Forms 3461 and 3461 ALT allow CBP officers to verify that the information regarding the consignee and shipment is correct and that a bond is on file with CBP.

Type of Information Collection: Paper Only Form 3461.

Estimated Number of Respondents: 28.

Estimated Number of Annual Responses per Respondent: 3.

Estimated Number of Total Annual Responses: 84.

Estimated Time per Response: 5 minutes.

Estimated Total Annual Burden Hours: 7 hours.

Type of Information Collection: Ace Cargo Release: Electronic Form 3461, 3461ALT.

Estimated Number of Respondents: 549.

Estimated Number of Annual Responses per Respondent: 274.

Estimated Number of Total Annual Responses: 150,426.

Estimated Time per Response: 5 minutes.

Estimated Total Annual Burden Hours: 12,536.

Dated: August 21, 2024.

Seth D. Renkema,

Branch Chief, Economic Impact Analysis Branch, U.S. Customs and Border Protection.

[FR Doc. 2024–19050 Filed 8–23–24; 8:45 am]

BILLING CODE 9111–14–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2024–0021]

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

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

ACTION: 60-Day notice and request for comments; revision.

SUMMARY: DHS CISA Cybersecurity Division (CSD) submits 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.

DATES: Comments are encouraged and will be accepted until October 25, 2024.

ADDRESSES: You may submit comments, identified by docket number CISA–2024–0021, by following the instructions below for submitting comment via the Federal eRulemaking Portal at *http://www.regulations.gov.*

Instructions: All comments received must include the agency name and docket number Docket # CISA–2024–0021. All comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided.

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

FOR FURTHER INFORMATION CONTACT: For specific questions related to collection activities, please contact Shannon Moser at 202–603–6924 or at *cisa.csd.jcdc.ca_oversight@cisa.dhs.gov.*

SUPPLEMENTARY INFORMATION: 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).

The Homeland Security Act of 2002, as amended, established ''a national cybersecurity and communications integration center (''the Center'') . . . to carry out certain responsibilities of the Director,'' 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), a division of the Center for internet Security, currently fulfills this function. CSD currently funds CIS's MS-ISAC division 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, now known as Sector Risk Management 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), 6 U.S.C. 652(e)(1)(C). The NCSR is a voluntary annual self-assessment.

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.

For a draft copy of the information collection, please contact the information contacr listed in this notice.

Analysis: 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

has been changed in order to keep up with the shifting threat landscape.

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, usually 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 End User survey follows the regular NCSR and will also be fully electronic. It contains 10 multiple choice and fill-in-the-blank answers and takes approximately 10 minutes to complete. The feedback survey will be administered via Qualtrics, and settings will be updated to opt out of collecting participants' IP addresses.

The NCSR is a voluntary self-assessment designed to measure the gaps and capabilities of cybersecurity programs within state, local, tribal and territorial governments. As it is voluntary, we do not know the number of potential respondents. To estimate the number of respondents, we looked at past participation to forecast what participation in the next three years would be. We then took the average of the three-year projection as our estimated annual respondents. This gave us an estimated 3,719 annual respondents. Table 1 presents the estimated number of respondents, based on historical data.

This submission is a revision to the current approved PRA information collection request that is set to expire on 12/31/2025.

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.

Analysis

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

Title of Collection: Nationwide Cyber Security Review Assessment.

OMB Control Number: CISA–1670–0040.

Frequency: Annually.

Affected Public: State, local, Tribal, and Territorial Government and Private Sector Individuals.

Number of Respondents: 4,210 for NCSR Assessment, 150 for End User Survey.

Estimated Time per Respondent: 2 hours per respondent for NCSR Assessment, 0.167 hours (10 minutes) per End User Survey.

Total Burden Hours: 8,445.

Total Annualized Respondent Cost: $557,355.

Total Annualized Government Cost: $547.67.

Robert J. Costello,

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

[FR Doc. 2024–19118 Filed 8–23–24; 8:45 am]

BILLING CODE 9111–LF–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2024–0005]

Notice of President's National Infrastructure Advisory Council Meeting

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

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

SUMMARY: CISA is publishing this notice to announce the following President's National Infrastructure Advisory Council (NIAC) meeting.

DATES:

Meeting Registration: Registration is required to attend the meeting and must be received no later than 5:00 p.m. Eastern Daylight Time (EDT) on September 4, 2024. For more information on how to participate, please contact *NIAC@cisa.dhs.gov.*

Speaker Registration: Registration to speak during the meeting's public comment period must be received no later than 5:00 p.m. EDT on September 4, 2024.

Written Comments: Written comments must be received no later than 5:00 p.m. EDT on September 4, 2024.

Meeting Date: The NIAC will meet on September 10, 2024, from 1:00 p.m. to 5:00 p.m. EDT. The meeting may close early if the council has completed its business.

ADDRESSES: The National Infrastructure Advisory Council's open session will be held in person at 1650 17th St. NW, Washington, DC; however, members of the public may participate via teleconference only. Requests to participate will be accepted and processed in the order in which they are received. For access to the conference call bridge, information on services for individuals with disabilities, or to request special assistance, please email *NIAC@cisa.dhs.gov* by 5:00 p.m. EDT on September 4, 2024. The NIAC is committed to ensuring all participants have equal access regardless of disability status. If you require a