GAO@100 U.S. GOVERNMENT ACCOUNTABILITY OFFICE
A Century of Non-Partisan Fact-Based Work

441 G St. N.W.
Washington, DC 20548

B-332975

February 23, 2021

The Honorable Jack Reed
Chairman
The Honorable James Inhofe
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Adam Smith
Chairman
The Honorable Mike Rogers
Ranking Member
Committee on Armed Services
House of Representatives

Subject: *Department of Defense, Defense Acquisition Regulations System: Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019–D041)*

Pursuant to section 801(a)(2)(A) of title 5, United States Code, this is our report on a major rule promulgated by the Department of Defense, Defense Acquisition Regulations System (DOD) entitled "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019–D041)" (RIN: 0750-AJ81). We received the rule on November 25, 2020.[1] It was published in the *Federal Register* as an interim rule on September 29, 2020. 85 Fed. Reg. 61505. The stated effective date of the rule is November 30, 2020.

According to DOD, this interim rule amends the Defense Federal Acquisition Regulation Supplement to implement a DOD Assessment Methodology and Cybersecurity Maturity Model Certification framework. DOD states this was done in order to assess contractor implementation of cybersecurity requirements and enhance the protection of unclassified information within the DOD supply chain.

The Congressional Review Act (CRA) requires a 60-day delay in the effective date of a major rule from the date of publication in the *Federal Register* or receipt of the rule by Congress, whichever is later. 5 U.S.C. § 801(a)(3)(A). This interim rule was published in the *Federal Register* on September 29, 2020. 85 Fed. Reg. 61505. The Senate received the rule on December 1, 2020. 166 Cong. Rec. S7326 (daily ed. Dec. 9, 2020). The House of Representatives received the rule on December 2, 2020. 166 Cong. Rec. H6856 (daily ed.

[1] The due date for this major rule report was December 17, 2020. Due to a processing error on our part, we did not determine that the submission was a major rule, which delayed our issuance of this report.

Dec. 4, 2020). The rule has a stated effective date of November 30, 2020. Therefore the final rule does not have the required 60-day delay in its effective date.

Enclosed is our assessment of DOD's compliance with the procedural steps required by section 801(a)(1)(B)(i) through (iv) of title 5 with respect to the rule. If you have any questions about this report or wish to contact GAO officials responsible for the evaluation work relating to the subject matter of the rule, please contact Shari Brewster, Assistant General Counsel, at (202) 512-6398.

Shirley A. Jones
Managing Associate General Counsel

Enclosure

cc: Patricia Toppings
OSD Federal Regulations Liaison Officer
Department of Defense

ENCLOSURE

REPORT UNDER 5 U.S.C. § 801(a)(2)(A) ON A MAJOR RULE
ISSUED BY THE
DEPARTMENT OF DEFENSE,
DEFENSE ACQUISITION REGULATIONS SYSTEM
ENTITLED
"DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENT:
ASSESSING CONTRACTOR IMPLEMENTATION OF
CYBERSECURITY REQUIREMENTS (DFARS CASE 2019–D041)"
(RIN: 0750-AJ81)

(i) Cost-benefit analysis

The Department of Defense, Defense Acquisition Regulations System (DOD) estimated the total annualized net costs associated with this interim rule to be $6,500,700,000, calculated in perpetuity in 2016 dollars at a 7 percent discount rate. According to DOD, the total annualized net costs comprise of estimated annualized costs of $16,300,000 associated with the National Institute of Standards and Technology (NIST) Special Publication (SP) DOD Assessments and $6,533,900,000 associated with the Cybersecurity Maturity Model Certification requirements, as well as estimated annualized savings of $49,400,000 associated with elimination of duplicate assessments. DOD further expected an unquantified benefit of enhanced protection of Federal Contract Information and Controlled Unclassified Information (CUI) within the defense industrial base sector from malicious cyber activity that threaten U.S. economic and national security.

(ii) Agency actions relevant to the Regulatory Flexibility Act (RFA), 5 U.S.C. §§ 603-605, 607, and 609

DOD prepared an initial regulatory flexibility analysis for this interim rule. The analysis included (1) a statement of the reason for the action; (2) a statement of the objectives of, and legal basis for, the rule; (3) a description and estimate of the number of small entities to which the rule will apply; (4) a description of projected reporting, recordkeeping, and other compliance requirements of the rule; (5) a description of relevant federal rules, which may duplicate, overlap, or conflict with the rule; and (6) a description of any significant alternatives to the rule which accomplish the stated objectives of applicable statutes and which minimize any significant economic impact of the rule on small entities.

(iii) Agency actions relevant to sections 202-205 of the Unfunded Mandates Reform Act of 1995, 2 U.S.C. §§ 1532-1535

The interim rule did not discuss the Act. In its submission to us, DOD indicated that preparation of a written statement under section 202 of the Act is not applicable to this interim rule.

(iv) Other relevant information or requirements under acts and executive orders

Administrative Procedure Act, 5 U.S.C. §§ 551 *et seq.*

DOD did not discuss the Administrative Procedure Act in this interim rule. DOD stated that it made a determination pursuant to section 1707(d) of title 41, United States Code, that urgent and compelling circumstances made compliance with the notice and comment requirements for

procurement regulations under section 1707(a) of title 41, United States Code, impracticable. Specifically, DOD stated that this rule provides the requirement for defense contractors to demonstrate implementation of standard cybersecurity processes and practices, which is necessary to ensure cybersecurity requirements are fully implemented to protect DOD and the defense industry base from malicious cyber activity. According to DOD, there is an urgent need for DOD to immediately begin assessing where vulnerabilities in its supply chain exist and take steps to correct such deficiencies, which can be accomplished by requiring contractors and subcontractors that handle DOD CUI on their information systems to complete a NIST SP 800-171 Basic Assessment. To that end, DOD further stated that, while this rule includes a delayed effective date from date of publication, contractors and subcontractors required to implement NIST SP 800-171 are encouraged to immediately conduct and submit a self-assessment as described in the rule to facilitate DOD's assessment. DOD also stated there is an equally urgent need to ensure the defense industry base contractors that have not fully implemented the basic safeguarding requirements under the current security requirements begin correcting those deficiencies immediately.

According to DOD, while a public comment process will not be completed prior to the rule's effective date, DOD has incorporated feedback solicited through extensive outreach already undertaken pursuant to section 1648(d) of the National Defense Authorization Act for Fiscal Year 2020, including through public meetings and extensive industry outreach conducted over the past year. Pub. L. 116-92, 133 Stat. 1198, 1757 (Dec. 20, 2019). DOD further stated, pursuant to section 1707 of title 41, United States Code, and section 1.501-3(b) of the Federal Acquisition Regulation, DOD will consider public comments received in response to this interim rule on or before November 30, 2020, in the formation of the final rule.

Paperwork Reduction Act (PRA), 44 U.S.C. §§ 3501-3520

DOD determined that this interim rule contains information collection requirements (ICR) under the Act. According to DOD, the Office of Management and Budget (OMB) authorized emergency processing of the ICR associated with this rule, consistent with 5 C.F.R. part 1320.13. DOD stated that it intends to provide a separate notice in the *Federal Register* requesting public comment on the ICR associated with this rule, titled "Assessing Contractor Implementation of Cybersecurity Requirements" (OMB Control Number 0750-0004). DOD estimated the total annual public reporting burden for the ICR associated with this rule would be 57,601 hours.

Statutory authorization for the rule

DOD promulgated this interim rule pursuant to section 1303 of title 41, United States Code.

Executive Order No. 12866 (Regulatory Planning and Review)

DOD determined that this interim rule is economically significant under the Order.

Executive Order No. 13132 (Federalism)

The interim rule did not address the Order. In its submission to us, DOD indicated that the Order was not applicable to this rule.