DEPARTMENT OF HOMELAND SECURITY

[Docket Number DHS–2024–0027]

Agency Information Collection Activities: VULNERABILITY DISCOVERY PROGRAM, OMB CONTROL NO. 1601–0028

AGENCY: Department of Homeland Security (DHS).

ACTION: 60-Day notice and request for comments.

SUMMARY: The Department of Homeland Security 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 encouraged and will be accepted until September 30, 2024. This process is conducted in accordance with 5 CFR 1320.1.

ADDRESSES: You may submit comments, identified by docket number Docket # DHS–2024–0027, at:

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

Instructions: All submissions received must include the agency name and docket number Docket # DHS–2024–2027. 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.*

SUPPLEMENTARY INFORMATION: Security vulnerabilities, defined in section 102(17) of the Cybersecurity Information Sharing Act of 2015, are any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control. Security vulnerability mitigation is a process starting with discovery of the vulnerability leading to applying some solution to resolve the vulnerability. There is constantly a search for security vulnerabilities within information systems, from individuals or nation states wishing to bypass security controls to gain invaluable information, to researchers seeking knowledge in the field of cyber security. Bypassing such security controls in the DHS and other Federal Agencies information systems can cause catastrophic damage including but not limited to loss in Personally Identifiable Information (PII), sensitive information gathering, and data manipulation.

Pursuant to section 101 of the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act, (commonly known as the SECURE Technologies Act) individuals, organizations, and/or companies may submit any discovered security vulnerabilities found associated with the information system of any Federal agency. This collection is used by these individuals, organizations, and/or companies who choose to submit a discovered vulnerability found associated with the information system of any Federal agency.

Specifically, DHS and Federal cybersecurity agencies are working to address vulnerabilities within DHS's components. While DHS had previously obtained approval to collect this information on its own behalf, recent cyberattacks and trends exploiting vulnerabilities have exemplified the need to have this capability government-wide. In June 2023, a major and widespread cyberattack occurred by Russian cybercriminals, that impacted multiple U.S. federal government agencies. This was reported to be a result of cybercriminals exploiting a vulnerability in widely used software known as MOVEit. Cybercriminals gained the opportunity exploit the software that agencies use to transfer data. This attack was reported to be widespread and allowed for cybercriminals to break into multiple networks due to lack of remediation. Impacted organizations included The Energy Department, Johns Hopkins University, and University of Georgia. The MOVEit exploitation appears to have affected at least 122 organizations and exposed the data of roughly 15 million people. These numbers are based on posts from CL0P, the Russian ransomware group that has claimed responsibility for the attacks. This is just a single example among a myriad of vulnerabilities and incidents that we strive to avoid.

Public Law 116–283, Sec. 1705 (which amended 44 U.S.C. 3553) permits extensive sharing of information regarding cybersecurity and the protection of information and information systems from cybersecurity risks between Federal Agencies covered by the Federal Information Security Modernization Act and the Department of Homeland Security. This unique authority makes DHS well positioned to host the approval of this information collection on behalf of other Federal agencies

DHS is requesting pursuant to 44 US Code 33554(a)(1)(B), that the information collection continue to be designated for any Federal agency's ability to utilize the standardized DHS online Vulnerability Disclosure Form to collect their own agency's vulnerability information and post the information on their own agency websites.

DHS leverages the form to collect information about vulnerabilities impacting DHS assets. The form includes the following: vulnerable host(s), necessary information for reproducing the security vulnerability, remediation or suggestions for remediation of the vulnerability, and potential impact on host, if not remediated.

This form allows Federal agencies to complete the following actions; (1) allow the individuals, organizations, and/or companies who discover vulnerabilities in the information systems to report their findings to the agency, and (2) provide the agencies initial insight into any newly discovered vulnerabilities, as well as zero-day vulnerabilities in order to mitigate the security issues prior to malicious actors acting upon the vulnerability for malicious intent.

The form also benefits researchers and provides a safe and lawful method to practice and discover new cyber methods to discover the vulnerabilities. It provides the same benefit to Federal agencies and promotes the enhancement of Federal information system security policies.

Respondents may electively submit their information directly to the agency in which they would like to report a vulnerability. Federal Agencies provide the form electronically via their agency's website. The information collected does not have an impact on small business or other small entities.

The collection of this information is related to the discovery of security vulnerabilities by individuals, organizations, and/or companies is needed to fulfill the congressional mandate in Section 101 of the SECURE Technologies Act related to creating Vulnerability Disclosure Policies. In addition, without the ability to collect information on newly discovered security vulnerabilities associated with Federal agency information systems, Federal agencies will rely solely on the internal security personnel and/or the discovery through a post occurrence breach of security controls.

There are no assurances of confidentiality provide. Any PII that is collected is for the sole purpose of feedback and dialogue. This information collection is covered by a Privacy Impact Assessment (PIA), DHS/ALL/PIA–006 DHS General Contacts List (June 15, 2007), and a System of Records Notice, DHS/ALL–002 Department of

Homeland Security (DHS) Mailing and Other Lists System, 73 FR 71659 (November 25, 2008).

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: Department of Homeland Security (DHS).

Title: VULNERABILITY DISCOVERY PROGRAM.

OMB Number: 1601–0028.

Frequency: Annually.

Affected Public: Individuals, Organizations, and/or Companies.

Number of Respondents: 3,000.

Estimated Time per Respondent: 3 hours.

Total Burden Hours: 9,000.

Robert Dorr,

Executive Director, Business Management Directorate.

[FR Doc. 2024–16855 Filed 7–30–24; 8:45 am]

BILLING CODE 9112–FL–P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

[Docket No. FR–7080–N–33]

30-Day Notice of Proposed Information Collection: OMB Circular A–11 Section 280 Customer Experience Clearance OMB Control No.: 2511–0001

AGENCY: Office of Policy Development and Research, Chief Data Officer, 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 30 days of public comment.

DATES: *Comments Due Date:* August 30, 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 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. Interested persons are also invited to submit comments regarding this proposal by name and/or OMB Control Number and should be sent to: Colette Pollard, Reports Management Officer, REE, Department of Housing and Urban Development, 451 7th Street SW, Room 8210, Washington, DC 20410; telephone (202) 402–3577 (this is not a toll-free number) or email: *PaperworkReductionActOffice@hud.gov.*

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* or 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 Ms. Pollard.

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

The **Federal Register** notice that solicited public comment on the information collection for a period of 60 days was published on May 17, 2024, at 89 FR 43423.

A. Overview of Information Collection

Title of Information Collection: Renewal of OMB Circular A–11 Section 280 Customer Experience Clearance.

OMB Approval Number: 2511–0001.

OMB Expiration Date: 09/30/2024.

Type of Request: Extension of an existing collection.

Form Number: None.

Description of the need for the information and proposed use: Under the PRA, (*44 U.S.C. 3501–3520*) Federal Agencies must obtain approval from the Office of Management and Budget (OMB) for each collection of information they conduct or sponsor. ''Collection of information'' is defined in *44 U.S.C. 3502(3)* and *5 CFR 1320.3(c)* and includes Agency requests or requirements that members of the public submit reports, keep records, or provide information to a third party. Section 3506(c)(2)(A) of the PRA requires Federal Agencies to provide a 60-day and a 30-day notice in the **Federal Register** concerning each proposed collection of information, including each proposed extension of an existing collection of information, before submitting the collection to OMB for approval. To comply with this requirement, HUD published the 60-day notice in the **Federal Register** on 05/17/2024 and is now publishing this 30-day notice of the proposed collection of information set forth in this document.

Whether seeking a loan, Social Security benefits, veterans' benefits, or other services provided by the Federal Government, individuals and businesses expect Government customer services to be efficient and intuitive, just like services from leading private-sector organizations. Yet the 2016 American Consumer Satisfaction Index and the 2017 Forrester Federal Customer Experience Index show that, on average, Government services lag nine percentage points behind the private sector.

A modern, streamlined and responsive customer experience means: Raising government-wide customer experience to the average of the private sector service industry; developing indicators for high-impact Federal programs to monitor progress towards excellent customer experience and mature digital services; and providing the structure (including increasing transparency) and resources to ensure customer experience is a focal point for agency leadership. To support this, OMB Circular A–11 Section 280 established government-wide standards for mature customer experience organizations in government and measurement. To enable Federal programs to deliver the experience taxpayers deserve, they must undertake three general categories of activities: Conduct ongoing customer research, gather and share customer feedback, and test services and digital products.