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. The vulnerability assessments are voluntary but are required in order for the organization to receive an 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. 2019–14698 Filed 7–9–19; 8:45 am]

BILLING CODE 9910–9P–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2019–0008]

IP Gateway User Registration

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

ACTION: 60-Day notice and request for comments; revision, 1670–0009.

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.

DATES: Comments are due by September 9, 2019.

ADDRESSES: You may submit comments, identified by docket number CISA–2019–0008, by one of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov.* Please follow the instructions for submitting comments.
- *Email: IPGatewayHelpDesk@hq.dhs.gov.* Please include docket number CISA–2019–0008 in the subject line of the message.
- *Mail:* Written comments and questions about this Information Collection Request should be forwarded to DHS/CISA/ISD, ATTN: 1670–0009, 245 Murray Lane SW, Mail Stop 0602, Washington, DC 20598–0602.

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.

Docket: For access to the docket and comments received, please go to *www.regulations.gov* and enter docket number CISA–2019–0008.

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

SUPPLEMENTARY INFORMATION: The Homeland Security Presidential

Directive–7, 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 IDS has developed the IP Gateway. The IP Gateway contains several capabilities which support the homeland security mission in the area of critical infrastructure (CI) protection.

The purpose of this collection is to gather the details pertaining to the users of the IP Gateway for the purpose of creating accounts to access the IP Gateway. This information is also used to verify a need to know to access the IP Gateway. After being vetted and granted access, users are prompted and required to take an online training course upon first logging into the system. After completing the training, users are permitted full access to the system. In addition, this collection will gather feedback from the users of the IP Gateway to determine any future system improvements.

The information gathered will be used by the CISA IP Gateway Program Management Team to vet users for a need to know and grant access to the system. As part of the registration process, users are required to take a one-time online training course. When logging into the system for the first time, the system prompts users to take the training courses. Users cannot opt out of the training and are required to take the course in order to gain and maintain access to the system. When users complete the training, the system automatically logs that the training is complete and allows full access to the system.

Additionally, CISA uses a Utilization Survey to assess the current functionality of the IP Gateway as well as identify any further capabilities to be developed. Through this process, the IP Gateway will remain a viable solution for the stakeholders. This survey is available to users as an ideal way to consolidate end user satisfaction feedback and gather undeveloped capabilities that would aid in the expansion and functionality of the IP Gateway.

The collection of information uses automated electronic forms. During the online registration process, there is an electronic form used to create a user account and an online training course required to grant access.

The survey is electronic and includes questions that measure the satisfaction of the user as well as a section to capture any improvements that the user would like to see added and/or corrected. This voluntary survey is available by clicking a link labeled ''User Survey'' on the IP Gateway landing page. By clicking on this link, the user is then provided the electronic form for them to complete and submit.

The changes to the collection since the previous OMB approval include: Updating the title of the collection, decrease in burden estimates and decrease in costs. The total annual burden cost for the collection has decreased by $31,909, from $37,230 to $5,321 due to a decrease in registrations, as registration is a one-time burden. The total number of responses has decreased by 1,150 from 1,500 to 350 since most users are already registered for the system as well as making updates for the number of survey responses received. The annual government cost for the collection has decreased by $95,188 from $107,857 to $12,668, due to removing the costs associated with designing the survey.

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: IP Gateway User Registration.

OMB Control Number: 1670–0009.

Frequency: Annually.

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

Number of Annualized Respondents: 250.

Estimated Time per Respondent: 0.17 hours, 0.5 hours.

Total Annualized Burden Hours: 92 hours.

Total Annualized Respondent Opportunity Cost: $5,321.

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

Total Annualized Government Cost: $12,668.

Scott Libby,

Deputy Chief Information Officer.

[FR Doc. 2019–14697 Filed 7–9–19; 8:45 am]

BILLING CODE 9110–9P–P

DEPARTMENT OF THE INTERIOR

Fish and Wildlife Service

[Docket No. FWS–R7–ES–2019–0053; FXES111607MRG01–190–FF07CAMM00]

Marine Mammals; Incidental Take During Specified Activities; Proposed Incidental Harassment Authorizations for Northern Sea Otters in Southeast Alaska

AGENCY: Fish and Wildlife Service, Interior.

ACTION: Notice of receipt of applications and proposed incidental harassment authorizations; availability of draft environmental assessments; request for comments.

SUMMARY: We, the U.S. Fish and Wildlife Service, have received two requests, one from the City and Borough of Sitka (CBS) and one from Duck Point Development II, LLC (DPD), for authorization to take small numbers of the southeast Alaska stock of northern sea otters incidental to pile driving in Sitka Sound and Port Frederick, Alaska, between April 1, 2019, and September 30, 2019. However, due to the time needed to process the request, we evaluated the estimated take of northern sea otters during project activities between July 22, 2019, and December 31, 2019. We estimate there may be up to 12 nonlethal, incidental takes by harassment of 4 northern sea otters for the CBS project, and up to 1,380 nonlethal, incidental takes by harassment of 220 northern sea otters for the DPD project. In accordance with provisions of the Marine Mammal Protection Act of 1972, we request comments on our proposed authorizations, which, if finalized, will be for take by Level B harassment only. We anticipate no take by injury or death and include none in these proposed authorizations.

DATES: Comments on the proposed incidental harassment authorizations and draft environmental assessments must be received by August 9, 2019.

ADDRESSES: *Document availability:* You may view these proposed authorizations, the application packages, supporting information, draft environmental assessments, and the