December 15, 2023

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

VIA ELECTRONIC SUBMISSION

Re: Request for Comment on Secure Software Self-Attestation Common Form

Dear Mr. Costello:

The Alliance for Digital Innovation (ADI) appreciates the opportunity to submit this letter to the Cybersecurity and Infrastructure Security Agency (CISA) in response to its draft Secure Software Self-Attestation Common Form (hereafter, the Self-Attestation Form), released on November 16, 2023.

ADI is a non-partisan alliance that advocates for the removal of institutional and bureaucratic barriers to the operation of a modern digital government. Our members provide key critical technologies to the federal government, including cloud infrastructure, digital identity solutions, human resources software, quantum computing, digital services, and a range of sophisticated cybersecurity tools and services.

We submit this letter to urge CISA to make several key changes to its Self-Attestation Form before issuing its final draft. We explain our proposed changes in detail below:

1. Provide Self-Attestation Form Exemptions for CSPs with FedRAMP Authorization to Operate (ATO)

ADI believes that the creation of new secure software development attestation requirements that are not harmonized with FedRAMP unduly burdens Cloud Service Providers (CSPs) with additional compliance requirements. Accordingly, ADI encourages CISA to provide Self-Attestation Form exemptions to CSPs on products for which they have already obtained a FedRAMP ATO. The FedRAMP program has a robust already has set of processes and procedures in place to evaluate the security of cloud offerings using certified Third-Party Assessor Organization (3PAO).

ADI would highlight that current FedRAMP requirements address most of the controls referenced in the Self-Attestation Form. Moreover, FedRAMP ATOs are already widely understood and used by stakeholders in both federal agencies and industry.

ADI acknowledges that providing such exemptions would likely require some modifications to FedRAMP requirements. However, these modifications would substantially reduce the burden of the collection of information, which CISA highlighted as a key concern in its Request for Comment.

2. Remove the Requirement for a CEO or COO's Signature

ADI believes that requiring a Chief Executive Officer (CEO) or Chief Operating Officer (COO) to sign the Self-Attestation Form poses a significant logistical burden to software producers. Large multinational companies with thousands of products may find it unfeasible to acquire a CEO or COO's signature for each individual product or product line.

Therefore, ADI encourages CISA to allow CEOs to identify appropriate designees to sign the form on behalf of their organization. This would ensure that the software producer can deliver the Self-Attestation Form in a timely manner.

3. Establish a more realistic burden estimates

ADI appreciates the government's interest in identifying realistic burdens on industry for complying with this requirement. Unfortunately, the current estimates significantly under-estimate the time and cost impacts. In order to verify compliance with these new requirements organizations must establish processes to identify, collect, and analyze evidence of compliance before they can recommend the Self-Attestation Form is signed. Generally, this will include individuals from product development, compliance, government affairs, and legal. ADI members estimate that this could take anywhere from 200-2000 hours per software product. ADI recommends CISA update the estimates for the burden on software producers to collect and analyze the information necessary to complete this form.

4. Protection of submitted information

ADI is concerned that Self-Attestation Forms or other artifacts that may be requested by agencies could include business sensitive and/or proprietary information. We recognize it is incumbent upon companies to properly mark any business sensitive information which they may provide to the government. ADI recommends that CISA provide guidance to agencies regarding the safeguarding of such information.

ADI appreciates the ability to submit these comments for CISA's consideration. As CISA continues its efforts to improve secure software development, ADI stands read to provide any additional insight or feedback.

Sincerely,

The Alliance for Digital Innovation