



Promoting Innovation Worldwide

Shalanda D. Young  
Director  
Office of Management and Budget  
Executive Office of the President  
1650 Pennsylvania Avenue, NW  
Washington, DC 20503

November 21, 2022

Dear Director Young,

The Information Technology Industry Council<sup>1</sup> (ITI) writes to request additional clarity around memorandum M-22-18. The memorandum is an important milestone in achieving the government's objective of securing the software development process. Yet, software producers face significant barriers, including ambiguous terminology, confusing timelines, and the potential for regulatory fragmentation.

Currently, there is no standard FAR clause or contract requirement that directs industry to comply with OMB M-22-18. The memo directs individual agencies to request information from suppliers, but we are concerned that these requests will be applied differently across the government, and even within agencies. This creates ambiguity and may ultimately delay progress towards the government's important software security goals.

To be effective, the federal government should adopt a harmonized approach across all agencies, provide clear pathways for the reuse of existing artifacts, processes, and certifications, and also define appropriate timelines for stakeholder implementation of attestation requirements. We believe the best way to achieve the government's goal of establishing repeatable, scalable processes that support the adoption of securely developed software is through the established regulatory process under the Administrative Procedure Act. To support the effective and consistent implementation of the government's cybersecurity objectives, we call upon OMB to use its role in establishing cross-government objectives and timelines for the rollout of secure software development lifecycle requirements to maximize harmonization and built-in flexibility while software producers work to comply with new guidance on short notice.

To these ends, we respectfully suggest the recommendations detailed below for OMB's consideration:

- **Clarify the mandate to leverage one standardized form for all agencies with the option to request addendums for mission-unique needs.** This will streamline the process across agencies and ensure consistency in agencies' interpretation of what constitutes an in-scope request for this attestation form and maximize the utility of attestations submitted by software producers beyond single-agency use cases. We

---

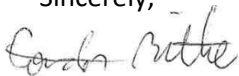
<sup>1</sup> The Information Technology Industry Council (ITI) is the premier global advocate for technology, representing the world's most innovative companies. We promote public policies and industry standards that advance competition and innovation worldwide. Our diverse membership and expert staff provide policymakers the broadest perspective and thought leadership from technology, hardware, software, services, and related industries.

encourage OMB to use its central role in the process to encourage harmonization around the proposed attestation form to the fullest extent possible, until longer term requirements are developed through the FAR process.

- **Discourage agencies from requiring artifacts until SBOMs are scalable and consumable.** We recognize and appreciate the value of flexibility built into the OMB process. Given the current level of (im-)maturity, we believe that SBOMs are not suitable contract requirements yet. The SBOM conversation needs more time to move towards a place where standardized SBOMs are scalable for all software categories and can be consumed by agencies. At this time, it is premature and of limited utility for software producers to provide an SBOM. We ask that OMB discourage agencies from requiring artifacts until there is a greater understanding of how they ought to be provided and until agencies are ready to consume the artifacts that they request.
- **Adjust the implementation timeline to allow for a standardized rollout through the established regulatory process under the Administrative Procedure Act.** This will remove interdependencies from the current timeline which is contingent on the timely release of a viable standardized attestation form to be operationalized across all in-scope agencies. Ideally, the implementation timeline will match that of FAR Case 2023-002 which will require software producers to comply with, and attest to complying with, applicable secure software development requirements per Section 4.n of Executive Order 14028.
- **Consider piloting the collection of attestations and artifacts per M-22-18 prior to mandating them.** This will produce helpful insights into the types of issues that may arise for agencies and software producers throughout the implementation process. Such lessons learned would help inform further streamlining efforts through rulemaking or otherwise.
- **Leverage the overlap with existing processes to the greatest extent possible to avoid the introduction of additional complexity.** Re-using established processes will expedite the adoption process and have a positive effect on standardizing the attestation process across agencies. The underlying NIST Guidance already maps controls to some existing standards. These efforts should be expanded to also include international standards and department-specific programs.

Thank you for your consideration of our recommendations. Both ITI and its members stand ready to engage with the government through the rulemaking process or otherwise to ensure these requirements are implemented consistently and according to commercial best practices. If you would like to discuss this letter in more detail, please contact Leopold Wildenauer at [lwildenauer@itic.org](mailto:lwildenauer@itic.org).

Sincerely,



Gordon Bitko  
Executive Vice President of Policy, Public Sector  
Information Technology Industry Council (ITI)

## Harmonization

We appreciate that industry was consulted repeatedly throughout the formulation process of the underlying NIST guidance. We believe that the government will benefit from continuing to consult stakeholders on the issuance of related guidance. While M-22-18 is addressed to federal agencies, there will be immediate downstream implications for software producers. Keeping in mind statutory authorities, the requirements for contractors will need to be defined through rulemaking. Amending the Federal Acquisition Regulation (FAR) will ensure regulatory harmonization, provide standardized guidance for federal contracting officials, and remove barriers for software producers to demonstrate their compliance.

## Standard Forms and Practices

There are benefits to adopting one standardized form across all federal agencies. As currently written, there is much room for how agencies may interpret M-22-18 which could fragment the government's approach to ensuring secure software development practices on federal networks. The memorandum does not mandate the use of one standardized form across all agencies. If agencies decide not to wait for the standardized form to become available, they risk an uncoordinated rollout that could proliferate reporting requirements and create confusion within agencies and industry with no additional benefits to software security. M-22-18 outlines minimum elements but does not specify the level of detail that agencies will request from software producers to demonstrate compliance. It is unclear whether software producers will be asked to attest to general policies and procedures or demonstrate how they meet specific requirements within the SSDF matrix, which would likely vary across different products. Relatedly, it is still unclear whether the attestation will apply at the product/service level or at the enterprise level.

A better way would mandate the use of one standardized form for all agencies with the option to request addendums for mission-unique needs. The software producer's responses to the baseline form and any agency-specific addendums should be reusable across agencies and collected at the highest level possible such that they would not contain sensitive information. Agencies should limit the development of an addendum or requesting additional artifacts to cases where a heightened level of program risk is present. They should also reference existing questions from the baseline form and other agencies' addendums to avoid duplication of work. Relying on one standardized form would also streamline this information collection under the Paperwork Reduction Act as it would make it easier for OIRA to review and approve the form. Moreover, collecting high-level attestations would have the added benefit of increasing software producers' willingness to post attestations publicly as is the case with high-level ISO certifications.

## Align Implementation Timeline to Match Rulemaking under FAR Case 2023-002

There is currently no standard FAR clause or contract requirement that directs industry to comply with OMB M-22-18. Instead, the memo directs individual agencies to request information from suppliers. It is the FAR Council's mandate – not OMB's – to implement NIST guidance as contractual requirements binding contractors and it is the FAR Council's actions that will ultimately have significant impacts on the current roadmap to implement M-22-18. It is unclear whether OMB or individual agencies have the statutory authority to require self-attestation from federal contractors in the absence of a new FAR clause or contractual amendment. We worry that agencies will invest

scarce resources to adopt bespoke requirements that will become obsolete once the FAR guidance becomes available.

As currently written, OMB M-22-18 adopts a phased roll out, beginning with agency-level collections before developing government-wide capacities. Agencies are directed to start collecting attestation forms for critical software in central agency systems 270 days after publication of the memo. However, GSA, OMB, and CISA will not establish the program plan for a government-wide repository for software attestations and artifacts until one year after the publication of the memo. This repository is not expected to assume full operational capability until September 2024. Having collection requirements but no centralized and secure solution to protect sensitive and proprietary materials will force each agency to create ad-hoc solutions which, inevitably, will lead to inconsistencies throughout the federal government. There must be a solution in place for protecting this sensitive information before mandating its collection. The work to have such a system is not trivial – both at an agency and even more so as a centralized solution. We worry that agencies will invest scarce resources to adopt bespoke requirements that will become obsolete once the FAR guidance becomes available.

We believe the government will achieve better outcomes if it requires the collection of conformance statements after the establishment of a government-wide standardized process and harmonizes the requirements across all agencies through the established regulatory process under the Administrative Procedure Act. The memo states that the Federal Acquisition Regulatory Council “plans to propose rulemaking on the use of a uniform standard self-attestation form.” In fact, the FAR Council recently opened FAR Case 2023-002 entitled *Supply Chain Software Security*. We expect that these updates will have a substantial impact on how agencies will apply the memo’s requirements. We see great value in using the regulatory process to harmonize the implementation of secure software development practices across all agencies and believe that this will avoid wasting precious resources on agency-specific efforts that will necessarily have to be rolled back anyway once the standardized FAR language becomes effective

### Reuse

We support the memo’s decision to accept existing artifacts to determine a software producer’s adherence to secure software development practices. Existing processes should be leveraged to the greatest extent possible to avoid the introduction of additional complexity. This will have a positive effect on standardizing the attestation process across agencies. Clarifying what existing attestations will be deemed acceptable will help software producers and plan for additional steps needed to demonstrate their compliance with the underlying NIST guidance. The reuse of artifacts should be encouraged to the greatest extent possible. The SSDF already maps controls to some existing standards like NIST SP 800-53 and SP 800-161. This mapping should serve as a basis for the reuse of supporting artifacts across cybersecurity schemes. These harmonization efforts should be expanded to include international standards like the ISO/IEC 20243, 27001, and 27002, and department specific efforts like the Department of Defense’s (DoD) Cybersecurity Maturity Model Certification (CMMC), or the Cloud Computing Security Requirements Guide (CC SRG).

To facilitate the reuse of attestations and artifacts within and across agencies, it would be helpful for OMB to issue additional guidance on the federal information sharing efforts. OMB M-22-18 contemplates a formal program that would centrally house artifacts and attestations across in-scope agencies. We believe that the GSA would be a viable place to stand up such a program and

be tasked with operating a shared repository of compliant providers. We will note, however, that this repository should be separated from the Federal Risk and Authorization Management Program (FedRAMP) repository as it will include significantly more software solutions than the 286 cloud service offerings that are currently authorized. Relatedly, if a vendor intends to sell the same software to multiple agencies, the process should be standardized to eliminate the need to provide multiple attestation forms. Likewise, if a vendor sells software through a government-wide acquisition contract (GWAC) or federal supply schedule, there should be no requirement to submit more than one attestation form. In fact, requiring multiple forms contradicts the purpose of shared services, which are intended to streamline the acquisition process of commodity products and services.

### Cloud Software

For cloud service offerings (CSOs), we recommend the reuse of artifacts produced in support of authorizations to operate (ATOs) awarded through FedRAMP within GSA. FedRAMP is currently conducting the final review of updating the baselines to reflect Revision 5 of SP 800-53. It is still unclear how products would be handled for the purposes of M-22-18 if they are FedRAMP certified pre-the latest guidance. We encourage OMB to explore how existing processes can be leveraged to the greatest extent possible to support M-22-18 implementation. Specifically, we believe that FedRAMP Joint Authorization Board (JAB) and agency ATOs provide a sufficiently high level of assurance for the certified cloud service offering.

Cloud service providers (CSPs) already submit significant security artifacts as part of participating in the FedRAMP program. Leveraging the existing process and accreditation structure would be the path of least resistance for agencies to access the necessary information for certified CSOs and should eliminate the need to require additional self or third-party attestation. Furthermore, the FedRAMP program management office publishes a list of authorized CSOs on the FedRAMP Marketplace. An authorization listing on the FedRAMP marketplace should be considered as meeting the public attestation requirement from M-22-18 and should automatically be approved for use by all agencies. If this is not feasible, any additional attestation requests should be limited to the control delta.

### Non-Cloud Software

For software offerings that are not based in the cloud, we similarly encourage OMB to explore alternative, less disruptive methods to provide Government visibility into secure software development details. We encourage the reuse of established processes to the greatest extent possible whenever they serve an equivalent function. For example, the SSDF specifically indexes the Building Security in Maturity Model (BSIMM), which industry already uses and has commercial assessments to support. We recommend that OMB explore how BSIMM assessments can be leveraged as a means of self-attestation. We also believe that there is merit in looking at established IT data reporting systems. Specifically, existing IT Service Management (ITSM) applications may be appropriate to offer precise insights into ongoing production processes. Businesses rely on ITSM to ensure that their processes are running correctly and efficiently. Some ITSM solutions can be used to demonstrate compliance to industry standards. These tools could be repurposed to create just-in-time reports on how a software producer meets the requirements from the underlying NIST guidance.

## Terminology and Implementation

We appreciate that the memorandum retains a certain level of ambiguity as this gives the producers and consumers of software the necessary agency and wiggle room to make risk-based decisions. At times, however, this ambiguity may inadvertently delay progress towards the government's important software security goals. Below, we identify areas where we see a need for additional clarity.

### Scope

M-22-18's exemption for agency developed software risks prolonging the use of potentially inconsistent and unsecure software development practices. We believe the SSDF and the NIST Software Supply Chain Security Guidance offer sound best practices for securing the software development lifecycle regardless of the systemic context in which any specific software was developed. We were surprised by the decision to exclude agency developed software from these requirements and believe that it should be corrected.

In fact, exempting agency developed software seems to only introduce additional complexity with no clear benefit to securing government networks. For example, consulting solutions that are offered to Federal Agencies fall into an unclear grey area. How will consulting solutions be treated per the OMB Memo? Would software developed under contract with a Federal Agency qualify for an exemption from attestation requirements? How should situations be handled in which consulting services entail fixes of software developed by third parties or software maintenance (module specific solutions)? Would these also fall under the exemption from attestations?

The federal government will achieve better and more secure outcomes if it applies the underlying NIST guidance to all software, including agency-developed software. Bringing agency-developed software into scope would also have the added benefit of building trust with industry partners. If the requirements apply without exceptions, public and private software producers will be incentivized to safeguard centrally aggregated information. This will help with the facilitation of secure information sharing between software producers and their partners in business and mission.

### SBOMs and Artifacts

Unfortunately, and despite year-long efforts on the part of government and industry, SBOMs are not yet suitable contract requirements. In fact, there are currently multiple efforts underway in Congress and the Executive Branch that focus on the utilization of SBOMs. Similarly, currently available industry tools create SBOMs of varying degrees of complexity, quality, completeness. The presence of multiple, at times inconsistent or even contradictory, efforts suggests a lacking maturity of SBOMs. This is further evident in a series of practical challenges related to implementation, including naming, identification, scalability, delivery and access, the linking to vulnerability information, as well as the applicability to cloud services, platforms and legacy software. These challenges make it difficult to effectively deploy and utilize SBOMs as a tool to foster transparency. The SBOM conversation needs more time to mature and move towards a place where SBOMs are scalable and consumable.



The definition of “artifacts” is unclear and could cover a wide range of asks. For example, it could include anything from design documents to static analysis results to architectural risk analysis writeups. These are not only proprietary, but they may – and do – contain information that creates in some cases unmitigable risk for suppliers. For example, static analysis results may contain information about as-yet unfixed, and therefore exploitable, security bugs. This could inadvertently introduce new risks, including increased risk for zero-day exploits and risks to intellectual property and patent infringement. We are understandably concerned about the security of sensitive proprietary information that may be collected and held by federal agencies. It is therefore critical to clarify the definition of artifacts and what protections will be afforded to safeguard sensitive information. We encourage OMB to use its central role in managing the attestation process to encourage harmonization around the use of artifacts. This includes encouraging agencies to limit requests for complementary artifacts to situations with unique security needs. It also entails deferring artifact requests for mechanisms like SBOM where development work is underway through CISA and other agencies.

#### Requirement Flow Down

The memorandum explicitly states that “agencies are required to obtain a self-attestation from the software producer before using the software.” In line with this guidance, third parties should not be held liable for providing the attestation on behalf of the software producer.

As agencies complete the required inventory of software that is already in use, they should provide the respective vendors with an itemized list of identified software and identify software that has been assessed as “critical software.” This will help with the identification of the software producer who will be responsible to provide the conformance statement.

For all new acquisitions of products that use covered software developed by a third party, it would be helpful to have standardized contracting language that can be flowed down to the respective software producers. Additionally, to maximize the utility of attestations it would be useful to maximize the flexibility offered to software producers in terms of how attestations are provided—whether on a per-product basis, per-company basis, or across a subset of products. Ideally, the forthcoming FAR Case would provide such standardized language in addition to mandating the use of a standardized attestation form for all federal agencies. This will streamline the process of flowing down requirements to the responsible entities and provide those software producers with a uniform way to report their adherence to secure software development practices.

#### Major version change

The language around major version changes highlights the difficulty in moving from policy to implementation. In fact, the current approach potentially exposes software producers to vastly different requirements solely on the basis of semantics with no marginal benefit to product security. While a major change could be if the software version number goes from 2.5 to 3.0, there is no standard for how major versus minor version changes are implemented across products or software producers. Software producers use different versioning systems with regards to both nomenclature and timing. Furthermore, versioning is not always fully correlated with major changes in the way of clarifying vulnerability exploitability. We believe software producers should retain the ability to define when there has been a major software release. Alternatively, for software for which an attestation has already been provided suppliers could simply be required to

notify agencies if any of the statements made in the attestation became untrue. We are concerned that triggering requirements with the issuance of major version change could discourage some vendors from implementing updates that are helpful to ensuring security across the software development lifecycle.

There is no obvious answer to what should trigger an attestation for legacy software. We have explored alternative approaches, which we would like to share to inform further discussions. One way we discussed were fixed interval updates to legacy software. However, that can be challenging for embedded software and firmware that is used in devices with long life cycles. Another option we discussed was to tie the reporting requirement to the contract renewal cycle, but this also does not address the underlying problems to produce attestations for legacy software. Specifically, third party components that were produced before the release of the NIST guidelines may not come into compliance, or a major update may only have changed part of a piece of software while other parts were untouched. The POA&M process may be suitable to track legacy components and their phase out. The process should encourage transparency and help guide a collaborative risk discussion which may also require mitigations on the consumer's side. Over time, as software goes through more iterations and the ecosystem matures as a whole, the frequency of this should decrease naturally.

#### POA&Ms

We appreciate the flexibility to accept POA&Ms as they are an important tool to address temporary deficiencies that arise in complex, dynamic environments. Undoubtedly, there will be instances where POA&Ms will be an appropriate tool to address temporary deficiencies and we expect software producers to avail themselves of this tool. To produce the best outcomes, POA&Ms should be flexibly construed and facilitate risk discussions between producers and consumers of software. Given the sensitivity of the information contained in POA&Ms, it will be essential to assure the secure use and timely closure of POA&Ms.

M-22-18 states that “documentation provided in lieu of a complete self-attestation [...] shall not be posted publicly by the vendor or the agency.” Not posting sensitive information publicly is a necessary but insufficient step. Additional protections are needed to appropriately safeguard the sensitive information contained in POA&Ms. To that end, agencies should default to requesting only the information necessary to understand and address the temporary deficiency. Limiting the amount of sensitive information that is contained in POA&Ms is in line with the principle of data minimization. Moreover, the sensitive information contained within POA&Ms requires protection not only at rest but in transit as well. GSA and other implementing agencies should work with software producers to define these terms and conditions.

#### **Additional recommendations**

In addition to the recommendations above, we respectfully propose the following suggestions for your consideration. While currently missing from the memorandum, we believe that these recommendations will benefit the federal government on its journey towards securing the development and supply chain of federally consumed software.



### Pilot Program

We believe there is value in conducting a cost impact assessment and launching a pilot program before mandating the collection of additional requirements. Typically, in cases where there are new requirements or standards in place, such as NIST 800-218, government performs an impact assessment which includes an industry assessment of new requirements, the cost of implementation, and then assesses the current state of the regulatory footprint. This information then can be used to determine the “cost of compliance” and give participants clear guidance on areas of focus and prioritization. From the publicly available information, it is unclear in this case whether any of these baseline measures have been performed. We also believe there could be value for one or two agencies to pilot the effort on behalf of the federal government. Piloting the implementation would produce helpful insights into the types of issues that may arise for agencies and software producers throughout the implementation. Such lessons learned would help inform further streamlining efforts through rulemaking or otherwise.

### Involve Acquisition Workforce

OMB should update the guidance to clarify the acquisition workforce’s responsibilities in implementing M-22-18 requirements. While currently missing from the memo, the agency’s Chief Information Officer should consult with the agency’s Chief Acquisition Officer to inform the implementation process. This will help standardize the implementation process and expose where there might be a need for additional workforce training or skillset development and provide helpful clarification to drive greater harmonization and streamlining of processes across agencies.