submitted to HHS, for which HRSA was deemed a custodian of the requested data given HRSA's oversight of the Provider Relief Fund. HRSA has reason to believe that information in the records could reasonably be considered confidential commercial information and exempt from disclosure under FOIA Exemption 4. FOIA Exemption 4 allows agencies to withhold trade secrets and commercial or financial information obtained from a person (business entities including hospitals are considered people under the FOIA) and is privileged or confidential. Both the Executive Order and HHS FOIA regulations permit agencies to notify a voluminous number of submitters by posting or publishing a notice in a place where the submitters are reasonably likely to become aware of it. See Executive Order 12600 or 45 CFR 5.42(a)(1). This notice satisfies this requirement. Additionally, HRSA will send predisclosure notices directly to hospitals for whom HRSA has contact information.

HRSA determined that, for those hospitals that did not receive a payment in the first round of the COVID–19 High Impact Area Distribution, the following responsive data could reasonably be considered confidential commercial information and exempt from disclosure under FOIA Exemption 4:

(1) number of COVID–19 admissions; and

(2) intensive care unit hospital beds for each facility (and associated Centers for Medicare & Medicaid Services' Certification Number (CCN))

HRSA must analyze the releasability of the data prior to making a release decision. Because organizations submitted data to HHS that was identified in the FOIA request, HRSA is notifying submitters of their full rights through this predisclosure notice. HHS's FOIA regulations provide affected entities with 10 working days from the date of this notice to object to disclosure of part or all of the information contained in these records.

A person who submits records to the government may designate part or all of the information in such records that they may consider exempt from disclosure under Exemption 4 of the FOIA. The designation must be in writing. See 45 CFR 5.41.

So that HRSA can determine how providers actually and customarily treat the disclosure of these data, please respond to the following questions with respect to the (1) number of COVID–19 admissions and (2) intensive care unit hospital beds for each facility (and associated CCN) and send your organization's response to *hotspotpdn@hrsa.gov* in the timeframe referenced in the dates section of this notice. Please include your organization's CCN and facility name in your response to ensure that it is attributed correctly.

(1) Do you customarily keep the requested information private or closely held? What steps have you taken to protect the confidentiality of the requested data, and to whom has it been disclosed?

(2) What facts support your belief that this information is commercial or financial in nature?

(3) Did the government provide you with an express or implied assurance of confidentiality when you shared the information with the government? If so, please explain.

(4) Were there express or implied indications at the time the information was submitted that the government would publicly disclose the information? If so, please explain.

(5) How would disclosure of this information harm an interest protected by Exemption 4 (such as by causing foreseeable harm to your economic or business interests)?

Intended Effects of the Action

In the event that a submitter fails to respond to the notice within the time specified, it will be considered to have no objection to disclosure of the information. Submitted objections will be given the appropriate consideration; however, responses are not an agreement that HRSA will withhold the information. If HRSA decides to release the information over objection, HRSA will inform submitters, in writing, along with HRSA's reasons for the decision to release. HRSA will include with such notice a description of the information to be disclosed or copies of the records as HRSA intends to release them. HRSA will also provide submitters with a specific date that HRSA intends to disclose the records, which must be at least 5 working days after the date of the intent to release notice. HRSA will not consider any information received after the date of a disclosure decision.

Maria G. Button,

Director, Executive Secretariat.

[FR Doc. 2023–04858 Filed 3–8–23; 8:45 am]

BILLING CODE 4165–15–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

Center For Scientific Review; Amended Notice of Meeting

Notice is hereby given of a change in the meeting of the Center for Scientific Review Special Emphasis Panel Member Conflict: Epidemiology and Population Health, March 28, 2023, 12:00 p.m. to March 28, 2023, 08:00 p.m., National Institutes of Health, Rockledge II, 6701 Rockledge Drive, Bethesda, MD 20892 which was published in the **Federal Register** on February 27, 2023, 88 FR 12388 Doc. 2023–03969.

This meeting is being amended to change the meeting start time from 12:00 p.m. to 11:00 a.m. The meeting is closed to the public.

Dated: March 3, 2023.

David W Freeman,

Program Analyst, Office of Federal Advisory Committee Policy.

[FR Doc. 2023–04798 Filed 3–8–23; 8:45 am]

BILLING CODE 4140–01–P

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Extension of Agency Information Collection Activity Under OMB Review: Cybersecurity Measures for Surface Modes

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 1652–0074, abstracted below, to OMB for an extension of the currently approved collection under the Paperwork Reduction Act (PRA). The ICR describes the nature of the information collection and its expected burden. Specifically, the collection involves the submission of data concerning the designation of a Cybersecurity Coordinator; the reporting of cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency; the development of a cybersecurity contingency/recovery plan to address cybersecurity gaps; and the completion of a cybersecurity assessment.

DATES: Send your comments by April 10, 2023. 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: Christina A. Walsh, TSA PRA Officer, Information Technology, TSA–11, Transportation Security Administration, 6595 Springfield Center Drive, Springfield, VA 20598–6011; telephone (571) 227–2062; 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 November 14, 2022, 87 FR 68185.

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: Cybersecurity Measures for Surface Modes.

Type of Request: Extension.

OMB Control Number: 1652–0074.

Form(s): TSA Optional Forms. TSA Surface Cybersecurity Vulnerability Assessment Form.

Affected Public: Owner/Operators with operations identified in 49 CFR part 1580 (Freight Rail), 49 CFR part 1582 (Mass Transit and Passenger Rail), and 49 CFR part 1584 (Over-the-Road Bus).

Abstract: Under the authorities of 49 U.S.C. 114, TSA may take immediate action to impose measures to protect transportation security without providing notice or an opportunity for comment.[1] On December 17, 2021, TSA issued the Security Directive (SD) 1580–21–01 series, *Enhancing Rail Cybersecurity,* and the SD 1582–21–01 series, *Enhancing Public Transportation and Passenger Railroad Cybersecurity,* which remain in effect as revised, mandating TSA-specified Owner/Operators of ''higher risk'' railroads and rail transit systems, respectively, to implement an array of cybersecurity measures to prevent disruption and degradation to their infrastructure; these security directives became effective December 31, 2021. In addition, on October 18, 2022, TSA issued the SD 1580/1582–2022–01 series, *Rail Cybersecurity Mitigation Actions and Testing,* which applies to Owner/Operators of the ''Higher Risk'' freight railroads identified in 49 CFR 1580.101 and additional TSA-designated freight and passenger railroads. This security directive, which is complementary to the requirements in the previous directives, took effect on October 24, 2022. On October 26, 2022, OMB approved TSA's request for an emergency approval, revising this information collection. *See* ICR Reference Number: 202210–1652–001. The collection covers both mandatory reporting under the security directives and collection of information voluntarily submitted under Information Circular (IC) 2021–01, *Enhancing Surface Transportation Cybersecurity,* which recommended voluntary implementation of actions and reporting by Owner/Operators not covered by the security directives. The OMB approval allowed for the additional institution of mandatory reporting requirements and collection of information voluntarily submitted. *See* ICR Reference Number: 202111–1652–003. TSA is now seeking renewal of this information collection for the maximum three-year approval period.

The cybersecurity threats to surface transportation infrastructure that necessitate these collections are within TSA's statutory 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.'' *See* 49 U.S.C. 114(d).

The requirements in the security directives and the recommendations in the IC allow TSA to execute its security responsibilities within the surface transportation industry, through awareness of potential security incidents and suspicious activities.

A. SD 1580/82–2022–01 Series

This security directive series includes the following information collection:

1. Submission of a Cybersecurity Implementation Plan to TSA for approval that identifies how the Owner/Operator will meet the required security outcomes in the SD;

2. Submission of an Annual Audit Plan for the required Cybersecurity Assessment Program; and

3. Documentation provided to TSA upon request as necessary to establish compliance.

B. SD 1580–21–01, SD 1582–21–01, and IC 2021–01 Series

These security directives and the IC remain in effect and include the following information collection requirements for the security directives and voluntary collection under the IC:

1. Provide contact information for a designated Cybersecurity Coordinator to TSA.

2. Report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency.

3. Submit a cybersecurity incident response plan to TSA.

4. Complete and submit a cybersecurity vulnerability assessment using a form provided by TSA.

TSA will use the collection of information to ensure compliance with TSA's cybersecurity measures required by the security directives and the recommendations under the IC.

Owner/Operators can complete and submit the required information via email or other electronic options provided by TSA. Documentation of compliance must be provided upon request. As the measures in the IC are voluntary, the IC does not require Owner/Operators to report on their compliance.

Portions of the responses that are deemed Sensitive Security Information

[1] TSA issues security directives for surface transportation operators under the statutory authority of 49 U.S.C. 114(l)(2)(A). This provision, from section 101 of the Aviation and Transportation Security Act (ATSA), Public Law 107–71 (115 Stat. 597; Nov. 19, 2001), states: ''Notwithstanding any other provision of law or executive order (including an executive order requiring a cost-benefit analysis), if the Administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security, the Administrator shall issue the regulation or security directive without providing notice or an opportunity for comment and without prior approval of the Secretary.''

(SSI) are protected in accordance with procedures meeting the transmission, handling, and storage requirements of SSI set forth in 49 CFR part 1520.[2]

Number of Respondents: 781.

Estimated Annual Burden Hours: An estimated 96,163 hours annually.

Dated: March 6, 2023.

Christina A. Walsh,

TSA Paperwork Reduction Act Officer, Information Technology.

[FR Doc. 2023–04859 Filed 3–8–23; 8:45 am]

BILLING CODE 9110–05–P

DEPARTMENT OF HOMELAND SECURITY

U.S. Citizenship and Immigration Services

[OMB Control Number 1615–0133]

Agency Information Collection Activities; Revision of a Currently Approved Collection: Request for Reduced Fee

AGENCY: U.S. Citizenship and Immigration Services, Department of Homeland Security.

ACTION: 60-Day notice.

SUMMARY: The Department of Homeland Security (DHS), U.S. Citizenship and Immigration Services (USCIS) invites the general public and other Federal agencies to comment upon this proposed revision of a currently approved collection of information. In accordance with the Paperwork Reduction Act (PRA) of 1995, the information collection notice is published in the **Federal Register** to obtain comments regarding the nature of the information collection, the categories of respondents, the estimated burden (*i.e.,* the time, effort, and resources used by the respondents to respond), the estimated cost to the respondent, and the actual information collection instruments.

DATES: Comments are encouraged and will be accepted for 60 days until May 8, 2023.

ADDRESSES: All submissions received must include the OMB Control Number 1615–0133 in the body of the letter, the agency name and Docket ID USCIS–2018–0002. Submit comments via the Federal eRulemaking Portal website at *https://www.regulations.gov* under e-Docket ID number USCIS–2018–0002.

FOR FURTHER INFORMATION CONTACT: USCIS, Office of Policy and Strategy, Regulatory Coordination Division, Jerry Rigdon, Acting Chief, telephone number (240) 721–3000 (This is not a toll-free number. Comments are not accepted via telephone message). Please note contact information provided here is solely for questions regarding this notice. It is not for individual case status inquiries. Applicants seeking information about the status of their individual cases can check Case Status Online, available at the USCIS website at *https://www.uscis.gov,* or call the USCIS Contact Center at 800–375–5283 (TTY 800–767–1833).

SUPPLEMENTARY INFORMATION:

Comments

You may access the information collection instrument with instructions or additional information by visiting the Federal eRulemaking Portal site at: *https://www.regulations.gov* and entering USCIS–2018–0002 in the search box. All submissions will be posted, without change, to the Federal eRulemaking Portal at *https://www.regulations.gov,* and will include any personal information you provide. Therefore, submitting this information makes it public. You may wish to consider limiting the amount of personal information that you provide in any voluntary submission you make to DHS. DHS may withhold information provided in comments from public viewing that it determines may impact the privacy of an individual or is offensive. For additional information, please read the Privacy Act notice that is available via the link in the footer of *https://www.regulations.gov.*

Written comments and suggestions from the public and affected agencies should address one or more of the following four points:

(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 submission of responses.

Overview of This Information Collection

(1) *Type of Information Collection:* Revision of a currently approved collection.

(2) *Title of the Form/Collection:* Request for Reduced Fee.

(3) *Agency form number, if any, and the applicable component of the DHS sponsoring the collection:* I–942; USCIS.

(4) *Affected public who will be asked or required to respond, as well as a brief abstract: Primary:* Individuals or households. USCIS uses the data collected on this form to verify that the applicant is eligible for a reduced fee for the immigration benefit being requested.

(5) *An estimate of the total number of respondents and the amount of time estimated for an average respondent to respond:* The estimated total number of respondents for the information collection I–942 is 4,491 and the estimated hour burden per response is 0.67 hour.

(6) *An estimate of the total public burden (in hours) associated with the collection:* The total estimated annual hour burden associated with this collection is 3,009 hours.

(7) *An estimate of the total public burden (in cost) associated with the collection:* The estimated total annual cost burden associated with this collection of information is $19,087.

Dated: March 1, 2023.

Jerry L. Rigdon,

Acting Branch Chief, Regulatory Coordination Division, Office of Policy and Strategy, U.S. Citizenship and Immigration Services, Department of Homeland Security.

[FR Doc. 2023–04791 Filed 3–8–23; 8:45 am]

BILLING CODE 9111–97–P

[2] In addition, all data in TSA systems are statutorily required to comply with the Federal Information Security Modernization Act 2014 (FISMA) following the National Institute of Standards and Technology Special Publication 800.37 REV2 or Risk Management Framework, and other federal information security requirements including Federal Information Processing Standards 199 and Executive Order 14028. All systems, networks, servers, clouds and endpoints under the FISMA boundary are hardened to meet the Department of Defense Security Technical Implementation Guidelines, as well as DHS Policy (4300.A) and TSA policy (TSA IA Handbook).