2101 Wilson Boulevard, Suite 700, Arlington, VA 22201-3060 • (703) 522-1820 • (703) 522-1885 Fax • NDIA.org

December 18, 2023

Robert J. Costello
Chief Information Officer
Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

Electronic Submission: www.reginfo.gov/public/do/PRAMain, *Docket No. CISA-2023-0001*

Re: Request for Comment on Secure Software Development Attestation Common Form

Dear Mr. Costello:

The National Defense Industry Association (NDIA) appreciates the opportunity to provide feedback in response to the Cybersecurity and Infrastructure Security Agency (CISA) request for comment on the Secure Software Development Attestation Common Form (Common Form).

NDIA is the nation's oldest and largest defense industry association, representing nearly 1,750 corporate and over 65,500 individual members from small, medium, and large contractors, a majority of which are small businesses. Our members engage daily with the federal government's national and homeland security apparatuses. They are well-versed in the array of cybersecurity requirements and standards across the Federal Government.

NDIA members highlight the lack of revision to this draft from the initial Common Form draft, especially considering the number of issues raised in the initial public comment period. NDIA would reiterate our original comments and concerns filed on June 26, 2023. Without addressing these and other issues, the Administration risks increasing costs for software and hardware products operated by software due to the increased risks and liabilities imposed on the government vendor community. NDIA is further concerned that many companies, particularly small businesses that may not have the legal or monetary resources to analyze and implement these requirements fully, are at risk of creating legal jeopardy for themselves through government enforcement mechanisms like the Department of Justice Civil-Cyber Fraud Initiative.

Further, there was an apparent lack of coordination between CISA, the Office of Management and Budget (OMB), the General Services Administration (GSA), and others regarding the timing of the release of the form and implementation guidance and the deadlines they set. GSA released guidance requiring software attestation in their acquisition efforts, but it preceded OMB's release of Memorandum M-22-18, both of which preceded the release of the Common Form. This lack of alignment necessitated OMB Memorandum M-23-16 to clarify the promulgation sequence of the form, guidance, compliance requirements, and deadlines. However, whether these misalignment and communications issues between implementing agencies have been resolved is unclear.

2101 Wilson Boulevard, Suite 700, Arlington, VA 22201-3060 • (703) 522-1820 • (703) 522-1885 Fax • NDIA.org

This version of the Common Form requires a signature from either the software producer's Chief Executive Officer (CEO) or Chief Operating Officer (COO). The government should consider allowing the CEO and/or COO attestation duties to be delegated to another senior management official (partner/principal) with cognizant authority over federal projects. In a large organization, particularly a partnership organization/LLP, the CEO or COO may find it difficult to attest to every software development project on time.

In addition to these concerns, NDIA would like to request clarification for the three questions proposed below:

1. Configurations for tax and audit modeling commercial off-the-shelf (COTS) products typically involve adjusting existing parameters, importing client-specific data, or selecting predefined calculation methods and formulas. However, these configurations do not alter the core functionality or security settings of the software.

    a. Can the government clarify whether COTS products with only minor configurations that do not involve security settings adjustments, such as tax and audit modeling tools, fall within the scope of the NIST Secure Software Development Framework?

2. The form requires a self-attestation for software “to whose code the producer delivers continuous changes,” such as software-as-a-service products.

    a. When must a producer provide a self-attestation for this type of software?

        i. When the software is first provided? Each time the software changes? Some other point?

3. Can the government clarify what constitutes sufficiency for attestation purposes concerning third-party products?

Conclusion

NDIA appreciates the opportunity to provide additional feedback and requests for clarification to the Common Form. NDIA and its industry partners look forward to continuing an open and collaborative dialogue on developing the Secure Software Development Attestation Common Form and its application to government acquisition activities. Thank you again for the opportunity.

Sincerely,

National Defense Industrial Association