5001-06-P

DEPARTMENT OF DEFENSE

Defense Acquisition Regulations System

[Docket Number DARS-2019-0021; OMB Control Number 0704-0478]

Information Collection Requirement; Defense Federal Acquisition Regulation Supplement (DFARS); Cyber Incident Reporting and Cloud Computing; Submission for OMB Review; Comment Request

AGENCY: Defense Acquisition Regulations System, Department of Defense (DoD).

ACTION: Notice.

SUMMARY: The Defense Acquisition Regulations System has submitted to OMB for clearance, the following proposal for collection of information under the provisions of the Paperwork Reduction Act.

DATES: Consideration will be given to all comments received by **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**

SUPPLEMENTARY INFORMATION:

A. TITLE AND OMB NUMBER. Safeguarding Covered Defense Information, Cyber Incident Reporting, and Cloud Computing; OMB Control Number 0704-0478.

B. NEEDS AND USES. 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.

C. ANNUAL BURDEN.

Number of Respondents: 2,017.

Responses per Respondent: 17.35.

Annual Responses: 34,974.

Average Burden Per Response: .29 hours.

Annual Burden Hours: 10,071.

Reporting Frequency: On Occasion

Affected Public. Businesses or other for-profit and not-for-profit institutions.

Respondent's Obligation: Required to obtain or retain benefits.

Frequency: On occasion.

Type of Request: Renewal of a currently approved collection.

D. PUBLIC COMMENTS.

A 60-day notice was published in the *Federal Register* at 84 FR 23532 on May 22, 2019. One respondent provided four comments, which are summarized below along with responses; however, the comments did not change the estimate of the burden.

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: (1) 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 (2) 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 points of contact (i.e., contracting officer, contracting officer's representative, or requiring activity) 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 CDI, 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.

E. DESK OFFICER. Comments and recommendations on the proposed information collection should be sent to Ms. Jasmeet Seehra, DoD Desk Officer, at *Oira_submission@omb.eop.gov*. Please identify the proposed information collection by DoD Desk Officer and the

Docket ID number and title of the information collection

You may also submit comments, identified by docket number and title, to: *Federal eRulemaking Portal*: *http://www.regulations.gov*. Follow the instructions for submitting comments.

F. DoD CLEARANCE OFFICER: Ms. Angela James. Written requests for copies of the information collection proposal should be sent to Ms. James at *whs.mc-alex.esd.mbx.dd-dod-information-collections@mail.mil*.

Jennifer Lee Hawes,

Regulatory Control Officer, Defense Acquisition Regulations System.

[FR Doc. 2019-16149 Filed: 7/29/2019 8:45 am; Publication Date: 7/30/2019]