Still, SBOM generation and sharing across the software supply chain was not seen as a commonly accepted practice in modern software. In 2018, the National Telecommunications and Information Administration (NTIA) convened the first multistakeholder process to promote software component transparency.[9] Over the subsequent three years, this stakeholder community developed guidance to help foster the idea of SBOM, including high-level overviews, initial advice on implementation, and technical resources.[10] When the NTIA-initiated, multistakeholder process concluded, NTIA noted ''what was an obscure idea became a key part of the global agenda around securing software supply chains.'' [11] In July 2022, CISA facilitated eight public listening sessions around four open topics (two for each topic): Cloud & Online Applications, Sharing & Exchanging SBOMs, Tooling & Implementation, and On-ramps & Adoption.[12] These public listening sessions resulted in the formation of four public, community-led workstreams around each of the four topics. The groups have been convening on a weekly basis since August 2022. More information can be found at *https://cisa.gov/SBOM.*

CISA believes that the concept of SBOM and its implementation would benefit from further refinement, and that a broad-based community effort can help scale and operationalize SBOM implementation. To support such a community effort to advance SBOM technologies, processes, and practices, CISA facilitated the 2023 CISA SBOM-a-Rama. The Winter 2024 SBOM-a-Rama will build on the 2023 event to offer updates as well as present new discussion topics for consideration by the community.

II. Topics for CISA SBOM-a-Rama

The goal of this meeting is to help the broader software and security community understand the current state of SBOM and what efforts have been made by different parts of the SBOM community, including CISA-facilitated, community-led work and other activity from sectors and governments. Attendees are invited to ask questions, share comments, and raise further issues that need attention. Specific presentations will be made on the community-led efforts around sharing SBOMs, cloud and online applications, tools and implementation, the Vulnerability Exploitability eXchange (VEX) model, and SBOM on-ramps and adoption. The event will also feature presentations and discussions on sector efforts around the world. CISA will also facilitate conversations on how the community can most efficiently make progress in addressing gaps in the SBOM ecosystem.

A full agenda will be posted in advance of the meeting at *https://www.cisa.gov/news-events/events/sbom-rama-winter-2024.*

III. Participation in the SBOM-a-Rama

This event is open to anyone. CISA welcomes participation from anyone interested in learning about the current state of SBOM practice and implementation including private sector practitioners, policy experts, academics, and representatives from non-U.S. organizations. Additional information, including the meeting link, will be available one week before the meeting date at *https://www.cisa.gov/news-events/events/sbom-rama-winter-2024.*

This notice is issued under the authority of 6 U.S.C. 652(c)(10)–(11) and 6 U.S.C. 659(c)(4).

Eric Goldstein,

Executive Assistant Director for Cybersecurity, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security.

[FR Doc. 2024–04235 Filed 2–28–24; 8:45 am]

BILLING CODE 9110–9P–P

cites a range of standards. *Managing Security Risks Inherent in the Use of Third-party Components,* SAFECode (May 2017), *available at https://www.safecode.org/wp-content/uploads/2017/05/SAFECode_TPC_Whitepaper.pdf.*

[9] National Telecommunications and Information Administration (NTIA), Notice of Open Meeting, 83 FR. 26434 (June 7, 2018).

[10] *Ntia.gov/SBOM.*

[11] NTIA, *Marking the Conclusion of NTIA's SBOM Process* (Feb. 9, 2022), *https://www.ntia.doc.gov/blog/2022/marking-conclusion-ntia-s-sbom-process.*

[12] Public Listening Sessions on Advancing SBOM Technology, Processes, and Practices, *https://www.federalregister.gov/documents/2022/06/01/2022-11733/public-listening-sessions-on-advancing-sbom-technology-processes-and-practices.*

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2024–0008]

Agency Information Collection Activities: Actively Exploited Vulnerability Submission Form

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

ACTION: 60-Day notice and request for comments; new collection request and OMB control number is 1670–NNEW.

SUMMARY: The Vulnerability Management (VM) within Cybersecurity and Infrastructure Security Agency (CISA) will submit the following Information Collection Request (ICR) to the Office of Management and Budget (OMB) for review.

DATES: Comments are encouraged and will be accepted until April 29, 2024.

ADDRESSES: You may submit comments, identified by docket number Docket # CISA–2024–0008, 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 # CISA–2024–0008. 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: Christopher Murray, *christopher.murray@cisa.dhs.gov,* or 202–984–0874.

SUPPLEMENTARY INFORMATION: The Cybersecurity and Infrastructure Security Agency (CISA) operates the federal information security incident center. Through this center, CISA provides technical assistance and guidance on detecting and handling security Vulnerability Disclosures, 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), see also 6 U.S.C. 659(c) (providing for cybersecurity services for both Federal Government and non-Federal Government entities).

CISA is responsible for performing coordinated Vulnerability Disclosure, which may originate outside the United States Government (USG) network/community and affect users within it, or originate within the USG community and affect users 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 external reporting of vulnerabilities that the reporting entity believe to be Known Exploited Vulnerabilities (KEV) eligible. Upon submission, CISA will evaluate the information provided, and then will add to the KEV Catalog, if all KEV 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: Actively Exploited Vulnerability Submission Form.

OMB Number: 1670–NEW.

Frequency: Per incident 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.

Annual Cost Burden: $37,956.

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

Total Annualized Government Cost: $145,924.

Robert J. Costello,

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

[FR Doc. 2024–04193 Filed 2–28–24; 8:45 am]

BILLING CODE 9110–9P–P

DEPARTMENT OF HOMELAND SECURITY

U.S. Citizenship and Immigration Services

[OMB Control Number 1615–0060]

Agency Information Collection Activities; Extension, Without Change, of a Currently Approved Collection: Medical Certification for Disability Exceptions

AGENCY: U.S. Citizenship and Immigration Services, Department of Homeland Security.

ACTION: 60-Day notice.

SUMMARY: The Department of Homeland Security (DHS), U.S. Citizenship and Immigration Services (USCIS) invites the general public and other Federal agencies to comment upon this proposed extension. In accordance with the Paperwork Reduction Act (PRA) of 1995, the information collection notice is published in the **Federal Register** to obtain comments regarding the nature of the information collection, the categories of respondents, the estimated burden (*i.e.,* the time, effort, and resources used by the respondents to respond), the estimated cost to the respondent, and the actual information collection instruments.

DATES: Comments are encouraged and will be accepted for 60 days until April 29, 2024.

ADDRESSES: All submissions received must include the OMB Control Number 1615–0060 in the body of the letter, the agency name and Docket ID USCIS–2008–0021. Submit comments via the Federal eRulemaking Portal website at *https://www.regulations.gov* under e-Docket ID number USCIS–2008–0021.

FOR FURTHER INFORMATION CONTACT: USCIS, Office of Policy and Strategy, Regulatory Coordination Division, Samantha Deshommes, Chief, telephone number (240) 721–3000 (This is not a toll-free number. Comments are not accepted via telephone message). Please note contact information provided here is solely for questions regarding this notice. It is not for individual case status inquiries. Applicants seeking information about the status of their individual cases can check Case Status Online, available at the USCIS website at *https://www.uscis.gov,* or call the USCIS Contact Center at 800–375–5283 (TTY 800–767–1833).

SUPPLEMENTARY INFORMATION:

Comments

You may access the information collection instrument with instructions or additional information by visiting the Federal eRulemaking Portal site at: *https://www.regulations.gov* and entering USCIS–2008–0021in the search box. Comments must be submitted in English, or an English translation must be provided. All submissions will be posted, without change, to the Federal eRulemaking Portal at *https://www.regulations.gov,* and will include any personal information you provide. Therefore, submitting this information makes it public. You may wish to consider limiting the amount of personal information that you provide in any voluntary submission you make to DHS. DHS may withhold information provided in comments from public viewing that it determines may impact the privacy of an individual or is offensive. For additional information, please read the Privacy Act notice that is available via the link in the footer of *https://www.regulations.gov.*

Written comments and suggestions from the public and affected agencies should address one or more of the following four points:

(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 submission of responses.

Overview of This Information Collection

(1) *Type of Information Collection:* Extension, Without Change, of a Currently Approved Collection.

(2) *Title of the Form/Collection:* Medical Certification for Disability Exceptions.

(3) *Agency form number, if any, and the applicable component of the DHS sponsoring the collection:* N–648; USCIS.

(4) *Affected public who will be asked or required to respond, as well as a brief abstract: Primary:* Individuals or households. USCIS uses the Form N–648 to substantiate a claim for an