suggestion or recommendation. You should provide personal contact information so that we can contact you if we have questions regarding your comments; but please note that all comments will be posted to the online docket without change and that any personal information you include can be searchable online. For more about privacy and the docket, visit *http://www.regulations.gov/privacyNotice.* We do accept anonymous comments.

We encourage you to submit comments through the Federal Portal at *http://www.regulations.gov.* If your material cannot be submitted using *http://www.regulations.gov,* contact the Coast Guard (see **FOR FURTHER INFORMATION CONTACT**). Documents mentioned in this notice and all public comments, will be in our online docket at *http://www.regulations.gov* and can be viewed by following that website's instructions. Additionally, if you go to the online docket and sign up for email alerts, you will be notified when comments are posted.

Do not submit detailed proposals for future CRADAs to *http://www.regulations.gov.* Instead, submit them directly to the Coast Guard (see **FOR FURTHER INFORMATION CONTACT**).

**Discussion**

CRADAs are authorized under 15 U.S.C. 3710(a).[1] A CRADA promotes the transfer of technology to the private sector for commercial use, as well as specified research or development efforts that are consistent with the mission of the Federal parties to the CRADA. The Federal party or parties agree with one or more non-Federal parties to share research resources, but the Federal party does not contribute funding.

CRADAs are not procurement contracts. Care is taken to ensure that CRADAs are not used to circumvent the contracting process. CRADAs have a specific purpose and should not be confused with procurement contracts, grants, and other type of agreements.

Under the proposed CRADA, the Coast Guard's Research and Development Center (R&DC) will collaborate with one or more non-Federal participants. Together, the R&DC and the non-Federal participants will identify the capabilities, benefits, risks, and technical limitations of enhancing air surveillance radar systems.

[1] The statute confers this authority on the head of each Federal agency. The Secretary of DHS's authority is delegated to the Coast Guard and other DHS organizational elements by DHS Delegation No. 0160.1, para. II.B.34.

We anticipate that the Coast Guard's contributions under the proposed CRADA will include the following:

(1) Provide end user input on operational needs and assessment of system performance;

(2) In conjunction with the non-Federal participant(s), assist in developing the evaluation test plan to be executed to meet the objectives of the CRADA;

(3) Provide qualified UAS operators for operation of UAS, as required under the CRADA;

(4) Provide the test range, test range support, facilities, and all approvals for operation of UAS as required under the CRADA;

(5) In conjunction with the non-Federal participant(s), assist with the development of a final report or brief that documents the methodologies, findings, conclusions, and recommendations under this CRADA.

We anticipate that the non-Federal participants' contributions under the proposed CRADA will include the following:

(1) Provide the air surveillance radar system and all other equipment required to conduct the evaluation as described in the test plan developed under this CRADA;

(2) Provide operators, as required, to operate and maintain the equipment to conduct the evaluation as described in the test plan;

(3) Provide shipment and delivery of all equipment for this evaluation;

(4) Provide personnel, travel, and other associated expenses as required;

(5) Collect and analyze evaluation test plan data; and

(6) Collaboratively develop a final report documenting the methodologies, findings, conclusions, and recommendations of this CRADA work.

The Coast Guard reserves the right to select for CRADA participants all, some, or no proposals submitted for this CRADA. The Coast Guard will provide no funding for reimbursement of proposal development costs. Proposals and any other material submitted in response to this notice will not be returned. Proposals submitted are expected to be unclassified and have no more than five single-sided pages (excluding cover page, DD 1494, JF–12, etc.). The Coast Guard will select proposals at its sole discretion on the basis of:

(1) How well they communicate an understanding of, and ability to meet, the proposed CRADA's goal; and

(2) How well they address the following criteria:

(a) Technical capability to support the non-Federal party contributions described; and

(b) Resources available for supporting the non-Federal party contributions described.

Currently, RADA Technologies LLC is being considered for participation in this CRADA because they have an air surveillance radar system solution in place for providing track classification and discrimination. However, we do not wish to exclude other viable participants from this or future similar CRADAs.

The goal of this CRADA is to evaluate track classification and discrimination technology and address its ability to perform specific operations. Special consideration will be given to small business firms/consortia, and preference will be given to business units located in the U.S.

This notice is issued under the authority of 5 U.S.C. 552(a) and 15 U.S.C. 3710(a).

Dated: September 22, 2022.

**Daniel P. Keane,**

*Captain, Commanding Officer, U.S. Coast Guard Research and Development Center, USCG.*

[FR Doc. 2022–21388 Filed 9–30–22; 8:45 am]

**BILLING CODE 9110–04–P**

## DEPARTMENT OF HOMELAND SECURITY

**[Docket No. CISA–2022–0011]**

## Agency Information Collection Activities: Nationwide Cyber Security Review (NCSR) Assessment

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

**ACTION:** 60-Day notice and request for comments; existing collection, 1670–0040

**SUMMARY:** CISA will submit the following renewal information for an existing collection request (ICR) to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995.

**DATES:** Comments are encouraged and will be accepted until December 2, 2022.

**ADDRESSES:** You may submit comments, identified by docket number CISA–1670–0040, by the following method:

- *Federal eRulemaking Portal: http://www.regulations.gov.* Please follow the instructions for submitting comments.

*Instructions:* All submissions received must include the words ''Cybersecurity and Infrastructure Security Agency'' and docket number CISA–2022–0011.

Comments received will be posted without alteration at *http://www.regulations.gov,* including any personal information provided. Comments submitted in response to this notice may be made available to the public through relevant websites. For this reason, please do not include in your comments information of a confidential nature, such as sensitive personal information or proprietary information. Please note that responses to this public comment request containing any routine notice about the confidentiality of the communication will be treated as public comments that may be made available to the public notwithstanding the inclusion of the routine notice.

**FOR FURTHER INFORMATION CONTACT:** For specific questions related to collection activities, please contact Amy Nicewick at 703–203–0634 or at *CISA.CSD.JCDC_MS-ISAC@cisa.dhs.gov.*

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

**SUPPLEMENTARY INFORMATION:** The Homeland Security Act of 2002, as amended, established ''a national cybersecurity and communications integration center [''the Center,'' now constituted as CSD] . . . to carry out certain responsibilities of the Under Secretary,'' including the provision of assessments. 6 U.S.C. 659(b). The Act also directs the composition of the Center to include an entity that collaborates with State and local governments on cybersecurity risks and incidents and has entered into a voluntary information sharing relationship with the Center. 6 U.S.C. 659(d)(1)(E). The Multistate Information Sharing and Analysis Center (MS–ISAC) currently fulfills this function. CSD funds the MS–ISAC through a Cooperative Agreement and maintains a close relationship with this entity. As part of the Cooperative Agreement, CISA directs the MS–ISAC to produce the NCSR as contemplated by Congress.

Generally, CSD has authority to perform risk and vulnerability assessments for Federal and non-Federal entities, with consent and upon request. CSD performs these assessments in accordance with its authority to provide voluntary technical assistance to Federal and non-Federal entities. See 6 U.S.C. 659(c)(6). This authority is consistent with the Department's responsibility to ''[c]onduct comprehensive assessments of the vulnerabilities of the Nation's critical infrastructure in coordination with the SSAs [Sector-Specific Agencies] and in collaboration with SLTT [State, Local, Tribal, and Territorial] entities and critical infrastructure owners and operators.'' Presidential Policy Directive (PPD)–21, at 3. A private sector entity or state and local government agency also has discretion to use a self-assessment tool offered by CSD or request CSD to perform an on-site risk and vulnerability assessment. See 6 U.S.C. 659(c)(6). The NCSR is a voluntary annual self-assessment.

In its reports to the Department of Homeland Security Appropriations Act, 2010, Congress requested a Nationwide Cyber Security Review (NCSR) from the National Cyber Security Division (NCSD), the predecessor organization of the Cybersecurity Division (CSD). S. Rep. No. 111–31, at 91 (2009), H.R. Rep. No. 111–298, at 96 (2009). The House Conference Report accompanying the Department of Homeland Security Appropriations Act, 2010 ''note[d] the importance of a comprehensive effort to assess the security level of cyberspace at all levels of government'' and directed DHS to ''develop the necessary tools for all levels of government to complete a cyber network security assessment so that a full measure of gaps and capabilities can be completed in the near future.'' H.R. Rep. No. 111–298, at 96 (2009). Concurrently, in its report accompanying the Department of Homeland Security Appropriations Bill, 2010, the Senate Committee on Appropriations recommended that DHS ''report on the status of cyber security measures in place, and gaps in all 50 States and the largest urban areas.'' S. Rep. No. 111–31, at 91 (2009).

Upon submission of the first NCSR report in March 2012, Congress further clarified its expectation ''that this survey will be updated every other year so that progress may be charted and further areas of concern may be identified.'' S. Rep. No. 112–169, at 100 (2012). In each subsequent year, Congress has referenced this NCSR in its explanatory comments and recommendations accompanying the Department of Homeland Security Appropriations. Consistent with Congressional mandates, CSD developed the NCSR to measure the gaps and capabilities of cybersecurity programs within SLTT governments. Using the anonymous results of the NCSR, CISA delivers a bi-annual summary report to Congress that provides a broad picture of the current cybersecurity gaps & capabilities of SLTT governments across the nation.

The assessment allows SLTT governments to manage cybersecurity related risks through the NIST Cybersecurity Framework (CSF) which consists of best practices, standards, and guidelines. In efforts of continuously providing Congress with an accurate representation of the SLTT gaps and capabilities the NCSR question set may slightly change from year-to-year.

The NCSR is an annual voluntary self-assessment that is hosted on LogicManager, which is a technology platform that provides a foundation for managing policies, controls, risks, assessments, and deficiencies across organizational lines of business. The NCSR self-assessment runs every year from October–February. In efforts to increase participation, the deadline is sometimes extended. The target audience for the NCSR are personnel within the SLTT community who are responsible for the cybersecurity management within their organization.

Through the NCSR, CISA and MS–ISAC will examine relationships, interactions, and processes governing IT management and the ability to effectively manage operational risk. Using the anonymous results of the NCSR, CISA delivers a biannual summary report to Congress that provides a broad picture of the cybersecurity gaps and capabilities of SLTT governments across the nation. The bi-annual summary report is shared with MS–ISAC members, NCSR End Users, and Congress. The report is also available on the MS–ISAC website, *https://www.cisecurity.org/ms-isac/services/ncsr/.*

Upon submission of the NCSR self-assessment, participants will immediately receive access to several reports specific to their organization and their cybersecurity posture. Additionally, after the annual NCSR survey closes, there will be a brief NCSR End User Survey offered to everyone who completed the NSCR assessment. The survey will provide feedback on participants' experiences, such as how they heard about the NCSR, what they found or did not find useful, how they will utilize the results of their assessment, and other information about their current and future interactions with the NCSR.

The NCSR assessment requires approximately two hours for completion and is located on the LogicManager Platform. During the assessment period, participants can respond at their own pace with the ability to save their progress during each session. If additional support is needed, participants can contact the NCSR helpdesk via phone and email.

The NCSR End User survey will be fully electronic. It contains less than 30 multiple choice and fill-in-the-blank answers and takes approximately 10

minutes to complete. The feedback survey will be administered via Survey Monkey and settings will be updated to opt out of collecting participants' IP addresses. There are no recordkeeping, capital, start-up, or maintenance costs associated with this information collection. There is no submission or filing fee associated with this collection. As all forms are completed via the LogicManager platform and SurveyMonkey, there are no associated collection, printing, or mailing costs. This is a renewal for an existing information collection not a new collection. OMB is particularly interested in comments that:

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.

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.

*Title of Collection:* Nationwide Cyber Security Review Assessment.

*OMB Control Number:* CISA–1670–0040.

*Frequency:* Annually.

*Affected Public:* State, Local, Tribal, and Territorial entities.

*Number of Respondents for NCSR Assessment:* 3,112.

*Estimated Time per Respondent Respondents for NCSR Assessment:* 2 hours.

*Number of Respondents for NCSR End User Survey:* 215.

*Estimated Time per Respondent for NCSR End User Survey:* 0.17 hours (10 minutes).

*Total Burden Hours:* 6,260.

*Total Burden Cost (Capital/Startup):* $0.

*Total Recordkeeping Burden:* $0.

*Total Burden Cost (Operating/Maintaining):* $0

*Total Hourly Burden Cost:* $389,427.

**Robert Costello,**

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

[FR Doc. 2022–21407 Filed 9–30–22; 8:45 am]

**BILLING CODE 9110–9P–P**

## DEPARTMENT OF HOMELAND SECURITY

### Transportation Security Administration

### Intent To Request an Extension From OMB of One Current Public Collection of Information: Pipeline Corporate Security Review 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 1652–0056, abstracted below, that we will submit to OMB for an extension in compliance with the Paperwork Reduction Act (PRA). On July 29, 2022, OMB approved TSA's request for an emergency revision of this collection to address the ongoing cybersecurity threat to pipeline systems and associated infrastructure. TSA is now seeking to renew the collection, which expires on January 31, 2023, with incorporation of the subject of the emergency revision. The ICR describes the nature of the information collection and its expected burden. The collection allows TSA to assess the current security practices in the pipeline industry through TSA's Pipeline Corporate Security Review (PCSR) program and allows for the continued institution of mandatory cybersecurity requirements under the TSA Security Directive (SD) Pipeline 2021–02 series. The PCSR program is part of the larger domain awareness, prevention, and protection program supporting TSA's and the Department of Homeland Security's missions. The updated ICR reflects changes to collection requirements based on TSA's update to the TSA SD 2021–02 series, released on July 21, 2022.

**DATES:** Send your comments by December 2, 2022.

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

**FOR FURTHER INFORMATION CONTACT:** Christina A. Walsh at the above address, or by telephone (571) 227–2062.

**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 *http://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 1652–0056; Pipeline Corporate Security Review (PCSR) Program.* Under the Aviation and Transportation Security Act [1] 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.'' [2] TSA is specifically empowered to assess threats to transportation; [3] develop policies, strategies, and plans for dealing with

[1] Public Law 107–71 (115 Stat. 597; Nov. 19, 2001), codified at 49 U.S.C. 114.

[2] *See* 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. 2135, 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 Administrator of TSA, subject to the Secretary's guidance and control, the authority vested in the Secretary with respect to TSA, including that in section 403(2) of the HSA.

[3] 49 U.S.C. 114(f)(2).