The meeting will be closed to the public in accordance with the provisions set forth in sections 552b(c)(4) and 552b(c)(6), title 5 U.S.C., as amended. The grant applications and the discussions could disclose confidential trade secrets or commercial property such as patentable material, and personal information concerning individuals associated with the grant applications, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

Name of Committee: National Institute of Environmental Health Sciences Special Emphasis Panel; NIEHS Review of U/R24 Applications.

Date: July 16, 2024.
Time: 10:30 a.m. to 5:30 p.m.
Agenda: To review and evaluate grant applications.
Place: National Institute of Environmental Health Sciences, Keystone Building, 530 Davis Drive, Durham, NC 27709 (Virtual Meeting).
Contact Person: Leroy Worth, Ph.D., Scientific Review Officer, Scientific Review Branch, Division of Extramural Research and Training, Nat. Institute of Environmental Health Sciences, P.O. Box 12233, MD, EC–30/Room 3171, Research Triangle Park, NC 27709, (984) 287–3340, *worth@niehs.nih.gov.*
(Catalogue of Federal Domestic Assistance Program Nos. 93.115, Biometry and Risk Estimation—Health Risks from Environmental Exposures; 93.142, NIEHS Hazardous Waste Worker Health and Safety Training; 93.143, NIEHS Superfund Hazardous Substances—Basic Research and Education; 93.894, Resources and Manpower Development in the Environmental Health Sciences; 93.113, Biological Response to Environmental Health Hazards; 93.114, Applied Toxicological Research and Testing, National Institutes of Health, HHS)

Dated: June 13, 2024.

Miguelina Perez,
Program Analyst, Office of Federal Advisory Committee Policy.
[FR Doc. 2024–13431 Filed 6–18–24; 8:45 am]
BILLING CODE 4140–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

National Heart, Lung, and Blood Institute; Notice of Meeting

Pursuant to section 1009 of the Federal Advisory Committee Act, as amended, notice is hereby given of a meeting of the Sleep Disorders Research Advisory Board.

The meeting will be held as a virtual meeting and will be open to the public as indicated below. Individuals who plan to view the virtual meeting and need special assistance or other reasonable accommodations to view the

meeting, should notify the Contact Person listed below in advance of the meeting.

The event is free and open to the public, however, registration is required. Please use this link to register: *https://nih.zoomgov.com/webinar/register/WN_otFJ3BJ6TZKuU5yghL59GQ.*

Name of Committee: Sleep Disorders Research Advisory Board.
Date: August 1, 2024.
Time: 1:00 p.m. to 4:00 p.m.
Agenda: The purpose of this meeting is to update the Advisory Board and stakeholders on the progress of sleep and circadian research activities across NIH.
Place: National Institutes of Health, Rockledge Centre I, 6705 Rockledge Drive, Bethesda, Maryland 20892 (Virtual Meeting).
Contact Person: Marishka Brown, Ph.D., SDRAB, Executive Secretary, Director, National Center on Sleep Disorders Research, National Heart, Lung, and Blood Institute, National Institutes of Health, 6705 Rockledge Dr., RKL1/407–B, Bethesda, MD 20814–7952, 301.435.0199, *ncsdr@nih.gov.*

Any member of the public interested in presenting oral comments to the committee may notify the Contact Person listed on this notice at least 10 days in advance of the meeting. Interested individuals and representatives of organizations may submit a letter of intent, a brief description of the organization represented, and a short description of the oral presentation. Only one representative of an organization may be allowed to present oral comments and if accepted by the committee, presentations may be limited to five minutes. Both printed and electronic copies are requested for the record. In addition, any interested person may file written comments with the committee by forwarding their statement to the Contact Person listed on this notice. The statement should include the name, address, telephone number and when applicable, the business or professional affiliation of the interested person.

Information is also available on the Sleep Disorders Research Advisory Board's home page: *https://www.nhlbi.nih.gov/about/advisory-and-peer-review-committees/sleep-disorders-research* where an agenda and any additional information for the meeting will be posted when available.

(Catalogue of Federal Domestic Assistance Program Nos. 93.233, National Center for Sleep Disorders Research; 93.837, Heart and Vascular Diseases Research; 93.838, Lung Diseases Research; 93.839, Blood Diseases and Resources Research, National Institutes of Health, HHS)

Dated: June 13, 2024.

David W. Freeman,
Supervisory Program Analyst, Office of Federal Advisory Committee Policy.
[FR Doc. 2024–13430 Filed 6–18–24; 8:45 am]
BILLING CODE 4140–01–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2024–0016]

Agency Information Collection Activities: National Initiative for Cybersecurity Careers and Studies Cybersecurity Education and Training Catalog Collection

AGENCY: Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS).

ACTION: 60-Day notice and request for comments; revised information collection request: 1670–0030.

SUMMARY: NICCS within CISA will submit the following Information Collection Request (ICR) to the Office of Management and Budget (OMB) for review and clearance.

DATES: Comments are encouraged and will be accepted until August 19, 2024. Submissions received after the deadline for receiving comments may not be considered.

ADDRESSES: You may submit comments, identified by docket number CISA–2024–0016, at: Federal eRulemaking Portal: *http://www.regulations.gov.* Please follow the instructions for submitting comments.

Instructions: All submissions received must include the agency name and docket number CISA–2024–0016. All comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to *http://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: Shannon Nguyen, 703–705–6246, *shannon.nguyen@cisa.dhs.gov.*

SUPPLEMENTARY INFORMATION: The Cybersecurity and Infrastructure Security Agency (CISA) Office of the Chief Learning Officer (OCLO) National Initiative for Cybersecurity Careers and Studies (NICCS) Training Catalog Batch Data seeks to collect information from organizations and academic institutions regarding their course specific technical information to NICCS regarding how their training courses map to the National Initiative for Cybersecurity (NICE) Workforce Framework for Cybersecurity (NICE Framework) Specialty Areas.

The NICCS website is a national online resource for cybersecurity awareness, education, talent management, and professional

development and training. Its mission is to provide comprehensive cybersecurity resources to the public.

To promote cybersecurity education, and to provide a comprehensive resource for the Nation, NICCS developed the Cybersecurity Training and Education Catalog. The NICCS Education and Training Catalog is a central location to help cybersecurity professionals of all skill levels find cybersecurity-related courses online and in person across the nation. All of the courses are aligned to the specialty areas of The Workforce Framework for Cybersecurity (NICE Framework). Organizations and or academic institution interested in listing courses with NICCS are requested to complete a vendor vetting process in order to be considered for inclusion in the NICCS education and Training Catalog. Once approved, organizations and academic institutions are asked to provide technical information ("training catalog batch data") to NICCS regarding how their training courses map to the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (NICE Framework) Specialty Areas. Course mapping to these Specialty Areas allows users to tailor their individual coursework and is dependent upon the training catalog batch data to do so. The training catalog batch data is technical in nature, is not privacy sensitive, and does not include personally identifiable information. The training catalog batch data is submitted to the CISA NICCS Supervisory Office (SO) for review. Then upon further review and approval, the organization/academic institution's course is listed in the NICCS Education and Training Catalog.

The cyber-specific authorities to receive such information support the Department's general authority to receive information from any federal or non-federal entity in support of the mission responsibilities of the Department. Section 201 of the Homeland Security Act authorizes the Secretary "[t]o access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies (including law enforcement agencies), and private sector entities, and to integrate such information, in support of the mission responsibilities of the Department." 6 U.S.C. 121(d)(1); see also 6 U.S.C. 121(d)(12). The following authorities also permit DHS to collect this information: Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. 3546; Presidential

Policy Directive (PPD)–21, Critical Infrastructure Identification, Prioritization, and Protection (2003); and National Security Presidential Directive (NSPD)–54/HSPD–23, Cybersecurity Policy (2009).

Note: Any information received from the public in support of the NICCS Cybersecurity Training and Education Catalog is completely voluntary. Organizations and individuals who do not provide information can still utilize the NICCS website and Catalog without restriction or penalty. An organization or individual who wants their information removed from the NICCS website and/or Cybersecurity Training and Education Catalog can email the NICCS Supervisory Office. There are no requirements for a provider to fill out a specific form for their information to be removed; standard email requests will be honored.

The Office of Management and Budget is particularly interested in comments which:

1. Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

2. Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;

3. Enhance the quality, utility, and clarity of the information to be collected; and

4. Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, *e.g.,* permitting electronic submissions of responses.

Analysis

CISA OCLO seeks to utilize four separate forms in order to collect the requested information from organizations and academic institutions. CISA OCLO will use the NICCS Cybersecurity Training Course Form and the NICCS Cybersecurity Certification Form to collect information via a publicly accessible website called the National Initiative for Cybersecurity Careers and Studies (NICCS) website (*https://niccs.cisa.gov*). Collected information from these two forms will be included in the Cybersecurity Training and Education Catalog that is hosted on the NICCS website. Requested information categories in these forms include the training providers name,

course title, course description, course length, course modality, among other course information useful for users.

The NICCS Supervisory Office will use information collected from the NICCS Vendor Vetting Form to primarily manage communications with the training/workforce development providers; this collected information will not be shared with the public and is intended for internal use only. Additionally, this information will be used to validate training providers before uploading their training and certification information to the Training Catalog. Requested information in the NICCS Vendor Vetting form include vendor name, address, points of contact and a few multiple-choice questions to ensure they are a legitimate business.

The NICCS Supervisory Office will use information collected from the NICCS Mapping Tool Form to provide an end user with information of how their position or job title aligns to the new Cybersecurity Framework 1.1. This collection of inputs and output (in the form of a report) will be savable by the end user on their computer to be uploaded at a later time for further use if required. This collected information will not be shared with the public and is intended for internal use only. Requested information in the NICCS Mapping form include: Selecting various work roles (based on the NICE Framework), selecting tasks required for that work role, and including job description details.

The information will be collected via fully electronic web forms or partially electronic via email. Collection will be coordinated between the public and NICCS via email.

The following forms are fully electronic:
- NICCS Vendor Vetting Web Form
- NICCS Cybersecurity Training Course Web Form
- NICCS Mapping Tool Web Form

The following forms are partially electronic:

- NICCS Certification Course Form

All information collected from the NICCS Cybersecurity Training Course Web Form, and the NICCS Certification Course Form will be stored in the public accessible NICCS Cybersecurity Training and Education Catalog (*https://niccs.cisa.gov/education-training/catalog*).

The NICCS Supervisory Office will electronically store information collected via the NICCS Vendor Vetting Form. This information collected will not be publicly accessible. Information collected for the NICCS Certification Course Form is collected via email in a

CSV format, and then compiled by the NICCS staff for upload to the NICCS Education and Training Catalog.

Information collected by the NICCS Mapping Tool is not being stored by NICCS. The information collected will not be publicly accessible. Users have the option of saving their input and results to be used at a later time, and the information would only be stored on the user's device.

Analysis

Agency: Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS).

Title: National Initiative for Cybersecurity Careers and Studies Cybersecurity Education and Training Catalog Collection.

OMB Number: 1670–0030.
Frequency: Annually.
Affected Public: General Public.
Number of Respondents: 500.
Estimated Time per Respondent: 0.775 Hours.
Total Burden Hours: 387.5.
Annualized Respondent Cost: $24,482.
Total Annualized Respondent Out-of-Pocket Cost: $0.
Total Annualized Government Cost: $161,490.

Robert J. Costello,

Chief Information Officer, Department of Homeland Security, Cybersecurity and Infrastructure Security Agency.

[FR Doc. 2024–13471 Filed 6–18–24; 8:45 am]

BILLING CODE 9111–LF–P

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Reinstatement of Agency Information Collection Activity Under OMB Review: Aircraft Operator Security

AGENCY: Transportation Security Administration, DHS.

ACTION: 30-Day notice.

SUMMARY: This notice announces that the Transportation Security Administration (TSA) has forwarded the Information Collection Request (ICR), Office of Management and Budget (OMB) control number 1652–0003, abstracted below, to OMB to review and approve the reinstatement of this previously approved collection under the Paperwork Reduction Act (PRA). The ICR describes the nature of the information collection and its expected burden. Aircraft operators must provide certain information to TSA and adopt

and implement a TSA-approved security program. These programs require aircraft operators to maintain and update records to ensure compliance with security provisions set forth in 49 CFR part 1544.

DATES: Send your comments by July 22, 2024. A comment to OMB is most effective if OMB receives it within 30 days of publication.

ADDRESSES: Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to *www.reginfo.gov/public/do/ PRAMain.* Find this particular information collection by selecting ''Currently under Review—Open for Public Comments'' and by using the find function.

FOR FURTHER INFORMATION CONTACT: Nicole Raymond, TSA PRA Officer, Information Technology (IT), TSA–11, Transportation Security Administration, 6595 Springfield Center Drive, Springfield, VA 20598–6011; telephone (571) 227–2526; email *TSAPRA@ tsa.dhs.gov.*

SUPPLEMENTARY INFORMATION: TSA published a **Federal Register** notice, with a 60-day comment period soliciting comments, of the following collection of information on July 20, 2023, 88 FR 46805.

Comments Invited

In accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*), an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid OMB control number. The ICR documentation will be available at *https://www.reginfo.gov* upon its submission to OMB. Therefore, in preparation for OMB review and approval of the following information collection, TSA is soliciting comments to—

(1) Evaluate whether the proposed information requirement is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

(2) Evaluate the accuracy of the agency's estimate of the burden;

(3) Enhance the quality, utility, and clarity of the information to be collected; and

(4) Minimize the burden of the collection of information on those who are to respond, including using appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology.

Information Collection Requirement

Title: Aircraft Operator Security, 49 CFR part 1544.

Type of Request: Reinstatement of a previously approved collection.

OMB Control Number: 1652–0003.
Forms(s): N/A.
Affected Public: Aircraft Operators.
Abstract: TSA's aircraft operator security standards regulations, codified at 49 CFR part 1544, require aircraft operators to adopt, maintain, update, and comply with TSA-approved comprehensive security programs to ensure the safety of persons and property traveling on their flights against acts of criminal violence and air piracy, and the introduction of explosives, incendiaries, or weapons aboard an aircraft. In addition, part 1544 requires the affected aircraft operators to submit information on aircraft operators' flight crews and other employees, passengers, and cargo. The information collection includes information regarding security program, amendments, fingerprint based criminal history records check (CHRC) applications; recordkeeping requirements for security program, CHRCs, and training. These programs and related records are subject to TSA inspection.

Number of Respondents: 634.
Estimated Annual Burden Hours: An estimated 542,632 hours annually.

Dated: June 14, 2024.

Nicole Raymond,

TSA Paperwork Reduction Act Officer, Information Technology.

[FR Doc. 2024–13483 Filed 6–18–24; 8:45 am]

BILLING CODE 9110–05–P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

[Docket No. FR–7080–N–27]

30-Day Notice of Proposed Information Collection: Submission Requirements for the Capital Advance Program Section 202/811, OMB Control No.: 2502–0470

AGENCY: Office of Policy Development and Research, Chief Data Officer, HUD.

ACTION: Notice.

SUMMARY: HUD is seeking approval from the Office of Management and Budget (OMB) for the information collection described below. In accordance with the Paperwork Reduction Act, HUD is requesting comment from all interested parties on the proposed collection of information. The purpose of this notice is to allow for an additional 30 days of public comment.