Name of Committee: Center for Scientific Review Special Emphasis Panel; Member Conflict: Sensorimotor, Olfaction, and Interoception.

Date: November 21, 2024.

Time: 12 p.m. to 6 p.m.

Agenda: To review and evaluate grant applications.

Address: National Institutes of Health, Rockledge II, 6701 Rockledge Drive, Bethesda, MD 20892.

Meeting Format: Virtual Meeting.

Contact Person: Kirk Thompson, Ph.D., Scientific Review Officer, Center for Scientific Review, National Institutes of Health, 6701 Rockledge Drive, Room 5184, MSC 7844, Bethesda, MD 20892, 301–435–1242, email: *kgt@mail.nih.gov.*

Name of Committee: Center for Scientific Review Special Emphasis Panel; Member Conflict: Skeletal Muscle and Rehabilitation Sciences.

Date: November 22, 2024.

Time: 9 a.m. to 6 p.m.

Agenda: To review and evaluate grant applications.

Address: National Institutes of Health, Rockledge II, 6701 Rockledge Drive, Bethesda, MD 20892.

Meeting Format: Virtual Meeting.

Contact Person: Chee Lim, Ph.D., Scientific Review Officer, Center for Scientific Review, National Institutes of Health, 6701 Rockledge Drive, Room 4128, Bethesda, MD 20892, (301) 435–1850, email: *limc4@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: October 24, 2024.

Bruce A. George,

Program Analyst, Office of Federal Advisory Committee Policy.

[FR Doc. 2024–25099 Filed 10–28–24; 8:45 am]

BILLING CODE 4140–01–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2024–0028]

Request for Comment on Product Security Bad Practices Guidance

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

ACTION: Notice of availability; extension of comment period.

SUMMARY: On October 16, 2024, the Cybersecurity Division (CSD) within the Cybersecurity and Infrastructure Security Agency (CISA) published a request for comment in the **Federal Register** on the voluntary, draft Product Security Bad Practices guidance, which requests feedback on the draft guidance. CISA is extending the comment period for the draft guidance for an additional fourteen days through December 16, 2024.

DATES: The comment period for the proposed voluntary guidance published on October 16, 2024, at 89 FR 83508 is extended. Comments and related materials must be submitted on or before December 16, 2024.

ADDRESSES: You may submit comments, identified by docket number CISA–2024–0028, by following the instructions below for submitting comments via the Federal eRulemaking Portal at *https://www.regulations.gov.*

Instructions: All comments received must include the agency name and docket number Docket Number CISA–2024–0028. All comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided. CISA reserves the right to publicly republish relevant and unedited comments in their entirety that are submitted to the docket. Do not include personal information such as account numbers, social security numbers, or the names of other individuals. Do not submit confidential business information or otherwise sensitive or protected information.

Docket: For access to the docket to read the draft Product Security Bad Practices Guidance or comments received, go to *https://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: Kirk Lawrence, 202–617–0036, *SecureByDesign@cisa.dhs.gov.*

SUPPLEMENTARY INFORMATION: On October 16, 2024, CISA published a request for comment on voluntary, draft Product Security Bad Practices guidance (89 FR 83508). In the draft guidance, we provided an overview of product security practices that are deemed exceptionally risky, particularly for organizations supporting critical infrastructure or national critical functions (NCFs), and it provides recommendations for software manufacturers to voluntarily mitigate these risks. The guidance contained in the document is non-binding, and while CISA encourages organizations to avoid these bad practices, the document imposes no requirement on them to do so. The draft guidance is scoped to software manufacturers who develop software products and services, including on-premises software, cloud services, and software as a service (SaaS), used in support of critical infrastructure or NCFs. The request for comment provided for a 45-day comment period, set to close on December 2, 2024. CISA received requests to extend the deadline given the Thanksgiving holiday. Therefore, the comment period is now open through December 16, 2024.

This notice is issued under the authority of 6 U.S.C. 652 and 659.

Jeffrey E. Greene,

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

[FR Doc. 2024–25078 Filed 10–28–24; 8:45 am]

BILLING CODE 9111–LF–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2024–0029]

Request for Comment on Security Requirements for Restricted Transactions Under Executive Order 14117

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

ACTION: Notice and request for comment.

SUMMARY: CISA seeks public input on the development of security requirements for restricted transactions as directed by Executive Order (E.O.) 14117, ''Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern.'' E.O. 14117 addresses national-security and foreign-policy threats that arise when countries of concern and covered persons can access bulk U.S. sensitive personal data or government-related data. The proposed CISA security requirements for restricted transactions would apply to classes of restricted transactions identified in regulations issued by the Department of Justice (DOJ).

DATES: Written comments are requested on or before November 29, 2024.

ADDRESSES: You may send comments, identified by docket number CISA–2024–0029, through the Federal eRulemaking Portal available at *http://www.regulations.gov.*

Instructions: All comments received will be posted to *https://www.regulations.gov,* including any personal information provided. For detailed instructions on sending comments and for information on the types of comments that are of particular interest to CISA, see the ''Public Participation'' and ''Request for Public Input'' heading of the **SUPPLEMENTARY INFORMATION** section of this document. Please note that this notice and request