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 10–16–18; 8:45 am]

BILLING CODE 9110–9P–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS–2018–0058]

Telecommunications Service Priority System

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

ACTION: 60-Day Notice and request for comments; Extension, 1670–0005.

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.

DATES: Comments are encouraged and will be accepted until December 17, 2018.

ADDRESSES: You may submit comments, identified by docket number DHS–2018–0058, by one of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov.* Please follow the instructions for submitting comments.
- *Email: deborah.bea@HQ.DHS.GOV.* Please include docket number DHS–2018–0058 in the subject line of the message.
- *Mail:* Written comments and questions about this Information Collection Request should be forwarded to DHS/NPPD/CS&C/OEC, ATTN: 1670–0005, 245 Murray Lane, SW, Mail Stop 0615, Deborah Bea, Arlington, VA 20528.

Instructions: All submissions received must include the words ''Department of Homeland Security'' and the docket number for this action. 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. 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: For specific questions related to collection activities, please contact Deborah Bea at 703.705.6302 or at *deborah.bea@HQ.DHS.GOV.*

SUPPLEMENTARY INFORMATION:

Telecommunications Service Priority (TSP) is authorized by E.O. 12472, E.O. 13618 and 47 CFR part 64. The DHS Office of Emergency Communications (OEC) uses the TSP Program to authorize national security and emergency preparedness organizations to receive priority treatment for vital voice and data circuits or other telecommunications service, under National Security or Emergency Preparedness telecommunications (NS/EP). The TSP Program provides service vendors a Federal Communications Commission (FCC) mandate to prioritize requests by identifying those services critical to national security and emergency preparedness. A TSP assignment ensures that it will receive priority attention by the service vendor before any non-TSP service.

Four broad categories serve as guidelines for determining whether a circuit or telecommunications service is eligible for priority provisioning or restoration. TSP service user organizations may be in the Federal, State, local, or tribal government, critical infrastructure sectors in industry, non-profit organizations that perform critical NS/EP functions, or foreign governments. Typical TSP service users are responsible for the command and control functions critical to management of and response to NS/EP situations, particularly during the first 24 to 72 hours following an event.

Information to request a priority, to obtain a sponsor for requesting a priority, and for other administrative requirements of the program is required from any person or organization having an NS/EP service for which they wish priority restoration from the vendor providing the service. Information is also required to allow immediate installation of a new service to support NS/EP requirements. Information is required from vendors to allow the OEC to track and identify the telecommunications services that are being provided priority treatment.

The forms used are the SF314 (Revalidation for Service Users), SF315 (TSP Request for Service Users), SF317 (TSP Action Appeal for Service Users), SF318 (TSP Service Confirmation for Service Vendors), and the SF319 (TSP Service Reconciliation for Service Vendors). The SF314 is for users to request that their existing TSP codes be revalidated for three more years. The SF315 is used to request restoration and/or provisioning for an organization's critical circuits. The SF317 is for organizations to appeal the denial of TSP restoration and/or provisioning. The SF318 is for service vendors to provide circuit ID information associated with TSP codes they've been given by their customers. The SF319 is for service vendors to provide data to the program office in order to reconcile their TSP data with the TSP database. Participants request TSP priorities via email in order to reduce the use of the paper forms. The paper forms will also be available for download via the TSP home page.

There have been no changes to the information being collected. The burden for the SF315 Form has increased due to better estimates, and the annual cost burden to respondents and annual government cost has increased due to increased wage rates and compensation factors.

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.

Title of Collection: Telecommunications Service Priority System.

OMB Control Number: 1670–0005.

Frequency: Annually.

Affected Public: State, Local, Tribal, and Territorial Governments and Private Sector.

Number of Respondents: 38,666.

Estimated Time per Respondent: 0.64 hours.

Total Burden Hours: 10,354 hours.

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

Total Recordkeeping Burden: $0.

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

David Epperson,

Chief Information Officer.

[FR Doc. 2018–22549 Filed 10–16–18; 8:45 am]

BILLING CODE 9110–9P–P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

[Docket No. FR–6083–N–03]

Manufactured Housing Consensus Committee (MHCC): Notice Inviting Nominations of Individuals To Serve on the Committee

AGENCY: Office of the Assistant Secretary for Housing—Federal Housing Commissioner, HUD.

ACTION: Notice of request for nominations to serve on the