimated time to submit a cyber-incident report remains at between 5 to 6 hours, however with this revision the overall weighted average for all reporting is now 0.46 hours or 28 minutes (16,760 total responses/7,695 total hours). See paragraphs 12 and 15 of this statement for additional details on the estimated burdens, associated data, and calculations.

Comment: The respondent commented on ways to enhance the quality, utility, and clarity of the information to be collected. Based on the normal rate of cybersecurity incidents in industry, reporting for a covered entity should occur frequently; clearly it is not. The respondent recommended additional public dialogue on the need for reporting in various forums, particularly business forums by senior leadership. Additionally, the respondent recommended further work with contracting officers and program managers through the Defense Acquisition University to not punish companies for reporting. The respondent cited fear of backlash as the number one reason companies do not report.

Response: DoD acknowledges the comment.

Comment: The respondent commented on ways to minimize the burden of the information collection. The respondent recommended using a simpler initial reporting form on the portal. The respondent also recommended configuring the current reporting mechanism as a typical commercial activity would to encourage information submission. The respondent noted that the ability to submit reports via email exists but could be enhanced and streamlined while continuing to meet information security requirements.

Response: The current web-based reporting mechanism is actually quite simple while including the all necessary elements needed by DoD to respond to the incident. It supports initial reporting and follow-on submission of new or updated information via the web-based reporting portal. While the ability to submit via alternate means is supported, the web-based reporting is the most efficient given the need by the contractor to identify data on the individual DoD contracts affected by the incident.

ii. A 30-day notice for the collection was published in the *Federal Register* on August 31, 2022, at 87 FR 54362.

9. Gifts or Payment

No payments or gifts are being offered to respondents as an incentive to participate in the collection, other than remuneration to contractors under their contracts.

10. Confidentiality

This information is disclosed only to the extent consistent with prudent business practices and current regulatory, statutory, and Freedom of Information Act requirements. No assurance of confidentiality is provided to respondents. A Privacy Act Statement is not required for this collection because DoD is not requesting individuals to furnish personal information for a system of records. A System of Record Notice (SORN) is not required for this collection because records are not retrievable by personally identifiable information (PII). A Privacy Impact Assessment (PIA) is not required for this collection because PII is not being collected electronically.

11. Sensitive Questions

No questions considered sensitive are being asked in this collection.

12. Respondent Burden and its Labor Costs

In the following estimates, hourly rates are based on the Locality Pay Area of Rest of U.S. General Schedule Pay Scale for 2022, GS-14, Step 5 of $60.56 plus 36.25% overhead, resulting in an hourly rate of $82.51, rounded to $83 per hour.

a. *252.204-7012, Safeguarding Unclassified Controlled Technical Information:*

i. Under paragraph (b)(2)(ii)(B) contractors may submit requests to vary from NIST SP 800-171 for certain covered contractor information systems. DoD estimates that approximately five requests to vary from NIST SP 800-171 are made each year; this estimate is increased to 10 to perpetuate this clearance since the Paperwork Reduction Act (PRA) applies when 10 or more members of the public are affected. DoD estimates that one hour is required to submit the variance request.

Estimation of Respondent Burden Hours and Labor Costs	
Number of respondents	10
Responses per respondent	1
Number of responses	10
Hours per response	1
Estimated hours (number of responses multiplied hours per response)	10
Cost per hour (hourly wage)	$83
Annual public burden (estimated hours multiplied by cost per hour)	$830

ii. Under paragraph (c)(1)(ii), contractors shall rapidly report cyber incidents to DoD. Approximately 580 cyber incident reports are submitted each year, and it can take from a few minutes to complete up to eight hours; therefore, an estimated five hours is used to calculate the burden hours. Further, under paragraph (g), contractors shall provide media, when requested, to enable the Government to perform damage assessment. In FY 2021, there were 48 media submissions. DoD estimates that approximately 48 contractors of the 580 contractors submitting cyber incident reports will be required each year to provide media for damage assessments, and, on average, it takes 10 hours to prepare and submit the media.

Estimation of Respondent Burden Hours and Labor Costs	
Number of respondents	580
Responses per respondent	1
Number of responses	580
Hours per response	5.83
Estimated hours (number of responses multiplied hours per response)	3,380
Cost per hour (hourly wage)	$83
Annual public burden (estimated hours multiplied by cost per hour)	$280,540

iii. The total estimated respondent burden hours and respondent labor cost under 252.204-7012 for contractors to: 1) submit requests to vary from NIST SP 800-171 for certain covered contractor information systems, under paragraph (b)(2)(ii)(B); 2) rapidly report cyber incidents to DoD, under paragraph (c)(1)(ii); and 3) provide media for damage assessments, under paragraph (g), are described in the tables below.

1. Estimation of Respondent Burden

The number of respondents includes the 48 respondents for media submissions as part of the 580 cyber incident respondents. The number of respondents includes the estimated 580 respondents for cyber incidents and 10 respondents for requests to vary from NIST SP 800-171.

Estimation of Respondent Burden Hours: 252.204-7012	
Number of respondents	590
Number of responses per respondent	1
Number of total annual responses	590
Hours per response	5.75
Annual respondent burden hours *(Total annual responses * hours per response)*	3,393

2. Labor Cost of Respondent Burden

The number of annual responses includes 48 media submissions as part of the 580 cyber incident response. The number of annual responses includes the estimated 580 responses for cyber incidents and 10 responses for requests to vary from NIST SP 800-171.

Labor Cost of Respondent Burden: 252.204-7012	
Number of total annual responses	590
Hours per response	5.75
Cost per hour (hourly wage)	$83
Labor burden per response *(Hours per response * hourly wage)*	$477
Annual Labor Burden *(Total annual responses * hours per response * hourly wage)*	$281,578

b. *252.204-7008, Compliance with Safeguarding Covered Defense Information Controls*

1. Estimation of Respondent Burden

DoD estimates that approximately five offerors will propose to vary from NIST SP 800-171 security requirements in accordance with paragraph (c)(2)(i) of the provision. Since the PRA applies to 10 or more members of the public, the estimate of five is increased to 10 to perpetuate the clearance for this provision to ensure coverage in the event of future increases in requests.

Estimation of Respondent Burden Hours: 252.204-7008	
Number of respondents	10
Number of responses per respondent	1
Number of total annual responses	10
Hours per response	1
Annual respondent burden hours *(Total annual responses * hours per response)*	10

2. Labor Cost of Respondent Burden

DoD estimates that approximately five offerors will propose to vary from NIST SP 800-171 security requirements in accordance with paragraph (c)(2)(i) of the provision. Since the PRA applies to 10 or more members of the public, the estimate of five is increased to 10 to perpetuate the clearance for this provision to ensure coverage in the event of future increases in requests.

Labor Cost of Respondent Burden: 252.204-7008	
Number of total annual responses	10
Hours per response	1

Cost per hour (hourly wage)	$83
Labor burden per response *(Hours per response * hourly wage)*	$83
Annual Labor Burden *(Total annual responses * hours per response * hourly wage)*	$830

c. *252.239-7009, Representation of Use of Cloud Computing*

1. Estimation of Respondent Burden

Offerors are required to represent their intentions to utilize cloud computing services in response to all solicitations for information technology services. According to the Federal Procurement Data System (FPDS) for FY 2019 through FY 2021, an average of 4,027 new contract awards per year were made to an average of 1,473 unique entities for information technology (IT) related services. It is estimated that there are approximately four offerors competing for each of the awards, which results in a total of approximately 16,108 responses. The same offeror may submit multiple responses to IT solicitations; and while we can identify the 1,473 unique contractors who received the awards, there is no specific data available to identify the unique number of offerors who submitted the estimated 16,108 solicitation responses. For the purposes of the estimate, DoD is assuming that the 1,473 unique awardees were the same entities that submitted offers on the 4,027 contract awards. Approximately 15 minutes is anticipated to be required to determine and submit the use of cloud computing representation.

Estimation of Respondent Burden Hours: 252.239-7009	
Number of respondents	1,473
Number of responses per respondent	10.9
Number of total annual responses	16,108
Hours per response	0.25
Annual respondent burden hours *(Total annual responses * hours per response)*	4,027

2. Labor Cost of Respondent Burden

Labor Cost of Respondent Burden: 252.239-7009	
Number of total annual responses	16,108
Hours per response	0.25
Cost per hour (hourly wage)	$83
Labor burden per response *(Hours per response * hourly wage)*	$20.75
Annual Labor Burden *(Total annual responses * hours per response *	$334,241

hourly wage)	

d. *252.239-7010, Cloud Computing Services:*

1. Estimation of Respondent Burden

There are three reporting requirements under this clause: paragraph (d) requires cyber incident reporting; paragraph (h) requires submission of information (media) related to a cyber event reported in paragraph (d); and paragraph (j) requires notifications of third-party access requests. The number of cyber incident reports is estimated to be 32 cyber incident reports by four respondents. It is estimated that the cyber incident reports will require four hours per response. Although there have been no media submissions or notifications of third-party access requests in 2019, 2020, and 2021, 10 respondents for each is estimated in order to continue the PRA clearance for media submissions and notifications of third-party access requests. It is estimated that the media submissions will take 10 hours per response and the notifications of third-party requests for access will take four hours per response.

Estimation of Respondent Burden Hours: 252.239-7010	
Number of respondents	24
Number of responses per respondent	2.17
Number of total annual responses	52
Hours per response	5.15
Annual respondent burden hours *(Total annual responses * hours per response)*	268

2. Labor Cost of Respondent Burden

Labor Cost of Respondent Burden: 252.239-7010	
Number of total annual responses	52
Hours per response	5.15
Cost per hour (hourly wage)	$83
Labor burden per response *(Hours per response * hourly wage)*	$427
Annual Labor Burden *(Total annual responses * hours per response * hourly wage)*	$22,227

e. *Total estimated burden for cyber reporting and cloud computing:* The following is the total of estimated burden and costs from paragraphs 12.a. through 12.d.

Estimation of Respondent Burden Hours and Labor Costs	
Number of respondents	2,097
Responses per respondent	7.99
Number of responses	16,760
Hours per response (approximately)	0.46
Estimated hours (number of responses multiplied hours per response)	7,695
Cost per hour (hourly wage)	$83
Annual public burden (estimated hours multiplied by cost per hour)	$638,685

13. Respondent Costs Other Than Burden Hour Costs

There are no annualized costs to respondents other than the labor burden costs addressed in Section 12 of this document to complete this collection.

14. Cost to the Federal Government

The following table illustrates the estimated Government burden from in-take, analysis, assessment, documentation development and completion of all required reviews for the information collections under DFARS 252.204-7012, 252.204-7008, 252.239-7009, and 252.239-7010:

Cost to the Federal Government					
Requirement	Responses	Hours/ Response	Total Hours	Cost/ Hour	Total Cost
252.204-7012(b)(2)(ii)(B)	10	1	10	$83	$830
252.204-7012(c)(1)(ii)	580	5	2,900	$83	$240,700
252.204-7012(g)	48	10	480	$83	$39,840
252.204-7008(c)(2)(i)	10	1	10	$83	$830
252.239-7009	16,108	0.08	1,289	$83	$106,957
252.239-7010(d)	32	1	32	$83	$2,656
252.239-7010(f/h)	10	10	100	$83	$8,300
252.239-7010(j)	10	4	40	$83	$3,320
Total			4,861	$83	$403,433

15. Reasons for Change in Burden

The burden has a net decrease since the previous approval due to a decrease in the number of estimated respondents under DFARS clause 252.239-7009, which was not offset by an increase in the number of respondents under DFARS clauses 252.239-7010 and 252.204-7012. In the previous approval, the number of estimated respondents under 252.239-7009 was 34,684 and it decreased to 16,108, based on FPDS data that showed a decrease in the number of IT services awards from FY 2019 through FY 2021. The number of IT services awards are multiplied by four to estimate the total number of respondents under 252.239-7010, so when the average number of awards decreased from 8,671 in the previous collection to 4,027, the total number of respondents decreased from 34,684 to 16,108.

In addition, in the previous approval, the number of respondents estimated to report cyber incidents under DFARS clause 252.204-7012 in 2019 was 200 respondents, which increased to 580 respondents in 2022. In addition, the number of respondents estimated to report cyber incidents under DFARS clause 252.239-7010 increased from 10 in 2019 to 32 in 2022. The estimates for this renewal use the actual number of reports submitted to DoD during FY 2021 via the web portal at http://dibnet.dod.mil as the baseline for the estimate. In addition, the hourly rate increased from $76 per hour in 2019 to $83 per hour in 2022 based on the Locality Pay Area of Rest of U.S. General Schedule Pay Scale for 2022. Despite these increases, the total burden decreased due to the decrease in the number of estimated respondents under 252.239-7010.

The total information collection public burden associated with DFARS clauses 252.204-7012, 252.204-7008, 252.239-7009, and 252.239-7010 has been changed as shown in the following table.

0704-0478			
Change in Burden	2019	2022	Difference
Number of respondents	2,017	2,097	80
Total annual responses	34,974	16,760	-18,214
Total hours	10,071	7,695	-2,376
Cost per hour	$76	$83	$7
Total annual cost to public	$765,396	$638,685	-$126,711

16. Publication of Results

The results of this information collection will not be published.

17. Non-Display of OMB Expiration Date

DoD is 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"

DoD is not requesting any exemptions to the provisions stated in 5 CFR 1320.9.