responding to a proposed suspension from the test, the participant should address the facts or conduct charges contained in the notice and state how compliance has been or will be achieved.

If no timely response is received, the proposed suspension becomes the final decision of CBP as of the date that the response period expires. If a timely response is received, the Director, CED, will issue a final decision in writing, by email, on the proposed suspension within thirty (30) business days after receiving the response from the test participant, unless such time is extended for good cause. Suspension of a test participant's privileges will take place either when the proposal becomes final, if the participant fails to timely respond to the proposed suspension, or upon the final adverse decision issued by the Director after the participant has responded. The decision to suspend a surety from participation in the test may be appealed to the Executive Assistant Commissioner, Office of Trade, within fifteen (15) days of the date of CBP's final adverse decision, by submitting an email entitled, ''Appeal—EIDS Suspension'', to the Executive Assistant Commissioner, CBP, at *EIDS@cbp.dhs.gov,* and attaching a copy of the decision being appealed. The surety filing the appeal must set forth its reasons for appealing the Director, CED's final decision. The Executive Assistant Commissioner's decision is not subject to further review.

V. Test Evaluation Criteria

All interested parties are invited to comment on any aspect of this test at any time. To ensure adequate feedback, participants are required to take part in evaluation of the test. CBP needs comments and feedback on all aspects of this test, including the design, conduct and implementation of the test, to determine whether to modify, alter, expand, limit, continue, end, or implement this program. Comments should be submitted via email to *EIDS@cbp.dhs.gov,* with the subject line reading ''Comments/Questions on EIDS Test.''

The EIDS test is intended to evaluate the feasibility of sending via email the CBP Form 5955A to sureties. CBP will evaluate whether the test: (1) improves CBP's ability to quickly, safely and securely transmit the CBP Form 5955A to the surety; (2) enables sureties to better track claims posted against their bonds; (3) enables sureties to timely respond to claims; (4) obtains buy-in from stakeholders (including FPF Officers, sureties, and trade associations); and, (5) facilitates legal compliance with the laws, regulations, policies, and instructions enforced by CBP. At the conclusion of the test, an evaluation will be conducted to assess the efficacy of the information received throughout the course of the test. The final results of the evaluation will be published in the **Federal Register** and the *Customs Bulletin* as required by section 101.9(b)(2) of the CBP regulations (19 CFR 101.9(b)(2)).

Should the EIDS test be successful and ultimately be codified under the CBP regulations, CBP anticipates that this data would greatly enhance CBP's penalty and liquidated damages notification process, reduce risk, and improve compliance operations. CBP would also anticipate greater visibility into bond claims, which will support better decision-making during and after the case resolution process.

VI. Confidentiality

Data submitted and entered into SEACATS may include confidential commercial or financial information which may be protected under the Trade Secrets Act (18 U.S.C. 1905), the Freedom of Information Act (5 U.S.C. 552), and the Privacy Act (5 U.S.C. 552a). The electronic notice of demand on surety will only contain that information that is currently provided on the paper CBP Form 5955A. However, as stated in previous test notices, participation in this test or any of the previous NCAP tests is not confidential and, therefore, upon receipt of a written Freedom of Information Act request, the name(s) of an approved participant(s) will be disclosed by CBP in accordance with 5 U.S.C. 552.

John P. Leonard,

Acting Executive Assistant Commissioner, Office of Trade.

[FR Doc. 2023–24907 Filed 11–9–23; 8:45 am]

BILLING CODE 9111–14–P

DEPARTMENT OF HOMELAND SECURITY

Agency Information Collection Activities: Science and Technology Collection of Qualitative Feedback

AGENCY: S&T, DHS.

ACTION: 30-Day notice and request for comments; Science and Technology Collection of Qualitative Feedback, DHS–2023–0039.

SUMMARY: The Department of Homeland Security, S&T/CIO, DHS will submit the following information collection request (ICR) to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995. DHS previously published this information collection request (ICR) in the **Federal Register** on November 1, 2023, for a 60-day public comment period. One comment was received by DHS. The purpose of this notice is to allow additional 30-days for public comments.

DATES: Comments are encouraged and will be accepted until December 13, 2023. This process is conducted in accordance with 5 CFR 1320.10.

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 30-day Review—Open for Public Comments'' or by using the search function.

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.

FOR FURTHER INFORMATION CONTACT: If additional information is required contact: DHS/S&T/OES/CIO/Business Management Office: Heather Erhuanga, *Heather.Erhuanga@hq.dhs.gov* or 202–941–8731 (not a toll-free number).

SUPPLEMENTARY INFORMATION: This notice relies on the authority of the Paperwork Reduction Act of 1995; 44 U.S.C. 3501 *et seq.,* chapter 35, as amended. An ICR is an application to OIRA seeking the approval, extension, or renewal of a S&T collection of information (collection). The ICR contains information describing the collection's purpose, the collection's likely burden on the affected public, an explanation of the necessity of the collection, and other important

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