This document is scheduled to be published in the
Federal Register on 04/27/2023 and available online at
federalregister.gov/d/2023-08823, and on **govinfo.gov**

9110-9P

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: 60-Day Notice and request for comments; New collection (Request for a new OMB Control Number).

SUMMARY: In accordance with the requirements of the Paperwork Reduction Act (PRA) of 1995, the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security (DHS), is soliciting public comment on a self-attestation form to be used by software producers in accordance with the Executive Order on Improving the Nation's Cybersecurity and the Office of Management and Budget's guidance in OMB M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*. In accordance with OMB M-22-18, Section III.C, CISA has agreed to serve as steward for this collection. After obtaining and considering public comment, CISA will prepare the submission requesting clearance of this collection as a Common Form to permit other agencies beyond DHS to use this form in order to streamline the information collection process in coordination with OMB.

DATES: Comments are encouraged and will be accepted until **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].**

ADDRESSES: You may submit comments, identified by docket number Docket # CISA-2023-0001, at:

- Federal eRulemaking Portal: https://www.regulations.gov. Please follow the instructions for submitting comments.

Instructions: All submissions received must include the agency name and docket number Docket # CISA-2023-0001. All comments received will be posted without change to https://www.regulations.gov, including any contact information provided.

Docket: For access to the docket to read background documents or comments received, go to https://www.regulations.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 E.O. 14028,[1] Improving the Nation's Cybersecurity. This order outlines over 55 actions. 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, Enhancing Software Supply Chain Security, 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

[1] 86 FR 26633, available at https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

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.[2] OMB implemented this requirement through OMB memorandum M-22-18 dated September 14, 2022.[3] Specifically, M-22-18 requires agencies to "obtain a self-attestation from the software producer before using the software." This requirement applies to new software developed after the date of memo issuance (September 14, 2022) as well as existing software that is modified by major version changes after the date of memo issuance. OMB M-22-18 brings into existence a new and sizeable conformity assessment community. The memorandum introduces conformity assessment expectations and activities for the supply chain starting with the software producer and ending with the federal agency putting the software in to use. 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. Invitation to Comment

The following analysis of the burden associated with this proposed information collection is specific to DHS as the agency sponsoring the common form. For the purposes of estimating the number of respondents, DHS has made the following assumptions and welcomes comments on all assumptions.

[2] Nat'l. Institute of Standards & Tech., SP 800-218, Secure Software Development Framework (SSDF) Version 1.1 (2002), available at https://csrc.nist.gov/publications/detail/sp/800-218/final.

[3] Off. of Mgmt. & Budget, Exec. Off. of the President, M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices (2022), available at https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf.

1. DHS is assuming vendors would have 2,689 initial form submissions and 1,345 resubmissions of the form, due to major software changes, per year. This estimate applies across DHS, including all component agencies. DHS based this estimate on initial contract award data for Fiscal Years 2019 through 2022 from DHS's Federal Procurement Data System (FPDS). DHS utilized data for contract awards that could, in the future, include a response to this collection based on FPDS Product and Service Code (PSC) of "D" Automatic Data Processing and Telecommunication and "R" Professional, Administrative and Management Support.

   Time burden for the attestation form includes time to review the form and understand requirements, gather information, review, and approve the release of information and submission. DHS assumes a three-hour burden per initial submission[4] for a software quality assurance analyst or tester and an additional 20 minutes per initial submission for a Chief Information Security Officer (CISO). Vendors would have to resubmit the attestation form for major software changes, and DHS assumes half the number of initial submissions will result in a resubmission. DHS assumes that resubmissions would take 1 hour and 30 minutes for a software quality assurance analyst or tester and retains 20 minutes for a CISO. DHS acknowledges the information collection request allows for a vendor to use a prior submitted form for multiple agencies. DHS welcomes public comment on how frequently this might happen and how to reduce respondent burdens due to his collection, where feasible.

[4] DHS based the estimated 3 hours on an information collection request related to contractor information security for certain telecommunications and video surveillance services or equipment. While not exactly the same requirements or scope, DHS found the burdens of 0199 collection to be similar to the burden in this proposed new collection. For more information, see Supporting Statement for OMB Control Number 9000-0199. https://www.reginfo.gov/public/do/PRAViewDocument?ref_nbr=202009-9000-002

To estimate opportunity costs, DHS uses an hourly compensation rate of $67.90 for a software quality assurance analyst or tester and $177.66 for a CISO.[5] DHS estimates software quality assurance analyst or tester annual hours would be 10,084 for initial and resubmissions by multiplying $67.90 compensation rate to estimate the opportunity cost of $684,733. DHS estimates CISO annual hourly burden of 1,345 hours and multiplying $177.66 compensation rate to a CISO estimate the opportunity cost of $238,890. DHS combines these two opportunity costs to calculate a total opportunity cost for the collection of $923,623.

2. DHS is assuming if a vendor needs to provide any additional attestation artifacts or documentation, including a Software Bill of Materials (SBOMs), that this information would be readily available and would not have to be generated specifically for doing business with the government. DHS is interested in comments on the burden and costs if SBOMs or additional artifacts materials need to be generated or reformatted to fulfill an agency/component request.
3. For the purposes of this initial collection, DHS is proposing the common form be a fillable/fileable PDF form. Vendors could access the form on the DHS/CISA website and submit via the DHS website OR email the completed form to CSCRM_PMO@cisa.dhs.gov. Other agencies will be required to seek approval to

[5] DHS uses wage estimates based on Bureau of Labor Statistics (BLS) Occupational Employment Statistics (OES). Within NAICS industry 541500 - Computer Systems Design and Related Services, DHS uses mean hourly wage rates for Software Quality Assurance Analysts and Testers (SOC 15-1253) at $47.09 and Chief Executives (11-1011) at $123.21. DHS applies a compensation factor of 1.44191 based on total hourly compensation of $67.64 divided by $46.91 wages/salaries for Private Industry Workers Management, Professional, and Related Occupations Sources:
https://www.bls.gov/oes/2021/may/naics4_541500.htm (BLS, OES: May 2021 National Industry Specific Occupational Employment and Wage Estimates.)
BLS, Employer Cost for Employment Compensation (ECEC Table 4)):
https://www.bls.gov/news.release/archives/ecec_03172023.htm (released March 17, 2023).

use the common form by submitting their agency-specific burden and cost analyses to OMB.

Input is requested on any aspect of the proposed common form including the instructions. DHS/CISA is particularly interested in

1. If the proposed collection of information to implement requirements of both the EO and the OMB guidance will have practical utility;
2. If DHS has accurately estimated the burden of the proposed collection of information, including the validity of the methodology and assumptions used;
3. Other ways for DHS to enhance the quality, utility, and clarity of the information to be collected; and
4. How DHS could 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: SECURE SOFTWARE DEVELOPMENT ATTESTATION

OMB Control Number: [INSERT DHS/CISA 4 DIGIT PREFIX THEN XXX]

Type of Review: Request for a new OMB Control Number, New Common Form

Expiration Date of Approval: NOT APPLICABLE

Frequency**:** ANNUALLY

Affected Public: BUSINESS – SOFTWARE PRODUCERS

Estimated Number of Respondents: 2,689

Estimated Number of Responses per Respondent: 1.5

Estimated Number of Responses: 4,034

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 Burden Hours for Initial Submissions: 8,963 hours

Total Annualized Burden Hours for Resubmissions: 2,466 hours

Total Annualized Burden Hours: 11,429 hours

Total Annualized Respondent Opportunity Cost: $923,623

Robert J. Costello,
Chief Information Officer,
Department of Homeland Security,
Cybersecurity and Infrastructure Security Agency.
[FR Doc. 2023-08823 Filed: 4/26/2023 8:45 am; Publication Date: 4/27/2023]