of which would constitute a clearly unwarranted invasion of personal privacy.

Name of Committee: Division of Intramural Research Board of Scientific Counselors, NIAID.

Date: December 9–11, 2024.

Time: 8:00 a.m. to 10:15 a.m.

Agenda: To review and evaluate personnel qualifications and performance, and competence of individual investigators.

Address: National Institute of Allergy and Infectious Diseases, National Institutes of Health, Building 50, Conference Room 1227/1233, 50 Center Drive, Bethesda, MD 20892.

Contact Person: Laurie Lewallen, Committee Manager, Division of Intramural Research, National Institute of Allergy and Infectious Diseases, National Institutes of Health, Building 33, Room 1N24, 33 North Drive, Bethesda, MD 20892, 301–761–6362, *Laurie.Lewallen@nih.gov*.

(Catalogue of Federal Domestic Assistance Program Nos. 93.855, Allergy, Immunology, and Transplantation Research; 93.856, Microbiology and Infectious Diseases Research, National Institutes of Health, HHS)

Dated: October 10, 2024.

Lauren A. Fleck,

Program Analyst, Office of Federal Advisory Committee Policy.

[FR Doc. 2024–23836 Filed 10–15–24; 8:45 am]

BILLING CODE 4140–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

National Institute on Drug Abuse; Notice of Closed Meetings

Pursuant to section 1009 of the Federal Advisory Committee Act, as amended, notice is hereby given of the following meetings.

The meetings will be closed to the public in accordance with the provisions set forth in sections 552b(c)(4) and 552b(c)(6), title 5 U.S.C., as amended. The grant applications and the discussions could disclose confidential trade secrets or commercial property such as patentable material, and personal information concerning individuals associated with the grant applications, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

Name of Committee: National Institute on Drug Abuse Special Emphasis Panel; Microglial Pathophysiology in Comorbid Substance Use Disorder (SUD) and HIV.

Date: November 5, 2024.

Time: 2:00 p.m. to 3:00 p.m.

Agenda: To review and evaluate grant applications.

Address: National Institute of Health, National Institute on Drug Abuse, 301 North Stonestreet Avenue, Bethesda, MD 20892.

Meeting Format: Virtual Meeting.

Contact Person: Meysam Yazdankhah, Ph.D., Scientific Review Officer, Scientific Review Branch, Office of Extramural Policy, National Institute on Drug Abuse, NIH, 301 North Stonestreet Avenue, MSC 6021, Bethesda, MD 20892, (301) 402–6965, *meysam.yazdankhah@nih.gov*.

Name of Committee: National Institute on Drug Abuse Special Emphasis Panel; Mechanistic Studies on Social Behavior in Substance Use Disorder.

Date: November 19, 2024.

Time: 11:00 a.m. to 4:00 p.m.

Agenda: To review and evaluate grant applications.

Address: National Institute of Health, National Institute on Drug Abuse, 301 North Stonestreet Avenue, Bethesda, MD 20892.

Meeting Format: Virtual Meeting.

Contact Person: Caitlin Elizabeth Angela Moyer, Ph.D., Scientific Review Officer, Scientific Review Branch, Office of Extramural Policy, National Institute on Drug Abuse, NIH, 301 North Stonestreet Avenue, MSC 6021, Bethesda, MD 20892, (301) 443–4577, *caitlin.moyer@nih.gov*.

Name of Committee: National Institute on Drug Abuse Special Emphasis Panel; High Priority HIV and Substance Use Research.

Date: November 20, 2024.

Time: 11:00 a.m. to 5:00 p.m.

Agenda: To review and evaluate grant applications.

Address: National Institute of Health, National Institute on Drug Abuse, 301 North Stonestreet Avenue, Bethesda, MD 20892.

Meeting Format: Virtual Meeting.

Contact Person: Trinh T. Tran, Ph.D., Scientific Review Officer, Scientific Review Branch, Office of Extramural Policy, National Institute on Drug Abuse, NIH, 301 North Stonestreet Avenue, MSC 6021, Bethesda, MD 20892, (301) 827–5843, *trinh.tran@nih.gov*.

(Catalogue of Federal Domestic Assistance Program Nos. 93.277, Drug Abuse Scientist Development Award for Clinicians, Scientist Development Awards, and Research Scientist Awards; 93.278, Drug Abuse National Research Service Awards for Research Training; 93.279, Drug Abuse and Addiction Research Programs, National Institutes of Health, HHS)

Dated: October 10, 2024.

Lauren A. Fleck,

Program Analyst, Office of Federal Advisory Committee Policy.

[FR Doc. 2024–23837 Filed 10–15–24; 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; request for comment.

SUMMARY: The Cybersecurity Division (CSD) within the Cybersecurity and Infrastructure Security Agency (CISA) requests feedback on draft Product Security Bad Practices guidance. Additionally, CISA requests input on analysis or approaches currently absent from the guidance.

DATES: Written comments are requested on or before December 2, 2024. Submissions received after the deadline for receiving comments may not be considered.

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 *http://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 *http://www.regulations.gov.*

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

SUPPLEMENTARY INFORMATION:

I. Public Participation

Interested persons are invited to comment on this notice by submitting written data, views, or arguments using the method identified in the aforementioned **ADDRESSES** section. All members of the public including, but not limited to, specialists in the field, academic experts, members of industry, public interest groups, and those with relevant economic expertise are invited to comment.

II. Background

In line with CISA's Secure by Design initiative, software manufacturers should ensure security is a core consideration from the onset of software development. CISA's draft, voluntary

Product Security Bad Practices guidance provides 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.

By choosing to follow the recommendations in the draft guidance, manufacturers will signal to customers that they are taking ownership of customer security outcomes, a key secure by design principle.

CISA strongly encourage all software manufacturers to avoid the product security bad practices included in the Product Security Bad Practices guidance. The Product Security Bad Practices guidance is co-sealed with the Federal Bureau of Investigation.

III. List of Topics for Commenters

CISA seeks comments on the draft Product Security Bad Practices guidance, in the following three categories. Note: the categories are explained in detail in the draft guidance itself, available at *https://www.cisa.gov/resources-tools/resources/product-security-bad-practices.*

1. Product properties, which describe the observable security-related qualities of a software product itself. Listed bad practices are:

a. A new product line is developed using a memory unsafe language or the manufacturer does not publish a memory safety roadmap by January 1, 2026.

b. The product includes user-provided input directly in the raw contents of a SQL database query string.

c. The product includes user-provided input directly in the raw contents of an operating system command string.

d. The product includes default passwords.

e. The product contains, at the time of release, a component with an exploitable vulnerability present on CISA's Known Exploited Vulnerabilities (KEV) Catalog.

f. The product uses open-source software components that have critical known exploitable vulnerabilities.[1]

2. Security features, which describe the security functionalities that a product supports. Listed bad practices are:

a. The baseline version of the product does not support multi-factor authentication.

b. The baseline version of the product does not make audit logs available.

3. Organizational processes and policies, which describe actions taken by a software manufacturer to ensure strong transparency in its approach to security. Listed bad practices are:

a. The organization fails to publish Common Vulnerabilities and Exposures (CVEs) with Common Weakness Enumerations (CWEs) in a timely manner (or at all).

b. The organization fails to publish a vulnerability disclosure policy.

CISA also welcomes comments on other areas or approaches currently absent from the guidance.

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. 2024–23869 Filed 10–15–24; 8:45 am]

BILLING CODE 9111–LF–P

DEPARTMENT OF HOMELAND SECURITY

[Docket Number DHS–2024–0028]

Agency Information Collection Activities: Office of the Immigration Detention Ombudsman (OIDO) Intake Form, DHS Form 405, OMB Control No. 1601–0030

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 December 16, 2024. This process is conducted in accordance with 5 CFR 1320.1

ADDRESSES: You may submit comments, identified by docket number Docket # DHS–2024–0028, 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–2024–0028. 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: The Department of Homeland Security's (DHS) Office of the Immigration Detention Ombudsman (OIDO) is an independent office tasked with resolving individual complaints from or about individuals in immigration detention regarding the potential violation of immigration detention standards or other potential misconduct. OIDO was established by Congress (sec. 106 of the Consolidated Appropriations Act, 2020, Pub. L. 116–93).

DHS Form 405—''Case Intake Form'' is intended for use by individuals wishing to submit a complaint to OIDO. Information collected will provide the office with details about the allegations the submitter seeks to have OIDO address. DHS is revising the information collection to refine several questions in Form 405 and to include an additional form, ''Privacy Waiver Authorizing Disclosure to a Third Party''. Information collected on the ''Privacy Waiver Authorizing Disclosure to a Third Party'' will allow OIDO to disclose permitted information to a third party, such as the detained individual's relatives and/or representatives.

The information collected on Form 405—''Case Intake Form'' allows OIDO to identify: (1) the individual submitting the complaint and their contact information; (2) the detained individual who is the subject of the complaint; (3) the government-owned or contracted facility where the individual is or was detained and for how long; and (4) relevant details about the complaint. All of this information will be used by OIDO to investigate, resolve, and if appropriate, provide redress.

Based on usability testing recommendations, DHS is revising Form 405. The form will be shortened by reducing extraneous sections, such as Question 12a (Category), Question 12b

[1] A critical vulnerability is one that has an Attack Vector of ''network,'' Privileges Required of ''None,'' does not require user interaction, and has a ''high'' impact on at least two of the Confidentiality, Integrity, and Availability loss vectors.