Place: National Institutes of Health, Rockledge II, 6701 Rockledge Drive, Bethesda, MD 20892 (Virtual Meeting).

Contact Person: Mollie Kim Manier, Ph.D., Scientific Review Officer, Center for Scientific Review, National Institutes of Health, 6701 Rockledge Drive, Bethesda, MD 20892, (301) 594–0510, *mollie.manier@nih.gov.*

Name of Committee: Center for Scientific Review Special Emphasis Panel; RFA–OD–24–001: Study and Techniques on Intimate Partner Violence in Different Populations.

Date: March 21, 2024.

Time: 12:00 p.m. to 7:00 p.m.

Agenda: To review and evaluate grant applications.

Place: National Institutes of Health, Rockledge II, 6701 Rockledge Drive, Bethesda, MD 20892 (Virtual Meeting).

Contact Person: Helena Eryam Dagadu, Ph.D., Scientific Review Officer, Center for Scientific Review, National Institutes of Health, 6701 Rockledge Drive, Room 3137, Bethesda, MD 20892, (301) 451–6273, *dagaduhe@csr.nih.gov.*

Name of Committee: Center for Scientific Review Special Emphasis Panel; Member Conflict: Communication, Motor Function, and Human Development.

Date: March 22, 2024.

Time: 10:00 a.m. to 7:00 p.m.

Agenda: To review and evaluate grant applications.

Place: National Institutes of Health, Rockledge II, 6701 Rockledge Drive, Bethesda, MD 20892 (Virtual Meeting).

Contact Person: Sara Louise Hargrave, Ph.D., Scientific Review Officer, Center for Scientific Review, National Institutes of Health, 6701 Rockledge Drive, Room 3170, Bethesda, MD 20892, (301) 443–7193, *hargravesl@mail.nih.gov.*

Name of Committee: Infectious Diseases and Immunology B Integrated Review Group; HIV Comorbidities and Clinical Studies Study Section.

Date: March 26–27, 2024.

Time: 9:00 a.m. to 8:00 p.m.

Agenda: To review and evaluate grant applications.

Place: The Westin Georgetown, 2350 M Street NW, Washington, DC 20037.

Contact Person: Shannon J. Sherman, Ph.D., Scientific Review Officer, Center for Scientific Review, The National Institutes of Health, 6701 Rockledge Drive, Bethesda, MD 20892, 301–594–0715, *shannon.sherman@nih.gov.*

Name of Committee: Center for Scientific Review Special Emphasis Panel; Small Business: SBIR/STTR Commercialization Readiness Pilot (CRP) Program.

Date: March 26–27, 2024.

Time: 10:00 a.m. to 2:00 p.m.

Agenda: To review and evaluate grant applications.

Place: National Institutes of Health, Rockledge II, 6701 Rockledge Drive, Bethesda, MD 20892 (Virtual Meeting).

Contact Person: Marie-Jose Belanger, Ph.D., Scientific Review Officer, Center for Scientific Review, National Institutes of Health, 6701 Rockledge Drive, Rm 6188, MSC 7804, Bethesda, MD 20892, 301–435–1267, *belangerm@csr.nih.gov.*

Name of Committee: Center for Scientific Review Special Emphasis Panel; Program Projects: Neuroscience and Genetics of Drug Abuse.

Date: March 26, 2024.

Time: 1:00 p.m. to 6:00 p.m.

Agenda: To review and evaluate grant applications.

Place: National Institutes of Health, Rockledge II, 6701 Rockledge Drive, Bethesda, MD 20892 (Virtual Meeting).

Contact Person: Jacek Topczewski, Ph.D., Scientific Review Officer, Center for Scientific Review, National Institutes of Health, 6701 Rockledge Drive, Room 1002A1, Bethesda, MD 20892, (301) 594–7574, *topczewskij2@csr.nih.gov.*

(Catalogue of Federal Domestic Assistance Program Nos. 93.306, Comparative Medicine; 93.333, Clinical Research, 93.306, 93.333, 93.337, 93.393–93.396, 93.837–93.844, 93.846–93.878, 93.892, 93.893, National Institutes of Health, HHS)

Dated: February 26, 2024.

Melanie J. Pantoja,

Program Analyst, Office of Federal Advisory Committee Policy.

[FR Doc. 2024–04253 Filed 2–28–24; 8:45 am]

BILLING CODE 4140–01–P

DEPARTMENT OF HOMELAND SECURITY

Winter 2024 CISA SBOM-a-Rama

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

ACTION: Announcement of meeting.

SUMMARY: CISA will facilitate a public event to build on existing community-led work around Software Bill of Materials (SBOM) on specific SBOM topics. 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.

DATES: February 29, 2024, 12 p.m. to 4 p.m. EST.

ADDRESSES: The event will be virtual. Connection and dial-in information for this virtual event will be available one week before this event at *https://www.cisa.gov/news-events/events/sbom-rama-winter-2024.*

FOR FURTHER INFORMATION CONTACT: Allan Friedman, 202–961–4349, *sbom@cisa.dhs.gov.*

SUPPLEMENTARY INFORMATION: An SBOM has been identified by the cybersecurity community as a key aspect of modern cybersecurity, including software security and supply chain security. Executive Order (E.O.) 14028 declares that ''the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.'' [1] SBOMs play a key role in providing this transparency.

E.O. 14028 defines SBOM as ''a formal record containing the details and supply chain relationships of various components used in building software.'' [2] The E.O. further notes that ''software developers and vendors often create products by assembling existing open source and commercial software components. The SBOM enumerates these components in a product.'' [3] Transparency from SBOMs aids multiple parties across the software lifecycle, including software developers, purchasers, and operators.[4] Recognizing the importance of SBOMs in transparency and security, and that SBOM evolution and refinement is likely to be most effective coming from the community; CISA is facilitating a public event which is intended to advance the software and security communities' understanding of SBOM creation, use, and implementation across the broader technology ecosystem.

I. SBOM Background

The idea of an SBOM is not novel.[5] It has been discussed and explored in the software industry for years, building on industrial and supply chain innovations.[6] Academics identified the potential value of a ''software bill of materials'' as far back as 1995,[7] and tracking use of third-party code is a longstanding software best practice.[8]

[1] E.O. 14028, Improving the Nation's Cybersecurity, 1, 86 FR 26633 (May 17, 2021).

[2] *Id.* at 10(j), 86 FR 26633 at 26646 (May 17, 2021).

[3] Ibid.

[4] Ibid.

[5] A brief summary of the history of a software bill of materials can be found in Carmody, S., Coravos, A., Fahs, G. et al. Building resilient medical technology supply chains with a software bill of materials. npj Digit. Med. 4, 34 (2021). *https://doi.org/10.1038/s41746-021-00403-w.*

[6] See ''Toyota Supply Chain Management: A Strategic Approach to Toyota's Renowned System'' by Ananth V. Iyer, Sridhar Seshadri, and Roy Vasher—a work about Edwards Deming's Supply Chain Management *https://books.google.com/books/about/Toyota_Supply_Chain_Management_A_Strateg.html?id=JY5wqdelrg8C.*

[7] Leblang D.B., Levine P.H., Software configuration management: Why is it needed and what should it do? In: Estublier J. (eds) Software Configuration Management Lecture Notes in Computer Science, vol. 1005, Springer, Berlin, Heidelberg (1995).

[8] The Software Assurance Forum for Excellence in Code (SAFECode), an industry consortium, has released a report on third party components that

Continued

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.