information describing the collection. There is one ICR for each collection.

S&T invites comments on whether this icr should be granted based on the collection being necessary for the proper performance of departmental functions. In particular, S&T would appreciate comments addressing: (1) the practical utility of the collection; (2) the accuracy of the estimated burden of the collection; (3) ways to enhance the quality, utility, and clarity of information subject to the collection; and (4) ways to minimize the burden of the collection on respondents, including the use of automated collection techniques or other forms of information technology. Burden means the total time, effort, or financial resources expended by persons to generate, maintain, retain, disclose or provide information to or for a federal agency.

Analysis

Agency: DHS/Science and Technology.

Title: Science and Technology Collection of Qualitative Feedback.

OMB Number: 1640–0018.

Frequency: Once.

Affected Public: Individuals.

Number of Respondents: An estimated 400,000 respondents will take the survey.

Estimated Time per Respondent: 30 minutes.

Total Burden Hours: 200,000 hours.

Total Burden Cost (capital/startup): There is no cost to participants other than their time.

Total Burden Cost (operating/maintaining): There is no cost to participants other than their time.

Gregg Piermarini,

Chief Information Officer, Science and Technology Directorate, Department of Homeland Security.

[FR Doc. 2023–24916 Filed 11–9–23; 8:45 am]

BILLING CODE 9110–9F–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2023–0006]

Notice of Cybersecurity and Infrastructure Security Agency Cybersecurity Advisory Committee Meeting

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

ACTION: Notice of Federal Advisory Committee Act (FACA) meeting; request for comments.

SUMMARY: CISA is publishing this notice to announce the CISA Cybersecurity Advisory Committee Quarterly Meeting will meet in person on Tuesday, December 5, 2023. This meeting will be partially closed to the public.

DATES:

Meeting Registration: Registration to attend the meeting is required and must be received no later than 5 p.m. Pacific standard time (PST) on Sunday, December 3, 2023.

Speaker Registration: Registration to speak during the meeting's public comment period must be received no later than 5 p.m. PST on December 3, 2023.

Written Comments: Written comments must be received no later than 5 p.m. PST on December 3, 2023.

Meeting Date: The CISA Cybersecurity Advisory Committee will meet in-person at Viasat, located at 2501 Gateway Rd., Carlsbad, CA 92009 on Tuesday, December 5, 2023, from 8:30 a.m. to 3 p.m. PST. The meeting may close early if the Committee has completed its business.

ADDRESSES: The CISA Cybersecurity Advisory Committee's meeting will be open to limited members of the public, per 41 CFR 102–3.150 and will be held in person at 2501 Gateway Rd., Carlsbad, CA 92009. A limited number of members of the public may participate in person or the public can participate via teleconference. To register to attend in person or request access to the conference call bridge, please email *CISA_CybersecurityAdvisoryCommittee@cisa.dhs.gov* by 5 p.m. PST December 3, 2023. The CISA Cybersecurity Advisory Committee is committed to ensuring all participants have equal access regardless of disability status. If you require a reasonable accommodation due to a disability to fully participate, please contact Ms. Megan Tsuyi at (202) 594–7374 as soon as possible.

Comments: Members of the public are invited to provide comment on issues that will be considered by the committee as listed in the **SUPPLEMENTARY INFORMATION** section below. Associated materials that may be discussed during the meeting will be made available for review at *https://www.cisa.gov/cisa-cybersecurity-advisory-committee-meeting-resources* by December 3, 2023. Comments should be submitted by 5 p.m. PST on November 30, 2023 and must be identified by Docket Number CISA–2023–0006. Comments may be submitted by one of the following methods:

- *Federal eRulemaking Portal: www.regulations.gov.* Please follow the instructions for submitting written comments.
- *Email: CISA_CybersecurityAdvisoryCommittee@cisa.dhs.gov.* Include the Docket Number CISA–2023–0006 in the subject line of the email.

Instructions: All submissions received must include the words ''Cybersecurity and Infrastructure Security Agency'' and the Docket Number for this action. Comments received will be posted without alteration to *www.regulations.gov,* including any personal information provided. You may wish to review the Privacy & Security notice available via a link on the homepage of *www.regulations.gov.*

Docket: For access to the docket and comments received by the CISA Cybersecurity Advisory Committee, please go to *www.regulations.gov* and enter docket number CISA–2023–0006.

A public comment period is scheduled to be held during the meeting from 1:35 p.m. to 1:45 p.m. PST. Speakers who wish to participate in the public comment period must email *CISA_CybersecurityAdvisoryCommittee@cisa.dhs.gov* to register. Speakers should limit their comments to 3 minutes and will speak in order of registration. Please note that the public comment period may end before the time indicated, depending on the number of speakers who register to participate.

FOR FURTHER INFORMATION CONTACT: Megan Tsuyi, 202–594–7374, *CISA_CybersecurityAdvisoryCommittee@cisa.dhs.gov.*

SUPPLEMENTARY INFORMATION: The CISA Cybersecurity Advisory Committee was established under the National Defense Authorization Act for Fiscal Year 2021, Public Law 116–283. Notice of this meeting is given under FACA, 5 U.S.C. ch. 10 (Pub. L. 92–463). The CISA Cybersecurity Advisory Committee advises the CISA Director on matters related to the development, refinement, and implementation of policies, programs, planning, and training pertaining to the cybersecurity mission of the Agency.

Agenda: The CISA Cybersecurity Advisory Committee will hold an in-person meeting on Tuesday, December 5, 2023, to discuss current CISA Cybersecurity Advisory Committee activities. The open session will include: (1) a period for public comment, (2) subcommittee updates, deliberation, and vote, (3) a discussion on the CSAC's strategic focus for 2024, and (4) an overview of the CSAC's annual report.

The Committee will also meet in a closed session from 8:30 a.m. to 1 p.m. PST to participate in an operational discussion that will address areas of

critical cybersecurity vulnerabilities and priorities for CISA. Government officials will share sensitive information with CSAC members on initiatives and future security requirements for assessing cyber risks to critical infrastructure.

Basis for Closure: In accordance with section 10(d) of FACA and 5 U.S.C. 552b(c)(9)(B), *The Government in the Sunshine Act,* it has been determined that certain agenda items require closure, as the premature disclosure of the information that will be discussed would be likely to significantly frustrate implementation of proposed agency actions.

This agenda item addresses areas of CISA's operations that include critical cybersecurity vulnerabilities and priorities for CISA. Government officials will share sensitive information with CSAC members on initiatives and future security requirements for assessing cyber risks to critical infrastructure.

As the premature disclosure of the information that will be discussed would be likely to significantly frustrate implementation of proposed agency action, this portion of the meeting is required to be closed pursuant to section 10(d) of FACA and 5 U.S.C. 552b(c)(9)(B).

Megan M. Tsuyi,

Designated Federal Officer, CISA Cybersecurity Advisory Committee, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security.

[FR Doc. 2023–24929 Filed 11–9–23; 8:45 am]

BILLING CODE 9110–9P–P

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Intent To Request Revision of Agency Information Collection Activity Under OMB Review: Baseline Assessment for Security Enhancement (BASE) Program

AGENCY: Transportation Security Administration, DHS.

ACTION: 60-Day notice.

SUMMARY: The Transportation Security Administration (TSA) invites public comment on one currently approved Information Collection Request (ICR), Office of Management and Budget (OMB) control number 1652–0062 abstracted below that we will submit to OMB for a revision in compliance with the Paperwork Reduction Act (PRA). The ICR covers the assessment of current security practices in public transportation passenger rail (PTPR) and highway and motor carrier (HWY) industries by way of the Baseline Assessment for Security Enhancement (BASE) program, which encompasses site visits and interviews, and is part of the larger domain awareness, prevention, and protection program that supports the mission of TSA and the Department of Homeland Security (DHS). This voluntary collection allows TSA to conduct transportation security-related assessments during site visits with security and operating officials of certain surface transportation modes.

DATES: Send your comments by January 12, 2024.

ADDRESSES: Comments may be emailed to *TSAPRA@tsa.dhs.gov* or delivered to the TSA PRA Officer, Information Technology, TSA 11, Transportation Security Administration, 6595 Springfield Center Drive, Springfield, VA 20598–6011.

FOR FURTHER INFORMATION CONTACT: Nicole Raymond at the above address, or by telephone (571) 227–2526.

SUPPLEMENTARY INFORMATION:

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

OMB Control Number 1652–0062; Baseline Assessment for Security Enhancement (BASE) Program. Under the Aviation and Transportation Security Act and delegated authority from the Secretary of Homeland Security, TSA has broad responsibility and authority for ''security in all modes of transportation including security responsibilities over modes of transportation that are exercised by the Department of Transportation.'' [1] TSA is also required to ''assess the security of each surface transportation mode and evaluate the effectiveness and efficiency of current Federal Government surface transportation security initiatives.'' [2]

TSA developed the BASE program in 2007, in an effort to engage with surface transportation entities to establish a ''baseline'' of security and emergency response operations. This program was initially created for PTPR (including rail and bus operations). Based on the success of the program, TSA developed the HWY BASE program in 2012. The HWY BASE applies to trucking, school bus contractors, school districts, and over-the-road motor coaches. This voluntary program enables TSA to collect and evaluate physical and operational preparedness information and critical assets and key point-of-contact lists. TSA also reviews emergency procedures and domain awareness training and provides an opportunity to share industry best practices.

The BASE program provides TSA with current information on adopted security-practices within the PTPR and HWY modes of the surface transportation sector. The information collected also allows TSA to dynamically adapt programs to the changing threat with an understanding of the improvements surface transportation entities make in their security posture. Additionally, the relationships these face-to-face contacts foster are critical to TSA's ability to reach out to the surface transportation entities participating in the BASE program.

In carrying out the voluntary BASE program, TSA's Transportation Security Inspectors-Surface (TSIs–S) conduct BASE reviews during site visits with security and operating officials of PTPR

[1] *See* Public Law 107–71, (115 Stat. 597, Nov. 19, 2001), codified at 49 U.S.C. 114(d). The TSA Administrator's current authorities under the Aviation and Transportation Security Act have been delegated to him by the Secretary of Homeland Security. Section 403(2) of the Homeland Security Act (HSA) of 2002, Public Law 107–296, (116 Stat. 2315, Nov. 25, 2002), transferred all functions of TSA, including those of the Secretary of Transportation and the Under Secretary of Transportation of Security related to TSA, to the Secretary of Homeland Security. Pursuant to DHS Delegation Number 7060.2, the Secretary delegated to the Assistant Secretary (now referred to as the Administrator of TSA), subject to the Secretary's guidance and control, the authority vested in the Secretary with respect to TSA, including that in sec. 403(2) of the HSA.

[2] *See* Executive Order 13416 of Dec. 5, 2006 (Strengthening Surface Transportation Security) at sec. 3(a).