DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2024–0027]

Agency Information Collection Activities: Vulnerability Reporting Submission Form

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

ACTION: 60-Day notice and request for comments; new information collection request and OMB 1670–NEW.

SUMMARY: The Vulnerability Management (VM) subdivision within 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 in accordance with the Paperwork Reduction Act of 1995.

DATES: Comments are encouraged and will be accepted until December 30, 2024.

ADDRESSES: You may submit comments, identified by docket number Docket # CISA–2024–0027, by following the instructions below for submitting comment via the Federal eRulemaking Portal at *http://www.regulations.gov.*

Instructions: All comments received must include the agency name and docket number Docket # CISA–2024–0027. All comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to *http://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: Kevin Donovan, 202–505–6441, *kevin.donovan@mail.cisa.dhs.gov.*

SUPPLEMENTARY INFORMATION: The Cybersecurity and Infrastructure Security Agency (CISA) operates Coordinated Vulnerability Disclosure (CVD) in partnership with industry stakeholders and community researchers alike. Through this collaboration, CISA provides technical assistance and guidance on detecting and handling security Vulnerability Disclosures, compiles, and analyzes incident information that may threaten information security. 6 U.S.C. 659(c)(1), see also 6 U.S.C. 659(c)(6) (providing for information sharing capabilities as the federal civilian interface for sharing of cybersecurity information and providing technical assistance and risk management support for both Federal Government and non-Federal Government entities). CISA is also authorized to carry out these CVD functions by 6 U.S.C. 659(n) on Coordinated Vulnerability Disclosure, which authorizes CISA to, in coordination with industry and other stakeholders, may develop and adhere to DHS policies and procedures for coordinating vulnerability disclosures.

CISA is responsible for performing Coordinated Vulnerability Disclosure, which may originate outside the United States Government (USG) network/community and affect users within the USG and/or broader community, or originate within the USG community and affect users both within and outside of it. Often, therefore, the effective handling of security incidents relies on information sharing among individual users, industry, and the USG, which may be facilitated by and through CISA. A dedicated form on the CISA website will allow for reporting of vulnerabilities that the reporting entity believe to be CISA Coordinated Vulnerability Disclosure (CVD) eligible. Upon submission, CISA will evaluate the information provided, and then will triage through the CVD process, if all CISA scoped CVD requirements are met.

For the developmental digital copy of this information collection for review, please contact the POC listed above in this notice request.

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: Vulnerability Disclosure Submission Form.

OMB Number: 1670–NEW.

Frequency: Per report on a voluntary basis.

Affected Public: State, Local, Territorial, and Tribal, International, Private sector partners.

Number of Respondents: 2,725.

Estimated Time per Respondent: 0.167 Hours.

Total Burden Hours: 454 Hours.

Annualized Respondent Cost: $39,536.

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

Total Annualized Government Cost: $63,447.

Robert J. Costello,

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

[FR Doc. 2024–25130 Filed 10–29–24; 8:45 am]

BILLING CODE 9111–LF–P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

[Docket No. FR–7092–N–39]

Privacy Act of 1974; System of Records

AGENCY: Office of Administration, HUD.

ACTION: Notice of a new system of records.

SUMMARY: Pursuant to the provisions of the Privacy Act of 1974, as amended, the Department of the Housing and Urban Development (HUD), proposes a new Privacy Act System of Records titled, Customer Relationship Management, to include all ''Customer Relationship Management'' systems in use by HUD. This notice incorporates the One Stop Customer Service, HUD Central, and Microsoft Dynamics systems. HUD's Customer Relation Management systems are designed to track, organize, rout, and respond to HUD's customer, which includes members of the public, individuals or organizations doing business with HUD, and other stakeholders who have an interest in how HUD operates.

DATES: Comments will be accepted on or before November 29, 2024. This proposed action will be effective on the date following the end of the comment period unless comments are received which result in a contrary determination.

ADDRESSES: Interested persons may submit comments, identified by docket number or by one of the following methods: