

DEPARTMENT OF EDUCATION**[Docket No. ED–2021–SCC–0095]****Agency Information Collection Activities; Submission to the Office of Management and Budget for Review and Approval; Comment Request; Trends in International Mathematics and Science Study (TIMSS 2023) Field Test Data Collection and Main Study Sampling, Recruitment, and Data Collection****AGENCY:** Institute of Education Sciences (IES), Department of Education (ED).**ACTION:** Notice.

SUMMARY: In accordance with the Paperwork Reduction Act of 1995, ED is proposing a revision of a currently approved collection.

DATES: Interested persons are invited to submit comments on or before December 27, 2021.

ADDRESSES: Written comments and recommendations for proposed information collection requests should be sent within 30 days of publication of this notice to www.reginfo.gov/public/do/PRAMain. Find this information collection request by selecting “Department of Education” under “Currently Under Review,” then check “Only Show ICR for Public Comment” checkbox. Comments may also be sent to ICDocketmgr@ed.gov.

FOR FURTHER INFORMATION CONTACT: For specific questions related to collection activities, please contact Carrie Clarady, (202) 245–6347.

SUPPLEMENTARY INFORMATION: The Department of Education (ED), in accordance with the Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3506(c)(2)(A)), provides the general public and Federal agencies with an opportunity to comment on proposed, revised, and continuing collections of information. This helps the Department assess the impact of its information collection requirements and minimize the public’s reporting burden. It also helps the public understand the Department’s information collection requirements and provide the requested data in the desired format. ED is soliciting comments on the proposed information collection request (ICR) that is described below. The Department of Education is especially interested in public comment addressing the following issues: (1) Is this collection necessary to the proper functions of the Department; (2) will this information be processed and used in a timely manner; (3) is the estimate of burden accurate; (4) how might the Department enhance the quality, utility, and clarity of the

information to be collected; and (5) how might the Department minimize the burden of this collection on the respondents, including through the use of information technology. Please note that written comments received in response to this notice will be considered public records.

Title of Collection: Trends in International Mathematics and Science Study (TIMSS 2023) Field Test Data Collection and Main Study Sampling, Recruitment, and Data Collection.

OMB Control Number: 1850–0695.

Type of Review: Revision of a currently approved collection.

Respondents/Affected Public: Individual or Households.

Total Estimated Number of Annual Responses: 50,996.

Total Estimated Number of Annual Burden Hours: 20,336.

Abstract: The Trends in International Mathematics and Science Study (TIMSS), conducted by the National Center for Education Statistics (NCES), within the U.S. Department of Education (ED), is an international assessment of fourth and eighth grade students’ achievement in mathematics and science. Since its inception in 1995, TIMSS has continued to assess students every 4 years (1995, 1999, 2003, 2007, 2011, 2015, and 2019), with the next TIMSS assessment, TIMSS 2023, being the eighth iteration of the study. In TIMSS 2023, approximately 65 countries or education systems will participate. The United States will participate in TIMSS 2023 to continue to monitor the progress of its students compared to that of other nations and to provide data on factors that may influence student achievement.

TIMSS is led by the International Association for the Evaluation of Educational Achievement (IEA), an international collective of research organizations and government agencies that create the frameworks used to develop the assessment, the survey instruments, and the study timeline. IEA decides and agrees upon a common set of standards, procedures, and timelines for collecting and reporting data, all of which must be followed by all participating countries. As a result, TIMSS is able to provide a reliable and comparable measure of student skills in participating countries. In the U.S., NCES conducts this study in collaboration with the IEA and a number of contractors to ensure proper implementation of the study and adoption of practices in adherence to the IEA’s standards. Participation in TIMSS is consistent with NCES’s mandate of acquiring and disseminating data on educational activities and

student achievement in the United States compared with foreign nations [The Educational Sciences Reform Act of 2002 (ESRA 2002, 20 U.S.C. §9543)].

A previous request to conduct sampling and recruitment activities associated with the TIMSS 2023 field test, which will be conducted in March and April 2022, was approved by OMB in May 2021 (OMB# 1850–0695 v.16). Because TIMSS is a collaborative effort among many parties, the United States must adhere to the international schedule set forth by the IEA, including the availability of final field test and main study plans as well as draft and final questionnaires. In order to meet the international data collection schedule, to align with recruitment for other NCES studies (e.g., the National Assessment of Education Progress, NAEP), and for schools to put the TIMSS 2023 field test assessment on their Spring 2022 calendars, recruitment activities for the field test will begin in June of 2021. This package requests approval for the field test data collection materials and the main study sampling, recruiting, and data collection plans. Recruitment activities for the main study will begin in January 2022, with the data collection activities currently scheduled to begin in March 2023.

Dated: November 19, 2021.

Stephanie Valentine,

PRA Coordinator, Strategic Collections and Clearance, Governance and Strategy Division, Office of Chief Data Officer, Office of Planning, Evaluation and Policy Development.

[FR Doc. 2021–25645 Filed 11–23–21; 8:45 am]

BILLING CODE 4000–01–P

DEPARTMENT OF ENERGY**Request for Information on DOE’s Cybersecurity Capability Maturity Model (C2M2) Version 2.0 (July 2021)**

AGENCY: Office of Cybersecurity, Energy Security, and Emergency Response; Department of Energy.

ACTION: Request for information.

SUMMARY: In July 2021, the Department of Energy (DOE) released Version 2.0 of the Cybersecurity Capability Maturity Model (C2M2), a tool that helps organizations evaluate and improve their cybersecurity capabilities, considering their specific risk environment. The update was guided by input from the Energy Sector C2M2 Working Group, which comprises 145 energy sector cybersecurity practitioners representing 77 energy sector and cybersecurity organizations. Version 2.0 updates the model from Version 1.1,

released in 2014, and includes a variety of updates to the model domains and practices to better address emerging technologies and the evolving cyber threat landscape. Since the release in July, DOE has piloted the updated model with energy companies and utilities. To obtain the broadest possible input, DOE seeks public comment on the C2M2 to inform the C2M2 Working Group as it develops future model updates.

DATES: Comments and information must be received on or before December 27, 2021.

ADDRESSES: To access and review the Cybersecurity Capability Maturity Model (C2M2), visit www.energy.gov/c2m2.

Comments should be submitted by email to C2M2@hq.doe.gov using the Comment Submission Form available here: <https://energy.gov/sites/default/files/2021-11/Comment%20Submission%20Form%20-%20Cybersecurity%20Capability%20Maturity%20Model%20%28C2M2%29.docx>. Use the email subject line: "C2M2 Public Comment from [name/organization]."

Although DOE has routinely accepted public comment submissions through a variety of mechanisms, including postal mail and hand delivery/courier, the Department has found it necessary to make temporary modifications to the comment submission process in light of the ongoing coronavirus 2019 ("COVID-19") pandemic. DOE is currently suspending receipt of public comments via postal mail and hand delivery/courier. If a commenter finds that this change poses an undue hardship, please contact CESER staff at (202) 586-3057 to discuss the need for alternative arrangements. Once the COVID-19 pandemic health emergency is resolved, DOE anticipates resuming all of its regular options for public comment submission, including postal mail and hand delivery/courier.

FOR FURTHER INFORMATION CONTACT: Mr. Fowad Muneer, Acting Deputy Assistant Secretary for the Cybersecurity for Energy Delivery Systems Division, U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response. Tel.: (202) 586-5961. Email: fowad.muneer@hq.doe.gov.

SUPPLEMENTARY INFORMATION: The C2M2 helps organizations evaluate and improve their cybersecurity capabilities, considering their specific risk environment. The model is a voluntary tool, tailored specifically for the energy industry, that enables companies to set targets, evaluate and benchmark their cybersecurity capabilities, and use the results to prioritize actions and

investments. It is scalable for a company of any size, and is designed to evaluate practice in both the information technology (IT) and operational technology (OT) environments.

DOE originally developed the C2M2 with input from energy industry partners in 2012, and released an updated Version 1.1 in 2014, with separate versions targeted for the electricity and oil and natural gas subsectors. Version 2.0, released July 2021, is designed for use across the energy sector, and can be used by other critical infrastructure sectors as well.

The Version 2.0 update was guided by input from the Energy Sector C2M2 Working Group, which DOE formed with the Electricity and Oil & National Gas Subsector Coordinating Councils. The update better addresses new technologies like cloud, mobile, and artificial intelligence, and evolving threats such as ransomware and supply chain risks.

While the structure of the model remains the same, this update resulted in some key changes:

- Revisions to two-thirds of model practices—including substantive changes and clarifications—along with additions, deletions, and combining of practices
- Addition of a Cybersecurity Architecture domain focused on planning, designing, and managing the cybersecurity control environment
- Significant updates to the Risk Management domain to incorporate leading risk management practices and enhance coordination between cyber and enterprise risk management
- Refresh of the Dependencies domain, now called the Third-Party Risk Management domain, to ensure the model effectively addresses third-party IT and OT cybersecurity risks, like sensitive data in the cloud and vendors with privileged access, as well as build supply chain security into organizational culture
- Integration of Information Sharing domain activities into the Threat and Vulnerability Management and Situational Awareness domains
- Addition of help text for each practice to improve clarity and consistency in how practices are applied

DOE requests public comment on the C2M2 to inform the C2M2 Working Group as it develops future model updates. Specifically, DOE seeks input on the following items:

- The usefulness of C2M2 practices in evaluating and improving cybersecurity program capabilities
- The applicability of practice language to the IT and OT environments in use by energy sector organizations

- The readability of and ability to understand practice language
- The completeness of cybersecurity domains, objectives, and practices included within the C2M2
- The effectiveness of guidance documentation (e.g., model introduction sections, domain introductions, and appendices) in conveying model concepts, architecture, and how to use the model
- Any other potential improvements to the C2M2 documentation or practices contained therein

For more information on the C2M2, or to review the model document, visit www.energy.gov/c2m2.

Confidential Business Information: Pursuant to 10 CFR 1004.11, any person submitting information that he or she believes to be confidential and exempt by law from public disclosure should submit via email two well-marked copies: One copy of the document marked "confidential" including all the information believed to be confidential, and one copy of the document marked "non-confidential" with the information believed to be confidential deleted. DOE will make its own determination about the confidential status of the information and treat it according to its determination.

Signing Authority

This document of the Department of Energy was signed on November 18, 2021, by Fowad Muneer, Acting Deputy Assistant Secretary for the Cybersecurity for Energy Delivery Systems Division, pursuant to delegated authority from the Secretary of Energy. That document with the original signature and date is maintained by DOE. For administrative purposes only, and in compliance with requirements of the Office of the Federal Register, the undersigned DOE Federal Register Liaison Officer has been authorized to sign and submit the document in electronic format for publication, as an official document of the Department of Energy. This administrative process in no way alters the legal effect of this document upon publication in the **Federal Register**.

Signed in Washington, DC, on November 19, 2021.

Treena V. Garrett,
Federal Register Liaison Officer, U.S.
Department of Energy.

[FR Doc. 2021-25669 Filed 11-23-21; 8:45 am]

BILLING CODE 6450-01-P