[FR Doc. 2024–24352 Filed 10–18–24; 8:45 am]
BILLING CODE 9110–12–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: 30-Day notice and request for comments.

SUMMARY: The Cybersecurity Division (CSD) within the Cybersecurity and Infrastructure Security Agency (CISA) submits the following information collection request (ICR) to the Office of Management and Budget (OMB) for review and clearance. CISA previously published this information collection request (ICR) in the **Federal Register** on June 26, 2024, for a 60-day public comment period. CISA received no comments related to this information collection during the comment period. The purpose of this notice is to allow additional 30-days for public comments.

DATES: Comments are encouraged and will be accepted until November 20, 2024. Submissions received after the deadline for receiving comments may not be considered.

ADDRESSES: Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to *www.reginfo.gov/public/do/PRAMain*. Find this particular information collection by selecting ''Currently under 30-day Review—Open for Public Comments'' or by using the search function.

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.

FOR FURTHER INFORMATION CONTACT: Brian DeWyngaert; 202–657–1360; *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.

Analysis

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

Title: Agency Information Collection Activities: Incident Reporting Form and Associated Submission Tools.

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.

Total Annual Burden Cost: $585,941.

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

Robert J. Costello,

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

[FR Doc. 2024–24312 Filed 10–18–24; 8:45 am]

BILLING CODE 9111–LF–P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

[Docket No. FR–7091–N–06]

60-Day Notice of Proposed Information Collection: Application for the Community Development Block Grant (ICDBG) Program for Indian Tribes and Alaska Native Villages; OMB Control No.: 2577–0191

AGENCY: Office of Public and Indian Housing, HUD.

ACTION: Notice.

SUMMARY: HUD is seeking approval from the Office of Management and Budget (OMB) for the information collection described below. In accordance with the Paperwork Reduction Act, HUD is requesting comment from all interested parties on the proposed collection of information. The purpose of this notice is to allow for 60 days of public comment.

DATES: *Comments Due Date:* December 20, 2024.

ADDRESSES: Interested persons are invited to submit comments regarding this proposal.

Written comments and recommendations for the proposed information collection can be sent within 60 days of publication of this notice to *www.regulations.gov.* Interested persons are also invited to submit comments regarding this proposal and comments should refer to the proposal by name and/or OMB Control Number and should be sent to: *Colette.Pollard@hud.gov,* Clearance Officer, REE, Department of Housing and Urban Development, 451 7th Street SW, Room 8210, Washington, DC 20410–5000.

FOR FURTHER INFORMATION CONTACT: Colette Pollard, Reports Management Officer, REE, Department of Housing and Urban Development, 451 7th Street SW, Washington, DC 20410; email *Colette.Pollard@hud.gov,* telephone (202) 402–3400. This is not a toll-free number. HUD welcomes and is prepared to receive calls from individuals who are deaf or hard of hearing, as well as individuals with speech or communication disabilities. To learn more about how to make an accessible telephone call, please visit *https://www.fcc.gov/consumers/guides/telecommunications-relay-service-trs.* Copies of available documents submitted to OMB may be obtained from Colette Pollard.

SUPPLEMENTARY INFORMATION: This notice informs the public that HUD is seeking approval from OMB for the information collection described in Section A.

A. Overview of Information Collection

Title of Information Collection: Indian Community Development Block Grant Information Collection.

OMB Approval Number: 2577–0191.

Type of Request: Renewal of a currently approved collection.

Form Number: SF–425, HUD–2516, and Annual Status and Evaluation Report (ASER).

Description of the need for the information and proposed use: Title I of the Housing and Community Development Act of 1974 authorizes Indian Community Development Block Grants (ICDBG) and requires that grants be awarded annually on a competitive basis. The purpose of the ICDBG program is to develop viable Indian and Alaska Native communities by creating decent housing, suitable living environments, and economic opportunities primarily for low- and moderate-income persons. Consistent with this objective, not less than 70 percent of the expenditures are to benefit low- and moderate-income persons. Eligible applicants include Federally recognized tribes, which includes Alaska Native communities, and tribally authorized tribal organizations. Eligible categories of funding include housing rehabilitation, land acquisition to support new housing, homeownership assistance, public facilities and improvements, economic development, and microenterprise programs. For a complete description of eligible activities, please refer to 24 CFR part 1003, subpart C.

The ICDBG program regulations are at 24 CFR part 1003. The ICDBG program requires eligible applicants to submit information to enable HUD to select the best projects for funding during annual competitions. Additionally, the information submitted is essential for HUD in monitoring grants to ensure that grantees are complying with applicable statutes and regulations and implementing activities as approved.

ICDBG recipients are required to submit a quarterly Federal Financial Report (SF–425) that describes the use of grant funds drawn from the