This document is scheduled to be published in the Federal Register on 10/17/2018 and available online at **https://federalregister.gov/d/2018-22548**, and on **govinfo.gov**

**9110-9P P**

**DEPARTMENT OF HOMELAND SECURITY**

**Nationwide Cyber Security Review Assessment**

**AGENCY:** Office of Cybersecurity and Communications (CS&C), National Protection and Programs Directorate (NPPD), Department of Homeland Security (DHS).

**ACTION:** 30-Day Notice and request for comments; New Collection, 1670-NEW.

**SUMMARY:** DHS NPPD CS&C 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. DHS previously published this information collection request (ICR) in the Federal Register on Thursday, July 5, 2018 at 83 FR 31412 for a 60-day public comment period. 0 comments were received by DHS. The purpose of this notice is to allow an additional 30 days for public comments.

**DATES:** Comments are encouraged and will be accepted until [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

**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-NEW - Nationwide Cyber Security Review Assessment.

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 e-mail comment, your e-mail 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:** For specific questions related to collection activities, please contact Donna Beach at 703-705-6213 or at SLTTCyber@HQ.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 Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) division. 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 [NCCIC]… to carry out certain responsibilities of the Under Secretary," including the provision of assessments. 6 U.S.C. 148(b). The Act also directs the

composition of the NCCIC 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 NCCIC. 6 U.S.C. 148(d)(1)(E). The Multistate Information Sharing and Analysis Center (MS-ISAC) currently fulfills this function. NPPD funds the MS-ISAC through a Cooperative Agreement and maintains a close relationship with this entity. As part of the Cooperative Agreement, DHS directs the MS-ISAC to produce the NCSR as contemplated by Congress.

Generally, NPPD has authority to perform risk and vulnerability assessments for Federal and non-Federal entities, with consent and upon request. The NCCIC performs these assessments in accordance with its authority to provide voluntary technical assistance to Federal and non-Federal entities. See 6 U.S.C. 148(c)(6), 143(2). 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 NPPD or request NPPD to perform an on-site risk and vulnerability assessment. See 6 U.S.C. 148(c)(6), 143(2), 6 U.S.C. 121(d)(2). 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, SECIR developed the NCSR to measure the gaps and capabilities of cybersecurity programs within SLTT governments. Using the anonymous results of the NCSR, DHS 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 governments' cybersecurity programs gaps and capabilities the NCSR question sets and surveys may slightly change from year-to-year to accurately reflect the current cybersecurity environment.

The NCSR is an annual voluntary self-assessment that is hosted on the RSA Archer Suite, 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 – December. In efforts of increasing 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, DHS & 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, DHS delivers a bi-annual summary report to Congress that provides a broad picture of the cybersecurity gaps & 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 from 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.

Additionally, MS-ISAC will administer a survey to those who were registered participants in the past and did not register or complete the most recent NCSR. The purpose of the Non-Response Survey is to solicit feedback on ways the NSCR could be improved to maximize benefits and increase response rates in the future.

The NCSR assessment requires approximately two hours for completion and is located on the RSA Archer Suite. 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.

The Non-Response Survey will be fully electronic and take approximately 10 minutes to complete. The survey will be administered via Survey Monkey and settings will be updated to opt out of collecting participants' IP addresses.

This is a new 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.

*Title of Collection*: Nationwide Cyber Security Review Assessment

*OMB Control Number*: 1670-NEW

*Frequency*: Annually

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

*Number of Respondents*: 591

*Estimated Time Per Respondent*: 2 hours

*Total Burden Hours*: 1,278

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

*Total Recordkeeping Burden:* $0

*Total Burden Cost (operating/maintaining):* $0

**David Epperson,**

*Chief Information Officer.*

[FR Doc. 2018-22548 Filed: 10/16/2018 8:45 am; Publication Date: 10/17/2018]