Between CY 2019 and CY 2021, CISA has performed 5,438 of these interactions at facilities and asked questions about assets at risk. Therefore, CISA estimates 1,813 respondents [20] for the second section of the instrument by annualizing the number of interactions described above (*i.e.,* 1,813 = [5438 respondents divided by a 3-year time-period]).

Estimated Time per Respondent: In the current information collection, the estimated time per respondent is 0.17 hours (10 minutes). In this ICR, CISA maintains this estimate.

Annual Burden Hours: The annual burden estimate is 375 hours [2,252 respondents × 1 response per respondent × 0.17 hours per respondent].

Total Annual Burden Cost: CISA assumes that SSOs will be responsible for providing this information. Therefore, to estimate the total annual burden, CISA multiplied the annual burden of 375 hours by the average hourly total compensation rate of SSOs of $90.41 [21] per hour. Therefore, the total annual burden cost for this instrument is $33,931 (375 hours multiplied by $90.41 per hour).

Total Burden Cost (Capital/Startup): CISA estimates that there are no capital/startup costs for this instrument.

Total Recordkeeping Burden: There is no recordkeeping burden for this instrument.

Public Participation: *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; 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).

[20] 1,812.67 = (5438 ÷ 3).

[21] $90.4142 is the total compensation per hour, including wages and benefits.

Analysis

Title of Collection: Chemical Security Assessment Tool

OMB Control Number: 1670–0007

Instrument: Top-Screen

Frequency: ''On occasion'' and ''Other''

Affected Public: Business or other for-profit

Number of Respondents: 3,817 respondents (estimate)

Estimated Time per Respondent: 2.04 hours

Total Annual Burden Hours: 7,785 hours

Total Annual Burden Cost: $703,829

Total Annual Burden Cost (capital/startup): $0

Total Recordkeeping Burden: $0

Instrument: Security Vulnerability Assessment and Alternative Security Program submitted in lieu of a Security Vulnerability Assessment

Frequency: ''On occasion'' and ''Other''

Affected Public: Business or other for-profit

Number of Respondents: 2,328 respondents (estimate)

Estimated Time per Respondent: 1.4136 hours

Total Annual Burden Hours: 3,291 hours

Total Annual Burden Cost: $297,530

Total Annual Burden Cost (capital/startup): $0

Total Recordkeeping Burden: $0

Instrument: Site Security Plan and Alternative Security Program submitted in lieu of a Site Security Plan.

Frequency: ''On occasion'' and ''Other''

Affected Public: Business or other for-profit.

Number of Respondents: 2,328 (estimate).

Estimated Time per Respondent: 7.845 hours.

Total Annual Burden Hours: 18,262 hours.

Total Annual Burden Cost: $1,651,158.

Total Annual Burden Cost (capital/startup): $0.

Total Recordkeeping Burden: $556,040.

Instrument: CFATS Help Desk

Frequency: ''On occasion'' and ''Other''.

Affected Public: Business or other for-profit.

Number of Respondents: 12,000 respondents (estimate).

Estimated Time per Respondent: 0.1167 hours.

Total Annual Burden Hours: 1,400 hours.

Total Annual Burden Cost: $126,580.

Total Annual Burden Cost (capital/startup): $0.

Total Recordkeeping Burden: $0.

Instrument: User Registration.

Frequency: ''On occasion'' and ''Other''.

Affected Public: Business or other for-profit.

Number of Respondents: 1,000 respondents (estimate).

Estimated Time per Respondent: 2.5 hours.

Total Annual Burden Hours: 2,500 hours.

Total Annual Burden Cost: $226,035.

Total Annual Burden Cost (capital/startup): $0.

Total Recordkeeping Burden: $0.

Instrument: Identification of Facilities and Assets at Risk.

Frequency: ''On occasion'' and ''Other''.

Affected Public: Business or other for-profit.

Number of Respondents: 2,252 respondents (estimate).

Estimated Time per Respondent: 0.17 hours.

Total Annual Burden Hours: 375 hours.

Total Annual Burden Cost: $33,931.

Total Annual Burden Cost (capital/startup): $0.

Total Recordkeeping Burden: $0.

Robert Costello,

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

[FR Doc. 2022–28076 Filed 12–23–22; 8:45 am]

BILLING CODE 9110–9P–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: 30-Day notice and request for comments; Reinstatement Without Change, OMB Control Number: DHS–1670–0040.

SUMMARY: The Joint Cyber Defense Collaborative (JCDC) within Cybersecurity and Infrastructure Security Agency (CISA) 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. CISA previously published this information collection request (ICR) in the **Federal Register** on October 3, 2022 for a 60-day public comment period. Zero comments were received by CISA. The purpose of this notice is to allow additional 30-days for public comments.

DATES: Comments are encouraged and will be accepted January 26, 2023. This process is conducted in accordance with 5 CFR 1320.10.

ADDRESSES: Interested persons are invited to submit written comments on the proposed information collection to the Office of Information and Regulatory Affairs, Office of Management and Budget. Comments should be addressed to OMB Desk Officer, Department of Homeland Security and sent via electronic mail to *dhsdeskofficer@omb.eop.gov.* All submissions must include the words ''Department of Homeland Security'' and the OMB Control Number 1670–0040—replace 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. If you send an email comment, your email address will be automatically captured and included as part of the comment that is placed in the public docket and made available on the internet. 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: If additional information is required contact: The Department of Homeland Security (DHS), Amy Nicewick at 703–203–0634 or at *CISA.CSD.JCDC_MS-ISAC@cisa.dhs.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.

This is a renewal of an information 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; 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

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

Title: Nationwide Cyber Security Review Assessment.

OMB Number: CISA–1670–0040.

Frequency: Annually.

Affected Public: State, local, Tribal, and Territorial entities.

Number of Respondents: 3112.

Estimated Time Per Respondent 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): $389,427 (Capital/Startup).

Total Burden Cost (operating/maintaining): $0 (Operating/Maintaining).

Robert J. Costello,

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

[FR Doc. 2022–28142 Filed 12–23–22; 8:45 am]

BILLING CODE 9110–9P–P

DEPARTMENT OF HOMELAND SECURITY

U.S. Citizenship and Immigration Services

[OMB Control Number 1615–NEW]

Agency Information Collection Activities; New Collection

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

ACTION: 30-Day notice.

SUMMARY: The Department of Homeland Security (DHS), U.S. Citizenship and Immigration Services (USCIS) will be submitting the following information collection request to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995. The purpose of this notice is to allow an additional 30 days for public comments.

DATES: Comments are encouraged and will be accepted until January 26, 2023.

ADDRESSES: Written comments and/or suggestions regarding the item(s) contained in this notice, especially regarding the estimated public burden and associated response time, must be submitted via the Federal eRulemaking Portal website at *http://www.regulations.gov* under e-Docket ID number USCIS–2022–0010. All submissions received must include the OMB Control Number 1615–NEW in the body of the letter, the agency name and Docket ID USCIS–2022–0010.

FOR FURTHER INFORMATION CONTACT: USCIS, Office of Policy and Strategy, Regulatory Coordination Division, Samantha Deshommes, 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 *http://www.uscis.gov,* or call the USCIS Contact Center at (800) 375–5283; TTY (800) 767–1833.

SUPPLEMENTARY INFORMATION:

Background

On March 15, 2022, President Biden signed the EB–5 Reform and Integrity Act of 2022, Div. BB of the Consolidated Appropriations Act, 2022 (Pub. L. 117–103) into law, which revised INA 203(b)(5). The law immediately repealed the former Regional Center (RC) Program statute at Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Act 1993, Public Law 102–395, 106 Stat. 1828, § 610(b).

The law also reauthorized a substantially reformed EB–5 Regional Center (RC) Program which became effective on May 14, 2022. Though USCIS will continue to provide similar services for the newly reformed RC program as it did under the former RC program (such as initial designations, petition adjudications, etc.), the newly