MANIFEST

Request for Comment on Secure Software Development Attestation Common Form

Cybersecurity and Infrastructure Security Agency
Federal Register #2023-25251
FR Citation 88 FR 78759
Docket # CISA-2023-0001

18 December 2023

Organization name, address, and country of business:
Manifest Cyber, Inc.
8 Riverview Road
Westport, CT 06880 USA
http://www.manifestcyber.com

Company representative:
Mike McDonel, Director of Business Operations
mike@manifestcyber.com
+1 419 439-8972

Introduction

Manifest is a software supply chain security company that helps organizations understand and reduce the cybersecurity risk in the technologies they produce and procure. Our flagship product is a software-as-a-service platform that leverages software bills of material (SBOMs), artificial intelligence bills of materials (AIBOMs), Vulnerability Exploitability eXchange (VEX) documents, and security attestations to harden our nation's software supply chain. By managing this content with Manifest, users can analyze risk in internally-developed or third-party tools and take steps to reduce that risk.

Manifest is grateful for the opportunity to address this timely and necessary Request for Information (RFI). Our response explores the most effectives steps that CISA can take to secure our nation's software supply chain.

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;

We believe that software supply chain transparency is, in principle, a valuable initiative. Software supply chain vulnerabilities are - by some accounts - increasing by some 700% year over year and costing billions of dollars in damages, lost productivity, and opportunity cost to other important initiatives. Executive Order 14028, OMB Memos M-22-18 and M-23-16, and other legislation recognize the importance of securing the software supply chains of our defense and federal civilian enterprises.

That being said, collecting attestations is only as useful as what the agencies will do with that information subsequently. In our professional opinion, SSDACF can be most impactful when certain criteria are met:

1) **Automated Submission.** The process of submitting attestations is automated to reduce burden on software vendors;
2) **Automated Collection and Review.** Federal agencies have SSDACF platforms and tooling in place to automate the receipt and review of these artifacts
3) **Combination with Software Bills of Materials (SBOMs)**. We believe that SBOMs should be required as mandatory artifacts to support and demonstrate a vendor's secure software development practices. SBOM capabilities have proliferated to the point where virtually every modern software vendor utilizing industry-standard CI/CD pipelines or software composition analysis (SCA) tooling can generate SBOMs quickly and affordably,

and the SBOMs themselves offer a window into vulnerabilities, outdated software components, and license issues within a software application.

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;

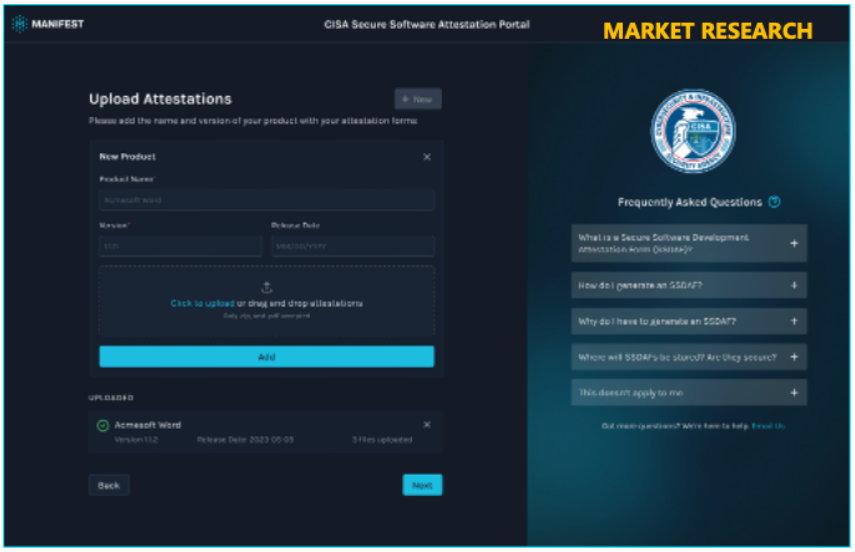
We believe that CISA is underestimating the burden of the proposed *manual* collection of SSDACF information. While most software vendors will have only a handful of products and SSDACF artifacts to submit, larger vendors will considerably skew both the estimated time for initial submission per respondent and estimated time for resubmission per respondent.

For instance, a single Fortune 500 technology company that we are familiar with will have on the order of 500+ SSDACFs to submit. Considering the demands on that organization's CEO or COO, simply signing 500+ artifacts is likely to take whole person-days per year.

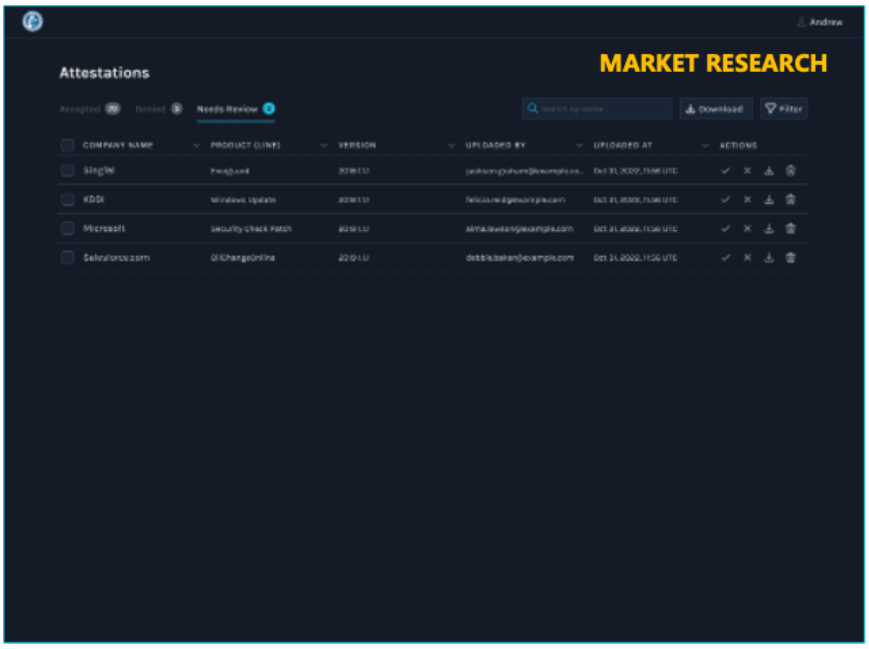
Providing an *automated and centralized* portal through which vendors can manage their submissions and provide bulk attestations and updates will be vital to limiting the burden on software vendors. It is critical that any such portal have two components:

1) A vendor component, whereby vendors can create SSDACF artifacts, manage their submissions, digitally sign their artifacts, and easily modify existing submissions
2) An agency component, whereby agencies can accept/reject submissions, request clarification from vendors, and catalog compliance/artifact expiration.

The SSDACF portal should not be built from scratch. Commercial software will be less expensive, more performant, more scalable, more maintainable, and delivered faster. Manifest has already invested in creating such a portal using exclusively FedRAMP High components and deployable into CISA's AWS VPC, as shown below:



The vendor component, whereby vendors upload and manage their SSDACF artifacts



The agency component, whereby SSDACF artifacts are reviewed by agency personnel and accepted/rejected and monitored for expiration/refresh

3: Enhance the quality, utility, and clarity of the information to be collected;

If CISA is going to undertake the considerable investment in requiring software supply chain attestations, those artifacts should be treated as a valuable dynamic resource rather than static

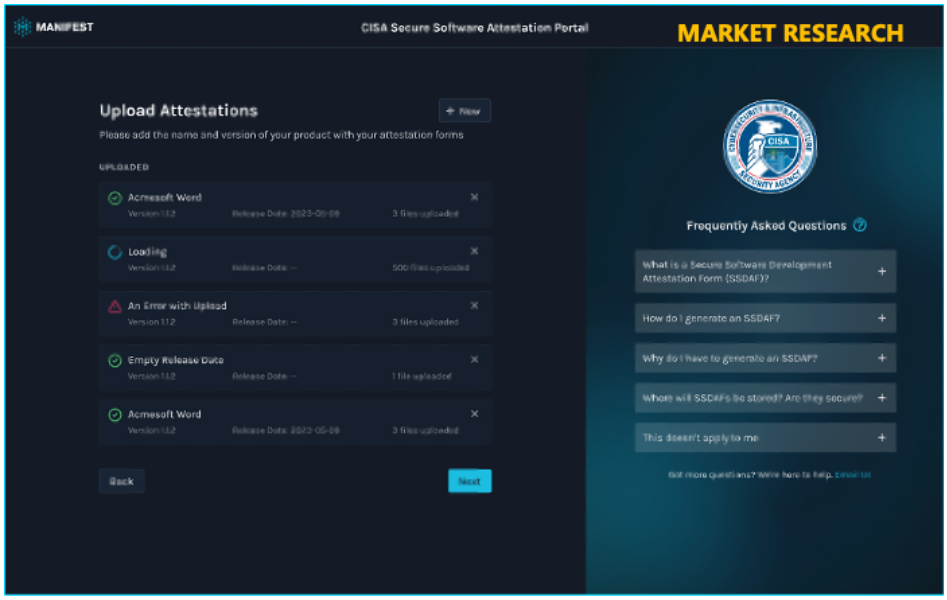
compliance artifacts. SSDACFs should also be used in conjunction with other CISA-backed software supply chain best practices, specifically software bills of materials (SBOMs) and Vulnerability Exploitability eXchange (VEX) documents. The SSDACF capability should be able to seamlessly operate with an SBOM and VEX management platform. The combination of information gleaned from SSDACFs, SBOMs, VEX documents, and other attestations will ensure that CISA has a more complete picture of the risks present within our nation's software supply chain.

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

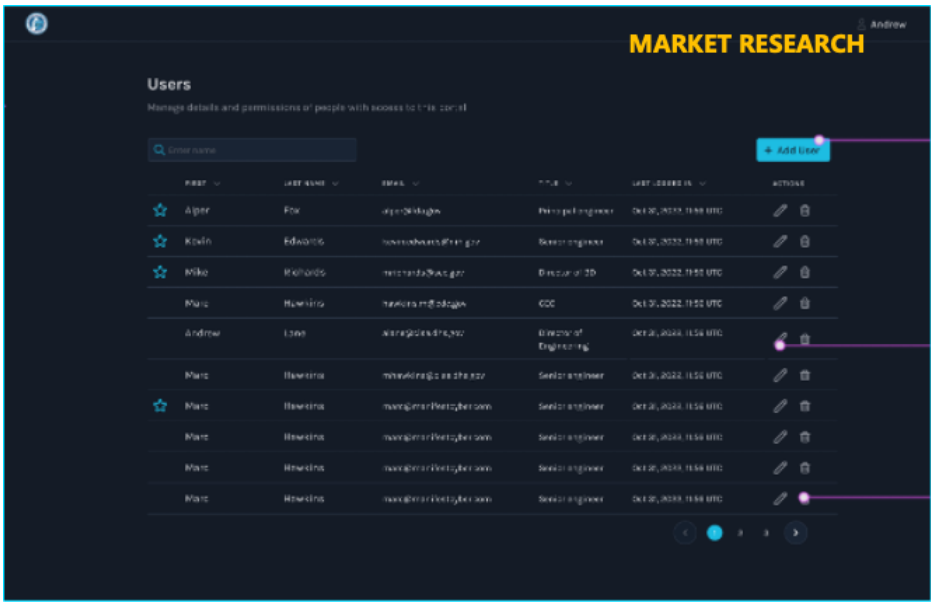
The broader U.S. government, led by CISA, will significantly reduce the burden of collecting, analyzing, and actioning SSDACF attestations by investing in a secure portal to manage the SSDACF collection process. The portal should be able to programmatically solicit SSDACF documents from software producers who are required to provide them and store them securely. This approach will minimize the burden on the USG personnel who will oversee the collection of the attestations and will streamline the submission process for software producers.

Such a platform would considerably reduce the burden on vendors, as it would:

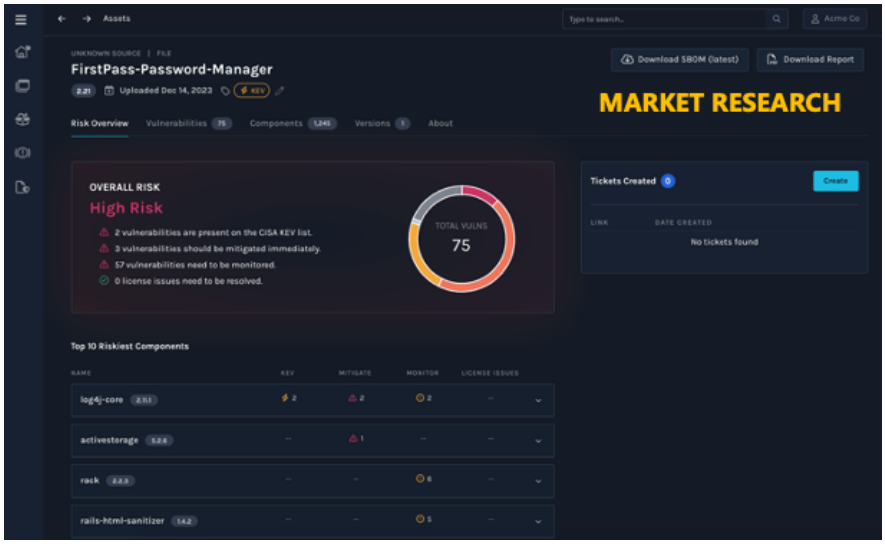
1) Allow vendors to create, sign, manage, update, and delete their submissions in a self-service manner without engaging agency personnel;
2) Accommodate SBOM upload, and have an agency-facing SBOM analytic capability to afford agencies an automated review of a submitted SBOM in CycloneDX or SPDX format;
3) Preserve user access and privileges to ensure that only agency personnel with authorization are permitted to access a given SSDACF or supplemental artifact, and that those artifacts can be shared directly with federal civilian executive branch agencies directly from the portal.



A vendor's ability to manage their attestations in a self-service manner is essential



Users should be managed within the platform for security and access control



The platform should seamlessly incorporate vendor SBOM analysis to validate the claims made in the SSDACF artifact

Conclusion

Secure software development initiatives are an important, valuable step toward securing the software supply chains of the United States and its agencies. If CISA approaches the SSDACF management process with an emphasis on efficient generation, collection, and analysis of these artifacts in conjunction with SBOM and VEX capabilities as described in this response, we believe CISA will be poised to leverage that content for meaningful action when new cybersecurity threats emerge.