9110-9P

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 [***INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER***].

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: 9/30/2022 8:45 am; Publication Date: 10/3/2022]