



December 10, 2023

Robert J. Costello
Chief Information Officer
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
245 Murray Lane
Washington, D.C. 20528-0380

Subject: Comments on Secure Software Development Attestation Common Form

Docket #: CISA-2023-0001

Document Number: 2023-25251

Publication Date: November 16, 2023

Fiery, LLC. appreciates the opportunity to comment on the Secure Software Development Attestation Common Form released by the Cybersecurity and Infrastructure Security Agency (CISA).

By way of background, Fiery, LLC. provides Digital Front End (DFE) technology for production and industrial printers. Fiery designs and manufactures DFEs for specific print hardware manufacturers (OEMs), including, Xerox, Canon, and Ricoh, among many others, providing custom computer hardware loaded with software - including software needed to interpret, render, and design files into color-separated images that the printer can produce. Fiery also provides a range of workflow software products for digital printing used to streamline and automate various digital print prepress and production tasks. Fiery OEM partners sell commercial print services and products to the US Federal Government under their own brand.

Fiery, LLC outlines herein a few questions about the proposed secure software self-attestation form that appear ambiguous or not clear.

Thank you for your time and consideration. If you have any questions, I may be reached at al.soto@fiery.com or **(510) 557-5023**

Al Soto / Product Management
Fiery, LLC



Fiery, LLC

6453 Kaiser Drive
Fremont, CA 94555
United States
Tel +1 650 357 3500
www.fiery.com

Questions

1. For software **developed** after September 14, 2022. Please define “developed”. We need to know if the development timeline applies to the start or to the end of the development cycle. For example, a new *software application* started development on January 1, 2022, and was completed on October 1, 2022. Is Self-Attestation required for this software application?
2. For products sold under OEM agreements; please provide clarification as to which company should be listed as the software producer. The developer of the application or the OEM that licensed the product from the developer of the application.
3. For products sold under OEM agreements; please clarify which date is considered the Release/Publish Date. For example, is it the date the software manufacturer declares the product released? or the date the OEM partner release the product?
4. Is the Release/Publish Date in the table found on Section I of the self-attestation form an optional field?
5. If the software producer is using third-party software under a Non-Disclosure Agreement (NDA) and/or a Master Service Agreement (MSA); is the software producer responsible to provide the self-attestation letter and SBOM for such third-party software? or the vendor who provides the third-party software is responsible for it?
6. Is there an official government form required when submitting a plan of actions and milestones (POA&M) for seeking exceptions to certain software that cannot be self-attested before the deadline?
 - 6.1. What is the process for seeking such exceptions?

