either to ensure that model weights do not become available, or to protect system integrity or human well-being (including privacy) and reduce security risks in those cases where weights are widely available?

c. What are the prospects for developing effective safeguards in the future?

d. Are there ways to regain control over and/or restrict access to and/or limit use of weights of an open foundation model that, either inadvertently or purposely, have already become widely available? What are the approximate costs of these methods today? How reliable are they?

e. What if any secure storage techniques or practices could be considered necessary to prevent unintentional distribution of model weights?

f. Which components of a foundation model need to be available, and to whom, in order to analyze, evaluate, certify, or red-team the model? To the extent possible, please identify specific evaluations or types of evaluations and the component(s) that need to be available for each.

g. Are there means by which to test or verify model weights? What methodology or methodologies exist to audit model weights and/or foundation models?

6. What are the legal or business issues or effects related to open foundation models?

a. In which ways is open-source software policy analogous (or not) to the availability of model weights? Are there lessons we can learn from the history and ecosystem of open-source software, open data, and other ''open'' initiatives for open foundation models, particularly the availability of model weights?

b. How, if at all, does the wide availability of model weights change the competition dynamics in the broader economy, specifically looking at industries such as but not limited to healthcare, marketing, and education?

c. How, if at all, do intellectual property-related issues—such as the license terms under which foundation model weights are made publicly available—influence competition, benefits, and risks? Which licenses are most prominent in the context of making model weights widely available? What are the tradeoffs associated with each of these licenses?

d. Are there concerns about potential barriers to interoperability stemming from different incompatible ''open'' licenses, *e.g.,* licenses with conflicting requirements, applied to AI components? Would standardizing license terms specifically for foundation model weights be beneficial? Are there particular examples in existence that could be useful?

7. What are current or potential voluntary, domestic regulatory, and international mechanisms to manage the risks and maximize the benefits of foundation models with widely available weights? What kind of entities should take a leadership role across which features of governance?

a. What security, legal, or other measures can reasonably be employed to reliably prevent wide availability of access to a foundation model's weights, or limit their end use?

b. How might the wide availability of open foundation model weights facilitate, or else frustrate, government action in AI regulation?

c. When, if ever, should entities deploying AI disclose to users or the general public that they are using open foundation models either with or without widely available weights?

d. What role, if any, should the U.S. government take in setting metrics for risk, creating standards for best practices, and/or supporting or restricting the availability of foundation model weights?

i. Should other government or non-government bodies, currently existing or not, support the government in this role? Should this vary by sector?

e. What should the role of model hosting services (*e.g.,* HuggingFace, GitHub, etc.) be in making dual-use models with open weights more or less available? Should hosting services host models that do not meet certain safety standards? By whom should those standards be prescribed?

f. Should there be different standards for government as opposed to private industry when it comes to sharing model weights of open foundation models or contracting with companies who use them?

g. What should the U.S. prioritize in working with other countries on this topic, and which countries are most important to work with?

h. What insights from other countries or other societal systems are most useful to consider?

i. Are there effective mechanisms or procedures that can be used by the government or companies to make decisions regarding an appropriate degree of availability of model weights in a dual-use foundation model or the dual-use foundation model ecosystem? Are there methods for making effective decisions about open AI deployment that balance both benefits and risks? This may include responsible capability scaling policies, preparedness frameworks, et cetera.

j. Are there particular individuals/entities who should or should not have access to open-weight foundation models? If so, why and under what circumstances?

8. In the face of continually changing technology, and given unforeseen risks and benefits, how can governments, companies, and individuals make decisions or plans today about open foundation models that will be useful in the future?

a. How should these potentially competing interests of innovation, competition, and security be addressed or balanced?

b. Noting that E.O. 14110 grants the Secretary of Commerce the capacity to adapt the threshold, is the amount of computational resources required to build a model, such as the cutoff of $10^{26}$ integer or floating-point operations used in the Executive order, a useful metric for thresholds to mitigate risk in the long-term, particularly for risks associated with wide availability of model weights?

c. Are there more robust risk metrics for foundation models with widely available weights that will stand the test of time? Should we look at models that fall outside of the dual-use foundation model definition?

9. What other issues, topics, or adjacent technological advancements should we consider when analyzing risks and benefits of dual-use foundation models with widely available model weights?

Dated: February 20, 2024.

**Stephanie Weiner,**

*Chief Counsel, National Telecommunications and Information Administration.*

[FR Doc. 2024–03763 Filed 2–23–24; 8:45 am]

**BILLING CODE 3510–60–P**

## DEPARTMENT OF DEFENSE

### Defense Acquisition Regulations System

**[Docket No. 2024–0006; OMB Control No. 0750–0004]**

### Information Collection Requirement; Defense Federal Acquisition Regulation Supplement; 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 DoD's 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 through 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 under Control Number 0750–0004 through June 30, 2024. DoD proposes that OMB approve an extension of the information collection requirement, to expire three years after the approval date.

**DATES:** DoD will consider all comments received by April 26, 2024.

**ADDRESSES:** You may submit comments, identified by OMB Control Number 0750–0004, using either of the following methods:

○ *Federal eRulemaking Portal: https://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.

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

**FOR FURTHER INFORMATION CONTACT:** Ms. Heather Kitchens, at 571–296–7152.

**SUPPLEMENTARY INFORMATION:**

*Title and OMB Number:* Defense Federal Acquisition Regulation Supplement (DFARS); Part 204 and Related Clauses, 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.

*Reporting Frequency:* At least annually.

*Number of Respondents:* 11,686.

*Responses Per Respondent:* 1.02, approximately

*Annual Responses:* 11,977.

*Average Burden per Response:* 4.92 hours

*Annual Burden Hours:* 58,885.

*Needs and Uses:* The collection of information is necessary for DoD to assess where vulnerabilities exist in its supply chain 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 National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171 security requirements pursuant to the clause at DFARS 252.204–7012 begin correcting these deficiencies immediately.

This requirement 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 as the basis for a mandatory DoD standard.

This requirement is implemented in the Defense Federal Acquisition Regulation Supplement (DFARS) through the solicitation provision at 252.204–7019, Notice of NIST SP 800–171 DoD Assessment Requirement, and the contract clause at 252.204–7020, NIST SP 800–171 DoD Assessment Requirements.

This clearance 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 products and commercial services, except for solicitations solely for the acquisition of commercially available off-the-shelf (COTS) items. Per the 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 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.
- 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 products and commercial services, 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 Assessment or High Assessment, if necessary. 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's DCMA's 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, DCMA's DIBCAC. DoD may choose to conduct a Medium Assessment 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 who 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.

**Jennifer Johnson,**

*Editor/Publisher, Defense Acquisition Regulations System.*

[FR Doc. 2024–03809 Filed 2–23–24; 8:45 am]

**BILLING CODE 6001–FR–P**

## DEPARTMENT OF EDUCATION

**[Docket No.: ED–2023–SCC–0217]**

## Agency Information Collection Activities; Submission to the Office of Management and Budget for Review and Approval; Comment Request; Comprehensive Literacy Program Evaluation: Comprehensive Literacy State Development (CLSD) Program Evaluation

**AGENCY:** Institute of Education Sciences, Department of Education (ED).

**ACTION:** Notice.

**SUMMARY:** In accordance with the Paperwork Reduction Act (PRA) of 1995, the Department is proposing an extension without change of a currently approved information collection request (ICR).

**DATES:** Interested persons are invited to submit comments on or before March 27, 2024.

**ADDRESSES:** Written comments and recommendations for proposed information collection requests should be submitted within 30 days of publication of this notice. Click on this link *www.reginfo.gov/public/do/PRAMain* to access the site. Find this information collection request (ICR) by selecting ''Department of Education'' under ''Currently Under Review,'' then