



DEPARTMENT OF DEFENSE

Defense Acquisition Regulations System

[Docket DARS-2020-0038; OMB Control No. 0750-0004]

Information Collection Requirement; Defense Federal Acquisition Regulation Supplement (DFARS); Assessing Contractor Implementation of Cybersecurity Requirements

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

ACTION: Notice and request for comments regarding a proposed extension of an approved information collection requirement.

SUMMARY: In compliance with the Paperwork Reduction Act of 1995, DoD announces the proposed extension of a public information collection requirement and seeks public comment on the provisions thereof. DoD invites comments on: 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 accuracy of the estimate of the burden of the proposed information collection; ways to enhance the quality, utility, and clarity of the information to be collected; and ways to minimize the burden of the information collection on respondents, including the use of automated collection techniques or other forms of information technology. The Office of Management and Budget (OMB) has approved this information collection for use through April 30, 2021. DoD proposes that OMB extend its approval for use for three additional years beyond the current expiration date.

DATES: Consideration will be given to all comments received by
[Insert date 60 days after date of publication in the FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by OMB Control Number 0750-0004, using any of the following methods:

Federal eRulemaking Portal: <http://www.regulations.gov>.

Follow the instructions for submitting comments.

Email: osd.dfars@mail.mil. Include OMB Control Number 0750-0004 in the subject line of the message.

Mail: Defense Acquisition Regulations System, Attn: Ms. Heather Kitchens, OUSD(A&S)DPC(DARS), 3060 Defense Pentagon, Room 3B938, Washington, DC 20301-3060.

Comments received generally will be posted without change to <http://www.regulations.gov>, including any personal information provided.

FOR FURTHER INFORMATION CONTACT: Ms. Heather Kitchens, telephone 571-372-6104.

SUPPLEMENTARY INFORMATION:

Title and OMB Number: Defense Federal Acquisition Regulation Supplement (DFARS), Assessing Contractor Implementation of Cybersecurity Requirements; OMB Control Number 0750-0004.

Affected Public: Businesses and other for-profit entities.

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

Type of Request: Extension of a currently approved collection.

Reporting Frequency: On occasion.

DOD estimates the annual public reporting burden for the information collection as follows:

a. *Basic Assessment*

Respondents: 13,068.

Responses per respondent: 1 approximately.

Total annual responses: 13,068.

Hours per response: .75.

Total burden hours: 9,801.

b. *Medium Assessment*

Respondents: 200.

Responses per respondent: 1.

Total annual responses: 200.

Hours per response: 8.

Total burden hours: 1,600.

c. *High Assessment*

Respondents: 110.

Responses per respondent: 1.

Total annual responses: 110.

Hours per response: 420.

Total burden hours: 46,200.

d. *Total Public Burden (All Entities)*

Respondents: 13,068.

Total annual responses: 13,378.

Total burden hours: 57,601.

e. *Total Public Burden (Small Entities)*

Respondents: 8,823.

Total annual responses: 9,023.

Total burden hours: 41,821.

DoD requested and OMB authorized emergency processing of an information collection that was assigned OMB Control Number 0750-0004. DFARS interim rule, Case 2019-D041, *Assessing Contractor Implementation of Cybersecurity Requirements*, published in the *Federal Register* at 85 FR 61505 on September 29, 2020, also provided a discussion of this information collection requirement.

Needs and Uses: The collection of information is necessary for DoD to immediately begin assessing where vulnerabilities in its supply chain exist and take steps to correct such deficiencies. In addition, the collection of information is necessary to ensure Defense Industrial Base (DIB) contractors that have not fully implemented the NIST SP 800-171 security requirements pursuant to DFARS 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, begin correcting these deficiencies immediately.

This collection of information supports implementation of section 1648 of the National Defense Authorization Act for Fiscal Year 2020 (Pub. L. 116-92). Section 1648(c)(2) directs the Secretary of Defense to develop a risk-based cybersecurity framework for the DIB sector, such as the Cybersecurity Maturity Model Certification (CMMC) framework, as the basis for a mandatory DoD standard. This requirement is implemented in the DFARS through the provision at 252.204-7019, *Notice of NIST SP 800-171 DoD Assessment Requirement*, and the clause at 252.204-7020, *NIST SP 800-171 DoD Assessment Requirements*. This information collection covers the following requirements:

- DFARS 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirement, is prescribed for use in all solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial items, except for solicitations solely for the acquisition of commercially available off-the-shelf (COTS) items. Per the new provision, if an offeror is required to have implemented NIST SP 800-171 per DFARS clause 252.204-7012, then the offeror shall have a current assessment posted in the Supplier Performance Risk System (SPRS) for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order in order to be considered for award. If the offeror does not have summary level scores of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old, unless a lesser time is specified in the solicitation) posted in SPRS, the offeror may conduct and submit a Basic Assessment for posting in SPRS.

- DFARS 252.204-7020, NIST SP 800-171 DoD Assessment Requirements, is prescribed for use in in all solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items, except for solicitations and contracts solely for the acquisition of COTS items. The clause requires the contractor to provide the Government access to its facilities, systems, and personnel in order to conduct a Medium or High Assessment, if necessary. For Basic Assessments, the contractor may submit summary level scores for posting to SPRS. Medium Assessments are assumed to be conducted by DoD Components, primarily by Program Management

Office cybersecurity personnel, in coordination with the Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC), as part of a separately scheduled visit (e.g., for a Critical Design Review). High Assessments will be conducted by, or in conjunction with, the DCMA DIBCAC. The Department may choose to conduct a Medium or High Assessment when warranted based on the criticality of the program(s)/technology(ies) associated with the contracted effort(s). For example, a Medium Assessment may be initiated by a Program Office that has determined that the risk associated with their programs warrants going beyond the Basic self-assessment. The results of that Medium Assessment may satisfy the Program Office, or may indicate the need for a High assessment. DoD will provide Medium and High Assessment summary level scores to the contractor and offer the opportunity for rebuttal and adjudication of assessment summary level scores prior to posting the summary level scores to SPRS. The requirements of this clause flow down to subcontractors.

Jennifer D. Johnson,

Regulatory Control Officer, Defense Acquisition Regulations System.

[FR Doc. 2020-24562 Filed: 11/4/2020 8:45 am; Publication Date: 11/5/2020]