9110-9P P

DEPARTMENT OF HOMELAND SECURITY

Agency Information Collection Activities: Vulnerability Assessments

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

ACTION: 30-Day Notice and request for comments; Revision, 1670-0035.

SUMMARY: DHS CISA ISD 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 ICR for a 60-day public comment period. No comments were received by CISA. The purpose of this notice is to allow an additional 30 days for public comments.

DATES: Comments are due by [***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, OMB. Comments should be addressed to the 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 1670-0035.

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: Ricky Morgan, 866-844-8163, IPGatewayHelpDesk@hq.dhs.gov.

SUPPLEMENTARY INFORMATION: The Presidential Policy Directive-21 and the National Infrastructure Protection Plan highlight the need for a centrally managed repository of infrastructure attributes capable of assessing risks and facilitating data sharing. To support this mission need, the DHS CISA ISD has developed a data collection system that contains several capabilities which support the homeland security mission in

the area of critical infrastructure (CI) protection.

Protective Security Advisors (PSAs) and Cyber Security Advisors (CSAs) conduct voluntary assessments on CI facilities. These assessments are web-based and are used to collect an organization's basic, high-level information, and its dependencies. This data is then used to determine a Protective Measures Index (PMI) and a Resilience Measures Index (RMI) for the assessed organization. This information allows an organization to see how it compares to other organizations within the same sector as well as allows them to see how adjusting certain aspects would change their score. This allows the organization to then determine where best to allocate funding and perform other high-level decision-making processes pertaining to the security and resiliency of the organization.

The information will be gathered by site visits, arranged between the organization owners and DHS PSAs or CSAs. The PSA or CSA will then visit the site and perform the assessment, as requested. They then return to complete the vulnerability assessment and input the data into the system where the data is then accessible to system users. Once available, the organization and other relevant system users can then review the data and use it for planning, risk identification, mitigation and decision making. All data is

captured electronically by the PSA, CSA or by the organization as a self-assessment. Participation in the vulnerability assessments is voluntary, but full completion of the assessment data collection is required if the organization desires to receive a complete evaluation of their security posture.

After assessments are input into the system, the user is prompted to participate in a feedback questionnaire. Every user is prompted to participate in the Post Assessment questionnaire after entering an assessment. Participation in the Post Assessment questionnaire is voluntary. The Post Assessment Questionnaires are designed to capture feedback about a vulnerability assessment and the system. There are three different questionnaires correlated and prompted after entering a particular assessment into the database. The results are used internally within DHS to make programmatic improvements.

The collection of information uses automated electronic vulnerability assessments and questionnaires. The vulnerability assessments and questionnaires are electronic in nature and include questions that measure the security, resiliency and dependencies of an organization. The vulnerability assessments are arranged at the request of an organization and are then scheduled and performed by a PSA or

CSA.

The changes to the collection since the previous OMB approval include: updating the title of the collection, adding three customer feedback questionnaires, increase in burden estimates and costs. The three questionnaires were added to the collection to provide user feedback on the content and functionality of the system. The addition of the questionnaires have increased the burden estimates by $3,861.

The annual burden cost for the collection has increased by $121,591, from $1,786,166 to $1,907,757, due to the addition of the Post Assessment Questionnaires and updated wage rates.

The annual government cost for the collection has increased by $509,195, from $1,710,959 to $2,220,152, due to the addition of the Post Assessment Questionnaires and updated wage rates.

This is a revision and 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: Cybersecurity and Infrastructure Security Agency Vulnerability Assessments

OMB Control Number: 1670-0035

Frequency: Annually

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

Number of Annualized Respondents: 3,181

Estimated Time Per Respondent: 7.5 hours, 0.17 hours

Total Annualized Burden Hours: 21,907 hours

Total Annualized Respondent Opportunity Cost: $1,907,757

Total Annualized Respondent Out-of-Pocket Cost: $0

Total Annualized Government Cost: $2,220,152

Scott Libby,
Deputy Chief Information Officer.
[FR Doc. 2019-24743 Filed: 11/13/2019 8:45 am; Publication Date: 11/14/2019]