TOTAL ESTIMATED ANNUALIZED BURDEN HOURS

Form name	Number of respondents	Number of responses per respondent	Total responses	Average burden per response (in hours)	Total burden hours
Eligible Applications	215	1	215	1.00	215.00
Institution/Loan Repayment Employment Form	*215	1	215	1.00	215.00
Authorization to Release Information Form	215	1	215	0.25	53.75
Disadvantaged Background Form	215	1	215	0.20	43.00
Total	860				526.75

* Respondents for this form is the institution on behalf of the applicant.

Maria G. Button,

Director, Executive Secretariat.

[FR Doc. 2023–25317 Filed 11–15–23; 8:45 am]

BILLING CODE 4165–15–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

National Institute of Neurological Disorders and Stroke; Notice of Meeting

Pursuant to section 1009 of the Federal Advisory Committee Act, as amended, notice is hereby given of a meeting of the National Advisory Neurological Disorders and Stroke Council.

The meeting will be partially open to the public as indicated below. Individuals who plan to participate and need special assistance, such as sign language interpretation or other reasonable accommodations, should notify the Contact Person listed below in advance of the meeting.

The meeting will be partially 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 Advisory Neurological Disorders and Stroke Council.

Date: February 14–15, 2024.

Open: February 14, 2024, 10:00 a.m. to 4:00 p.m.

Agenda: Report by the Director, NINDS; Report by the Director, Division of Extramural Activities; and Administrative and Program Developments.

Open session will be videocast from this link: https://videocast.nih.gov/watch=52772.

Closed: February 14, 2024, 4:00 p.m. to 5:30 p.m.

February 15, 2024, 9:30 a.m. to 12:30 p.m.

Agenda: To review and evaluate grant applications.

Place: National Institutes of Health, 6001 Executive Boulevard, Room 1131, Rockville, Maryland 20852 (Virtual Meeting).

Contact Person: David Owens, Ph.D., Director of Extramural Activities (Acting), National Institute of Neurological Disorders and Stroke, NIH 6001 Executive Blvd., 5th Floor, MSC 9531, Bethesda, MD 20892, (301) 496–9248, *owensd@ninds.nih.gov.*

Any interested person may file written comments with the committee by forwarding the statement to the Contact Person listed on this notice at least 10 days in advance of the meeting. The statement should include the name, address, telephone number and when applicable, the business or professional affiliation of the interested person.

Information is also available on the Institute's/Center's home page: *www.ninds.nih.gov,* where an agenda and any additional information for the meeting will be posted when available.

(Catalogue of Federal Domestic Assistance Program Nos. 93.853, Clinical Research Related to Neurological Disorders; 93.854, Biological Basis Research in the Neurosciences, National Institutes of Health, HHS.)

Dated: November 7, 2023.

David W. Freeman,

Supervisory Program Analyst, Office of Federal Advisory Committee Policy.

[FR Doc. 2023–25260 Filed 11–15–23; 8:45 am]

BILLING CODE 4140–01–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA–2023–0001]

Agency Information Collection Activities: Request for Comment on Secure Software Development Attestation Common Form

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

ACTION: 30-Day notice and request for comments.

SUMMARY: The Cyber Supply Chain Risk Management (C–SCRM) Program Management Office (PMO) 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 and clearance. CISA previously published this information collection request (ICR) in the **Federal Register** on April 27, 2023, for a 60-day public comment period. 110 comments were received by CISA. The purpose of this notice is to allow additional 30-days for public comments.

DATES: Comments are encouraged and will be accepted until December 18, 2023.

ADDRESSES: Written comments and recommendations for the proposed information collection should be sent to *www.reginfo.gov/public/do/PRAMain.* Find this information collection by selecting ''Currently under Review—Open for Public Comments'' or by using the search function.

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.

This process is conducted in accordance with 5 CFR 1320.10.

FOR FURTHER INFORMATION CONTACT: Shon Lyublanovits, 888–282–0870, *central@cisa.dhs.gov.*

SUPPLEMENTARY INFORMATION:

I. Background

In response to incidents such as the Colonial Pipeline and Solar Winds attacks, on May 12, 2021, President Biden signed Executive Order 14028 [1] on *Improving the Nation's Cybersecurity.* This order outlines over 55 actions [2] federal agencies need to take to improve cybersecurity. These actions range from developing strategies for critical software use to directly removing certain software products that do not comply with revamped standards. The objective of the executive order is to bolster the cybersecurity of federal systems. This Executive order addresses seven key points:

- Remove barriers to cyber threat information sharing between government and the private sector
- Modernize and implement more robust cybersecurity standards in the Federal Government
- Improve software supply chain security
- Establish a Cybersecurity Safety Review Board
- Create a standard playbook for responding to cyber incidents
- Improve detection of cybersecurity incidents on Federal Government networks
- Improve investigative and remediation capabilities

Section 4 of the E.O. observed, ''The development of commercial software often lacks transparency, sufficient focus on the stability of the software to resist attack, and adequate controls to prevent tampering by malicious actors.'' To address these concerns, the Executive Order required the National Institute of Standards and Technology (NIST) to issue guidance including standards, procedures, or criteria to strengthen the security of the software supply chain.

To put this guidance into practice, the Executive Order, through the Office of Management and Budget (OMB), requires agencies to only use software provided by software producers who can attest to complying with Federal Government-specified secure software development practices, as described in NIST Special Publication (SP) 800–218 Secure Software Development Framework.[3] OMB implemented this requirement through OMB memorandum M–22–18 dated September 14, 2022.[4] Specifically, M–22–18 requires agencies to ''obtain a self-attestation from the software producer before using the software.'' (Enhancing the Security of the Software Supply Chain through Secure Software Development Practices, Page 6, Sep. 14, 2022)

A copy of the current draft of the self attestation form is available at *https://www.cisa.gov/resources-tools/resources/secure-software-self-attestation-common-form.*

On June 9, 2023, OMB subsequently updated M–22–18 with M–23–16, ''Update to Memorandum M–22–18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices.'' M–23–16 states that ''Agencies must collect attestations for critical software subject to the requirements of M–22–18 and this memorandum no later than three months after the M–22–18 attestation common form released by the Cybersecurity and Infrastructure Security Agency (CISA) (hereinafter 'common form') is approved by OMB under the Paperwork Reduction Act (PRA). Six months after the common form's PRA approval by OMB, agencies must collect attestations for all software subject to the requirements delineated in M–22–18, as amended by this memorandum.'' (Update to Memorandum M–22–18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices, page 2, June 9, 2023) Per M–22–18, as amended by M–23–16, this requirement applies to agencies' use of software developed after the effective date of M–22–18 (Sep. 14, 2022), as well as use of existing software that is modified by major version changes after the effective date of M–22–18 (September 14, 2022). CISA's common self-attestation form does not preclude agencies from adding agency-specific requirements to the minimum requirements in CISA's common self-attestation form. However, any agency specific attestation requirements, modification and/or supplementation of these common forms will require clearance by OMB/OIRA under the PRA process and are not covered by this notice.

II. Responses

CISA received 110 comments in response to the 60-day public notice for the secure software self-attestation common form which concluded the 26th of June 2023. Comments can be found at *regulations.gov* under docket number CISA–2023–0001.[5] Summaries of the comments and CISA responses can be found at: *www.reginfo.gov/public/do/PRAMain.* Find this information collection by selecting ''Currently under Review—Open for Public Comments'' or by using the search function. As result of public comment, CISA has changed the draft self attestation common form described in the 60-day notice in the following manner:

- Added the citations to the appropriate NIST Guidance under ''What is the Purpose of Filling out this form'' to now read: ''to issue guidance ''identifying practices that enhance the security of the software supply chain.'' The NIST Secure Software Development Framework (SSDF), SP 800–218, and the NIST Software Supply Chain Security Guidance (these two documents, taken together, are hereinafter referred to as ''NIST Guidance'') include a set of practices that create the foundation for developing secure software.'' ''
- Included references to M–23–16 throughout.
- Under ''What is the Purpose of Filling out this Form?'' edited the ''and'' to ''or'' in the list of software that requires self-attestation.
- Edited the software products and components that are not in scope for M–22–18, as amended by M–23–16, and do not require self attestation to now read:

1. ''Software developed by Federal agencies;
2. Open source software that is freely and directly obtained by a federal agency; or
3. Software that is freely obtained and publicly available.''

This aligns with M–23–16. This changes is also reflected in the Form on page 8.

- Under ''Filling Out the Form,'' added ''When the software producer chooses to verify conformance with the minimum requirements by a certified FedRAMP Third Party Assessor Organization (3PAO) or other 3PAO approved in writing by an appropriate agency official, the software producer must attach the assessment in lieu of a signed attestation. The 3PAO must use relevant NIST Guidance, which

[1] *https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.*

[2] *https://www.natlawreview.com/article/2021-cybersecurity-recap-government-contractors-and-what-to-expect-2022-part-1-4.*

[3] *https://doi.org/10.6028/NIST.SP.800-218.*

[4] *https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf.*

[5] *https://www.federalregister.gov/documents/2023/04/27/2023-08823/agency-information-collection-activities-request-for-comment-on-secure-software-development.*

includes all elements outlined in this form, as part of the assessment baseline. To rely upon a third-party assessment, the software producer must check the appropriate box in Section III and attach the assessment to the form. The producer need not sign the form in this instance.''

• Modified language under ''Additional Information'' to clarify that an agency may still use the producer's software if the producer identifies the practices to which they cannot attest, documents practices they have in place to mitigate associated risks, and submits a plan of actions and milestones (POA&M) to the agency.

• Added additional language (in italics) under ''Additional Information'' to include: ''Software producers may be asked by agencies to provide additional attestation artifacts or documentation, such as a Software Bill of Materials (SBOMs) or documentation from *a certified FedRAMP third party assessor organization (3PAO) or other 3PAO approved in writing by an appropriate agency official*.''

• Under ''Additional Information,'' removed ''If the relevant software has been verified by a certified FedRAMP third party assessor organization (3PAO) or other 3PAO approved in writing by an appropriate agency official, and the assessor used relevant NIST guidance, the software producer does not need to submit a signed attestation. However, relevant documentation from the 3PAO is required.''

• Moved the minimum attestation reference to the appendix.

• Added ''Version 1.0'' to the form.

• Added ''Revised Attestation'' in the case of necessary corrections or edits.

• In Section I, on page 8, added that additional pages can be attached to the attestation if more lines are needed to appropriately list all relevant products.

• Removed Product Line from Type of Attestation due to confusion. Product line presents problem such as when a new product is added. Also removed ''product line'' in the file name structure example on page 3.

• Modified the language on page 8 to now read: ''Note: In signing this attestation, software producers are attesting to adhering to the secure software development practices outlined in Section III.'' This clarifies the practices to which software producers are attesting.

• Removed First Name, Last Name and modified to just Name.

• Under Requirement #2 in Section III, modified to remove redundancies and now reads: ''The software producer has made a good-faith effort to maintain trusted source code supply chains by employing automated tools or comparable processes to address the security of internal code and third-party components and manage related vulnerabilities.'' This modification is also reflected in the reference table in the appendix.

• Removed duplicative requirement previously listed under 3). This modification is also reflected in the reference table in the appendix.

• Modified minimum requirement regarding provenance to now read: ''The software producer maintains provenance for internal code and third-party components incorporated into the software.'' This modification is also reflected in the reference table in the appendix.

• Modified minimum requirement regarding security vulnerabilities to now read:

○ ''(4) The software producer employs automated tools or comparable processes that check for security vulnerabilities. In addition:

(a) The software producer operates these processes on an ongoing basis and, at a minimum, prior to product, version, or update releases;

(b) The software producer has a policy or process to address discovered security vulnerabilities prior to product release; and

(c) The software producer operates a vulnerability disclosure program and accepts, reviews, and addresses disclosed software vulnerabilities in a timely fashion and according to any timelines specified in the vulnerability disclosure program or applicable policies.''

A redundant ''and'' was removed under section 4(a). These modifications are also reflected in the reference table in the appendix.

• Added ''To the best of my knowledge'' after ''I attest'' in both instances in the attestation section (Section III).

• Modified signature line to clarify signature of CEO or COO is acceptable; it now reads: ''Signature of CEO or COO and Date (YYYY–MM–DD).'' This modification is also reflected in the instructions on page 3.

• Added ''OR'' between CEO signature and 3PAO certification option and modified ''I attest that the referenced software has been verified by a certified FedRAMP Third Party Assessor Organization (3PAO) or other 3PAO approved in writing by an appropriate agency official has evaluated our conformance to all elements in this form'' to ''A certified FedRAMP Third Party Assessor Organization (3PAO) or other 3PAO approved in writing by an appropriate agency official has evaluated our conformance to all elements in this form. The 3PAO used relevant NIST Guidance, which includes all elements outlined in this form, as the assessment baseline. The assessment is attached.''

• Under Attachment(s) removed: ''Please check the appropriate boxes below, if applicable: There are addendums and/or artifacts attached to this self-attestation form, the title and contents of which are delineated below the signature line. I attest the referenced software has been verified by a certified FedRAMP Third Party Assessor Organization (3PAO) or other 3PAO approved in writing by an appropriate agency official, and the Assessor used relevant NIST Guidance, which includes all elements outlined in this form, as the assessment baseline. Relevant documentation is attached.''

• Removed ''Title of Individual signing on behalf of the organization.''

Analysis

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

Title: Secure Software Development Attestation.

OMB Number: 1670–NEW.

Frequency: Annually.

Affected Public: Business-Software Producers.

Estimated Number of Respondents per Initial Submission: 16,688.

Estimated Number of Respondents per Resubmission: 8,344.

Estimated Number of Responses per Respondent per Initial Submission: 3.

Estimated Number of Responses per Respondent per Resubmission: 1.

Estimated Time for Initial Submission per Respondent: 3 hours and 20 minutes.

Estimated Time for Resubmission per Respondent: 1 hour and 50 minutes.

Total Annualized Hours for Initial Submission: 83,432 hours.

Total Annualized Hours for Resubmission: 7,647 hours.

Estimated Number of Respondents per POA&M Development: 14,105.

Estimated Number of Responses per Respondent per POA&M Development: 1.

Estimated Time for POA&M Development per Respondent: 6 Hours.

Total Annualized Hours for POA&M Development: 84,630 hours.

Estimated Cost to Public: $13,264,954.

Robert J. Costello,

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

[FR Doc. 2023–25251 Filed 11–15–23; 8:45 am]

BILLING CODE 9110–9P–P