2. Provide necessary technology equipment and services needed to conduct test scenarios;

3. Provide technical assistance for the test plan;

4. Provide support services during the Coast Guard's test scenarios in accordance with the agreed upon test plan; and

5. Provide test data review and feedback as agreed upon completion of testing.

The Coast Guard reserves the right to select for CRADA participants all, some, or no proposals submitted for this CRADA. The Coast Guard will provide no funding for reimbursement of proposal development costs. Proposals and any other material submitted in response to this notice will not be returned. Proposals submitted are expected to be unclassified and have not more than five single-sided pages (excluding cover page, DD 1494, JF–12, etc.). The Coast Guard will select proposals at its sole discretion on the basis of:

1. How well they communicate an understanding, of and ability to meet, the proposed CRADA's goal; and

2. How well they address the following criteria:

a. Technical capability to support the non-Federal party contributions described, and

b. Resources available for supporting the non-Federal party contributions described.

Currently, the Coast Guard is considering Axon Enterprise, Inc. for participation in this CRADA. This consideration is based on the fact that Axon Enterprise, Inc. has demonstrated its technical capability and ability to comply with DHS and DoD requirements for BWC implementation. However, we do not wish to exclude other viable participants from this or similar CRADAs in the future.

This is a technology evaluation effort. The goal of this CRADA is to evaluate technology for its potential compatibility, integration, and ease of use with Coast Guard uniforms, Personal Protective Equipment (PPE), and enforcement gear used by Coast Guard personnel as well as the compatibility, integration, and ease of use with Coast Guard Information Technology (IT) systems. Special consideration will be given to small business firms and consortia, and preference will be given to business units located in the U.S.

This notice is issued under the authority of 5 U.S.C. 552(a).

Dated: June 20, 2024.

M.P. Chien,

Captain, Commanding Officer, U.S. Coast Guard Research and Development Center.

[FR Doc. 2024–13927 Filed 6–25–24; 8:45 am]

BILLING CODE 9110–04–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2024–0013]

Agency Information Collection Activities: Incident Reporting Form and Associated Submission Tools (ICR 1670–0037)

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

ACTION: 60-Day notice and request for comments.

SUMMARY: DHS CISA Cybersecurity Division (CSD) submits the following Information Collection Request (ICR) renewal 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 August 26, 2024.

ADDRESSES: You may submit comments, identified by docket number CISA–2024–0013 at;

- *Federal eRulemaking Portal: http://www.regulations.gov.* Please follow the instructions for submitting comments.

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 alternation to *http://www.regulations.gov,* including any personal information provided.

Docket: For access to the docket to read background documents or comments received, please go to *http://www.regulations.gov* and enter docket number CISA–2024–0013.

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: Brian DeWyngaert; 703–235–5737; *Brian.dewyngaert@cisa.dhs.gov.*

SUPPLEMENTARY INFORMATION: CISA serves as ''a Federal civilian interface for the multi-directional and cross-sector sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities.'' 6 U.S.C. 659(c)(1).

CISA is responsible for performing, coordinating, and supporting response to information security incidents, which may originate outside the Federal community and affect users within it, or originate within the Federal community and affect users outside of it. CISA uses the information from incident reports to develop timely and actionable information for distribution to federal departments and agencies; state, local, tribal and territorial (SLTT) governments; critical infrastructure owners and operators; private industry; and international organizations. Often, the effective handling of security incidents relies on information sharing among individual users, industry, and the Federal Government, which may be facilitated by and through CISA.

Pursuant to the *Federal Information Security Modernization Act of 2014 (FISMA), 44 U.S.C. 3552 et seq.*, CISA operates the federal information security incident center for the United States Federal Government. 44 U.S.C. 3556. Federal agencies notify and consult with CISA regarding information security incidents involving federal information systems. CISA provides federal agencies with technical assistance and guidance on detecting and handling security incidents, compile and analyze incident information that threatens information security, inform agencies of current and potential threats and vulnerabilities, and provide intelligence or other information about cyber threats, vulnerabilities, and incidents to agencies. 44 U.S.C. 3556(a). CISA also receives voluntary incident reports from non-federal entities.

CISA's website (at *https://www.cisa.gov/*) is a primary tool used by constituents to report incident information, access information sharing products and services, and interact with CISA. Constituents, which may include anyone or any entity in the public, use forms located on the website to complete these activities. Incident reports are primarily submitted using CISA's internet reporting system,

available at *https://www.cisa.gov/forms/report.* CISA collects cyber threat indicators and defensive measures in accordance with the requirements of the Cybersecurity Information Sharing Act of 2015 through CISA's Cyber Threat Indicator and Defensive Measure Submission System, *https://www.cisa.gov/forms/share-indicators.* CISA shares cyber threat indicators and defensive measures it receives with certain federal entities in an automated and real-time manner. 6 U.S.C. 1504(c).

By accepting incident reports and feedback, and interacting among federal agencies, industry, the research community, state and local governments, and others to disseminate reasoned and actionable cybersecurity information to the public, CISA has provided a way for citizens, businesses, and other institutions to communicate and coordinate directly with the Federal Government about cybersecurity. The information is collected via the following forms:

1. The Incident Reporting Form, DHS Cyber Threat Indicator and Defensive Measure Submission System, and Malware Analysis Submission Form enable end users to report incidents and indicators as well as submit malware artifacts associated with incidents to CISA. This information is used by DHS to conduct analyses and provide warnings of system threats and vulnerabilities, and to develop mitigation strategies as appropriate. These forms also request the user's name, email address, organization, and infrastructure sector. The primary purpose for the collection of this information is to allow DHS to contact requestors regarding their request.

2. The Mail Lists Form enables end users to subscribe to the National Cyber Awareness System's mailing lists, which deliver the content of and links to CISA's information sharing products. The user must provide an email address in order to subscribe or unsubscribe, though subscribing or unsubscribing are optional. The primary purpose for the collection of this information is to allow DHS to contact requestors regarding their request.

3. The Cyber Security Evaluation Tool (CSET) Download Form, which requests the name, email address, organization, infrastructure sector, country, and intended use of those seeking to download the CSET. All requested fields are optional. The primary purpose for the collection of this information is to allow DHS to contact requestors regarding their request.

Web form submission is also used as the collection method for the other forms listed. In addition to web-based electronic forms, information may be collected through email or telephone. These methods enable individuals, private sector entities, personnel working at other federal or state agencies, and international entities, including individuals, companies and other nations' governments to submit information.

This information collection request is a renewal of an existing collection of information. There are minor changes to the forms, questions, or other collection instruments. These changes reflect the addition of questions for reporting purposes. With this renewal, CISA is replacing the current Advanced Malware Analysis Capability (AMAC) submission form with the Malware Analysis Submission Form (''Malware Next-Gen''), but that form's questions will not change. CISA is also updating the Incident Reporting Form by removing one question, modifying some of the existing questions, and adding questions in order to both improve user experience and help the agency efficiently categorize incident reporting data. To review the developmental digital copy of this updated information collection, please contact the POC listed above in this notice request.

This collection of information will not have a significant economic impact on a substantial number of small entities. Due to increases in wage rates, the changes to the collection since the previous OMB approval include updated burden and cost estimates. The annual burden cost increased by $42,540, from $543,401 to $585,941. The annual government cost increased by $610,548, from $1,886,112 to $2,496,660.

The Office of Management and Budget is particularly interested in comments which:

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.

Analysis

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

Title: Clearance for the Collection of Information through CISA Reporting Forms.

OMB Number: 1670–0037.

Frequency: Annually.

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

Number of Respondents: 139,125.

Estimated Time per Respondent: 0.3333 hours, 0.1667 hours, or 0.0167 hours.

Total Burden Hours: 13,852 hours.

Annualized Respondent Cost: $585,941.

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

Total Annualized Government Cost: $2,496,660.

Robert J. Costello,

Chief Information Officer, Department of Homeland Security, Cybersecurity and Infrastructure Security Agency.

[FR Doc. 2024–14009 Filed 6–25–24; 8:45 am]

BILLING CODE 9111–LF–P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

[Docket No. FR–7083–N–02]

60-Day Notice of Proposed Information Collection; Affirmative Fair Housing Marketing Plan—HUD 935.2A, HUD 935.2B, and HUD 935.2C; OMB Control Number: 2529–0013

AGENCY: Office of the Assistant Secretary for Fair Housing and Equal Opportunity, HUD.

ACTION: Notice.

SUMMARY: This notice solicits public comment for a period of 60 days, consistent with the Paperwork Reduction Act of 1995 (PRA), on the Affirmative Fair Housing Marketing Plan (AFHMP) forms. The AFHMP forms collect information on the advertising and outreach activities of owners/developers of HUD Multifamily, Single Family, and Condominium/Cooperative Housing projects to attract applicants/buyers that are least likely to apply due to their race, color, national origin, religion, sex (including sexual orientation and gender identity), disability, or familial status. The purpose of this notice is to allow for 60 days of public comment.