SUPPORTING STATEMENT

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

A. JUSTIFICATION

1. Need for the Information Collection

DoD revised the Defense Federal Acquisition Regulation Supplement (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

Collection of this information is consistent with 5 CFR 1320.5(d)(2). No special circumstances are required.

8. Consultation and Public Comments

a. This collection is consistent with the guidelines in 5 CFR 1320.6. Public comments were solicited in the *Federal Register* at 84 FR 23532 on May 22, 2019, as required by 5 CFR 1320.8(d). One respondent provided four comments on the reporting burden expressing concern that the current information collection and incident-reporting requirements are overly burdensome, particularly for commercial-item contractors. The comments are outside the scope of the notice published in the *Federal Register* for the proposed extension for an additional three years of an approved information collection requirement. The four comments are summarized below along with responses provided as follows:

Comment: To ensure proper safeguarding of contractors' attributional/proprietary information, the respondent recommends that the contractor submitting the information be (1) afforded an opportunity to review and propose redactions prior to release, (2) permitted to apply protective markings to information after its submission to the Government, and (3) allotted additional time to pursue any administrative or legal remedies in the event that the Government plans to disclose information that the contractor has otherwise proposed to be withheld.

Response: DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, authorizes DoD to release information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is not created by or for DoD. It further states that: (i) the Government will protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this clause that includes contractor attributional/proprietary information; and (ii) in making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released. A foundational element of the mandatory reporting requirement is the recognition that the information being shared between the parties may include extremely sensitive information that requires protection. Information regarding the Government's safeguarding of information received from the contractors that require protection can be referenced in the DoD Privacy Impact Assessment (PIA). The PIA provides detailed procedures for handling personally identifiable information (PII), attributional information about the strengths or vulnerabilities of specific covered contractor information systems, information providing a perceived or real competitive advantage on future procurement action, and contractor information marked as proprietary or commercial or financial information (see OMB Control Number 0704-0489, DoD's Defense Industrial Base (DIB) Cybersecurity (CS) Activities Cyber Incident Reporting). Additionally, 32 CFR part 236 implements mandatory information sharing requirements of 10 U.S.C. 391 and 393 by requiring DoD contractors to report key information regarding cyber incidents, and to provide access to equipment or information enabling DoD to conduct forensic analysis to determine if or how DoD information was impacted in a cyber incident. The rule's implementation of these requirements is tailored to minimize the sharing of unnecessary information (whether sensitive or not), including by carefully tailoring the information required in the initial incident reports (32 CFR 236.4(c)), by expressly limiting the scope of the

requirement to provide DoD with access to only such information that is "necessary to conduct a forensic analysis," and by affirmatively requiring the Government to safeguard any contractor attributional/proprietary information that has been shared (or derived from information that has been shared) against any unauthorized access or use. In the event that the contractor believes that there is information that meets the criteria for mandatory reporting, but the contractor desires not to share that information due to its sensitivity, then the contractor should immediately raise that issue to the DoD contracting officer for the contract(s) governing the activity in question.

Comment: The respondent commented that the "rapidly reporting" requirement at DFARS 252.204-7012(c)(1)(2) is extremely burdensome on contractors. The respondent recommends either extending the period to report or, otherwise, amending the clause to explain that the 72-hour reporting period begins to run once a contractor knows or should have known that covered defense information (CDI) was adversely impacted or it is "highly likely" that CDI was adversely impacted. The respondent also recommends that a medium assurance certificate need not be required for initial reporting, since this limits the person(s) within the entity who may report and may impede the ability to report within the requisite time period.

Response: The contractor is required to report known or potential cyber incidents within 72 hours of discovery. Timeliness in reporting cyber incidents is a key element in cybersecurity and provides the clearest understanding of the cyber threat targeting DoD information. The 72-hour period has proven to be an effective balance of the need for timely reporting while recognizing the challenges inherent in the initial phases of investigating a cyber incident. Contractors should report available information within the 72-hour period and provide updates if more information becomes available. The requirement to have medium assurance certificates is important to communicate securely with DoD and to securely access DoD's reporting website.

Comment: The respondent commented that there is often ambiguity as to what is considered CDI under specific contracts, which ought to be resolved by the Government, as agency personnel are best suited to identify the CDI being provided to a contractor and make appropriate notifications. The respondent recommended that DoD develop processes and procedures for engaging with contractors on the designation of information as CDI during the solicitation process or otherwise before the contract is finalized.

Response: Processes already exist for the contractor to engage with DoD personnel to request clarification regarding covered defense information, both during the solicitation phase and during contract performance.

Comment: The respondent commented that certain commands within the Department have created contract-specific requirements mandating that contractors apply the protections and reporting requirements of DFARS 252.204-7012 – including the reporting and record-keeping obligations – to categories of information much broader than CDI. The respondent recommends that commercial-item contractors and contractors that do not possess CDI, regardless of contract-specific cybersecurity requirements, be exempt from the reporting and recordkeeping requirements. The respondent further suggests that agencies be required to obtain approval from

a centralized office within the Department and to explain the basis for requiring protections in excess of what is required by DFARS 252.204-7012.

Response: Covered defense information is a term used to identify information that requires protection under DFARS clause 252.204-7012 that means unclassified controlled technical information or other information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies. When the acquisition of commercial items or services involves covered defense information, DFARS clause 252.204-7012 and any additional contract-specific cybersecurity requirements incorporated by the requiring activity will apply to both the solicitation and resulting contract. DFARS 252.204-7012 requires the contractor to provide adequate security on any unclassified information system that is owned, or operated by or for, the contractor and that processes, stores, or transmits covered defense information. Covered defense information, when provided to the contractor, by or on behalf of DoD in support of the performance of the contract, must be marked or otherwise identified in the contract, task order, or delivery order. If a contractor has reason to question whether the information requires protection under this clause, the contractor should consult with the cognizant contracting officer for clarification. DoD agencies follow the Department's policies for information protection contained in DoD Manual (DoDM) 5200.01 Vol 4, DoD Information Security Program: CUI, and in DoD Instruction (DoDI) 5230.24, Distribution Statements on Technical Documents. As these policies have been in place for several years, the Department does not require a centralized office to oversee their execution.

b. A notice of submission to OMB for clearance of this information collection was published in the *Federal Register* on July 30, 2019 at 84 FR 36905.

c. For the purpose of calculating respondent burden, DoD subject matter experts in the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) Damage Assessment Management Office (DAMO) and the Defense Industrial Base (DIB) Cyber Security Program, DoD Chief Information Office were contacted to obtain current data.

9. Gifts or Payment

The Government will provide no payment or gifts to respondents, other than remuneration of contractors in accordance with the terms of their contracts.

10. Confidentiality

This information is disclosed only to the extent consistent with statutory requirements, current regulations, and prudent business practices. The Privacy Act Statement of Records Notice (SORN) system identifier, DCIO 01, Defense Industrial Base (DIB) Cybersecurity Records, includes stipulations related to the release and disclosure of information collected. An update was published in the *Federal Register* on September 28, 2016 at 81 FR 66642 (see related OMB Control Number 0704-0490).

11. Sensitive Questions

No questions of a sensitive nature are involved. Only the minimum information to report a cyber incident is required.

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 2019, GS-14, Step 5 of $55.99 plus 36.25% overhead, resulting in an hourly rate of $76.29, rounded to $76 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 ten to perpetuate this clearance since the Paperwork Reduction Act (PRA) applies when ten 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)	$76
Annual public burden (estimated hours multiplied by cost per hour)	$760

ii. Under paragraph (c)(1)(ii), contractors shall rapidly report cyber incidents to DoD. Approximately 200 cyber incident reports are submitted each year, and it can take from a few minutes to complete up to eight hours; therefore, a median of four 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. DoD estimates that approximately 40 contractors will be required each year to provide media for damage assessments, and, on average, it takes 10 hours to prepare and submit the media. In FY 2018, there were 37 media submissions.

Estimation of Respondent Burden Hours and Labor Costs	
Number of respondents	200
Responses per respondent	1.2
Number of responses	240
Hours per response	5

Estimated hours (number of responses multiplied hours per response)	1,200
Cost per hour (hourly wage)	$76
Annual public burden (estimated hours multiplied by cost per hour)	$91,200

b. *252.204-7008, Compliance with Safeguarding Covered Defense Information Controls:* DoD estimates that approximately 5 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 ten or more members of the public, the estimate of five is increased to ten to perpetuate the clearance for this provision to ensure coverage in the event of future increases in requests.

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)	$76
Annual public burden (estimated hours multiplied by cost per hour)	$760

c. *252.239-7009, Representation of Use of Cloud Computing:* Offerors will be 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), there were 8,671 new contract awards were made to 1,787 unique entities for IT related services in FY 2018. It is estimated that there are approximately four offerors competing for each of the awards, which results in a total of approximately 34,684 responses. The same offeror may submit multiple responses to IT solicitations; and, while we can identify the 1,787 unique contractors who received the awards, there is no specific data available to identify the unique number of offerors who submitted the estimated 34,684 solicitation responses. For the purposes of the estimate, DoD is assuming that the 1,787 unique awardees were the same entities submitted offers on the 8,671 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 and Labor Costs	
Number of respondents	1,787
Responses per respondent	19.4
Number of responses	34,684
Hours per response (15 minutes)	0.25
Estimated hours (number of responses multiplied hours per response)	8,671
Cost per hour (hourly wage)	$76

Annual public burden (estimated hours multiplied by cost per hour)	$658,996

d. *252.239-7010, Cloud Computing Services:* Offerors are required to represent their intentions to utilize cloud computing services in response to all solicitations for information technology services. 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. For cyber incident reporting, while there has only been one report, ten respondents and responses requiring 4 hours per response are estimated in order to continue the PRA clearance for this report. Similarly, to continue the clearance, ten media submissions are estimated for the cyber reports, which would require 10 hours per submission to submit. Third-party requests are estimated to be a rare occurrence, and a total of ten respondents and responses is projected, and each request is expected to take 4 hours to prepare and submit.

Estimation of Respondent Burden Hours and Labor Costs	
Number of respondents	10
Responses per respondent	3
Number of responses	30
Hours per response	6
Estimated hours (number of responses multiplied hours per response)	180
Cost per hour (hourly wage)	$76
Annual public burden (estimated hours multiplied by cost per hour)	$13,680

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	2,017
Responses per respondent	17.34
Number of responses	34,974
Hours per response (approximately)	.29
Estimated hours (number of responses multiplied hours per response)	10,071
Cost per hour (hourly wage)	$76
Annual public burden (estimated hours multiplied by cost per hour)	$765,396

13. Respondent Costs Other Than Burden Hour Costs

DoD does not estimate any burden hours apart from the hours in items 12 and 14.

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/Resp	Total Hours	Cost/Hr	Total Cost
252.204-7012(b)(2)(ii)(B)	10	1	10	$76	$760
252.204-7012(c)(1)(ii)	200	4	800	$76	$60,800
252.204-7012(g)	40	10	400	$76	$30,400
252.204-7008(c)(2)(i)	10	1	10	$76	$760
252.239-7009	34,684	.08	2,775	$76	$210,900
252.239-7010(d)	10	4	40	$76	$3,040
252.239-7010(f/h)	10	10	100	$76	$7,600
252.239-7010(j)	10	4	40	$76	$3,040
Total			4,175	$76	$317,300

15. Reasons for Change in Burden

This information collection updates the existing collection approval by reducing the estimated number of DoD contractors and offerors expected to report and the associated burden hours. As a result, 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. The area of greatest decrease is for reporting of cyber incidents. Previously, the total number of cleared defense contractors (10,000) was used to project the estimated number of probable cyber incidents, and it was estimated that each of these contractors would submit five reports. The estimates for this 2019 renewal uses the actual number of reports submitted to DoD during FY 2018 via the web portal at http://dibnet.dod.mil as the baseline for the estimate.

OMB Control #0704-0478	2015 Estimate	2019 Estimate	Change in Burden
Number of respondents	10,954	2,017	-8,937
Total annual responses	60,493	34,974	-25,520
Total hours	250,840	10,071	-240,769
Total annual cost to public	$16,053,494	$765,396	-$15,288,098

16. Publication of Results

Results of this information will not be tabulated or published.

17. Non-Display of OMB Expiration Date

DoD is not requesting approval to omit display of the expiration date of OMB approval on the instrument of collection.

18. Exceptions to "Certification for Paperwork Reduction Submissions"

DoD is not requesting exception to satisfy the statutory requirements.

B. COLLECTION OF INFORMATION EMPLOYING STATISTICAL METHODS

Statistical methods will not be employed.