SOFTWARE AQUISITION GUIDE FACT SHEET

WHAT IS THE SOFTWARE ACQUISITION GUIDE?

The level of transparency provided by suppliers of software and cyber-physical devices relative to their development and third-party management practices can make technology acquisitions challenging. While they may have a general understanding of the core cybersecurity requirements for a particular acquisition, acquisition staff often lack the ability to assess whether a given supplier has practices and policies in place that better meet the ongoing expectations of enterprise users of the products.

The Software Acquisition Guide aligns with the Cybersecurity and Infrastructure Security Agency's (CISA) Secure by Design principles but focuses on the "Secure by Demand" elements. By providing recommendations for agency personnel (including mission owners, contracting staff, or requirements offices), this guide allows acquisition professionals to engage in more relevant discussions with their enterprise risk owners (such as Chief Information Officers and Chief Information Security Officers) and candidate suppliers. These discussions should foster better risk-informed decisions for acquisition and procurement of software and cyber-physical products. The information and insights gathered from suppliers help raise the bar on cybersecurity transparency. The guide aligns with pre-existing work from the National Institute of Standards and Technology (NIST) and CISA, requirements from the Office of Management and Budget (OMB) and the General Services Administration (GSA), and requirements such as the CISA Secure Software Development Attestation Form (or agency-specific variations of that form).

SOFTWARE ASSURANCE (SwA) BACKGROUND

- **NIST Definition of Software Assurance:** The level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the lifecycle. **NIST Sources:** CNSSI 4009-2015 from DoDI 5200.44.
- **Framing:** Understanding the role SwA plays in information and communications technology (ICT) supply chain risk management (SCRM).
- **Goal:** Influence broader adoption and use of consistent and relevant SwA standards and guidelines in ICT SCRM by suppliers and consumers.

FREQUENTLY ASKED QUESTIONS

1. What is the purpose of the Software Acquisition Guide?

Many well-known cyber incidents have exploited vulnerabilities and weaknesses in software and within software supply chains; thus, software assurance spans both proprietary and open-source software and impacts both private sector and government enterprises.

Customers and mission owners, as often represented by their acquisition and procurement organizations, may use the guidance in the Software Acquisition Guide as a basis to describe, assess, and measure suppliers' cybersecurity practices relative to the software lifecycle and CISA Secure by Design principles without requiring that acquisition staff become cybersecurity experts.

The Software Acquisition Guide builds on existing U.S. government cybersecurity guidance to address four phases of software ownership: software development practices, supply chains, deployment, and vulnerability management. By focusing the Software Acquisition Guide on the procurement and acquisition process, customers can indicate that software suppliers' cybersecurity and Secure by Design practices are a key consideration, particularly for high assurance and medium assurance environments.

2. Who is the target audience for the Software Acquisition Guide?

This document has an intended audience of individuals in software acquisition roles supporting government agencies and suppliers of software.

3. Is there a tool to help me answer the questions in the Software Acquisition Guide?

Yes. A companion spreadsheet questionnaire complements the Software Acquisition Guide, and it can be used to expedite answering questions in the Software Acquisition Guide.

4. How should the Software Acquisition Guide be used?

This Software Acquisition Guide is intended to support ongoing dialogue between procurement officials, government security teams, and software suppliers to clarify the expectations, obtain transparency, and assess the security risks of a software product and determine its security suitability for the intended use. Agencies will potentially need to follow applicable procedures for information collection, such as compliance with the Paperwork Reduction Act (PRA), independently before they use the questionnaire with members of the public.

5. Can software suppliers use the Software Acquisition Guide?

Yes. Software suppliers should be able to describe the security controls used within their development environments, apply similar controls to their software supply chain, and provide guidance to software operators. The Software Acquisition Guide is a virtual "how-to" manual to help software suppliers properly implement key CISA Secure by Design principles and practices.

6. Can the Software Acquisition Guide be used by non-government procurers?

Yes. The Software Acquisition Guide and the companion spreadsheet can be used by anyone interested in reducing risks in their software supply chains, either internally or externally sourced. It provides insights on secure software development practices that could be used as evaluation criteria when considering prospective suppliers or products. As such, non-federal consumers could use the Software Acquisition Guide in their source selection activities to identify products which are or are not following NIST, Secure Software Development Framework (SSDF), and CISA Secure by Design principles and practices. Suppliers could use the Software Acquisition Guide to better understand consumer interests and to evaluate their own practices in mitigating risks in their software supply chains.

7. Can the Software Acquisition Guide be used to create a Plan of Action and Milestones (POA&M)?

Yes. The Software Acquisition Guide begins by focusing on Supplier Governance and Attestations and provides questions agency personnel, including mission owners and contracting staff or requirements officers, could use in communications with software suppliers to address software products. For suppliers, these conversations on security principles within the context of secure software lifecycle practices could serve as a basis for creating a POA&M for any unmet agency requirements.

8. Can the Software Acquisition Guide be used to create contract language and evaluation criteria?

Questions in the Software Acquisition Guide can be used by enterprise users to inform the structuring of contract language, procurement planning, and evaluation criteria to convey expectations more explicitly to candidate suppliers. Government procurements would still need to comply with applicable acquisition laws, regulations, and policies.

9. How does this relate to the ICT SCRM Task Force Vendor SCRM Template?

The Software Acquisition Guide was inspired by the Vendor SCRM Template but is exclusively focused on software.

10. How could the Software Acquisition Guide be used by resellers and contractors?

Resellers and contractors include a wide spectrum of businesses ranging from entities that simply distribute software to those that integrate multiple software components into a larger solution.

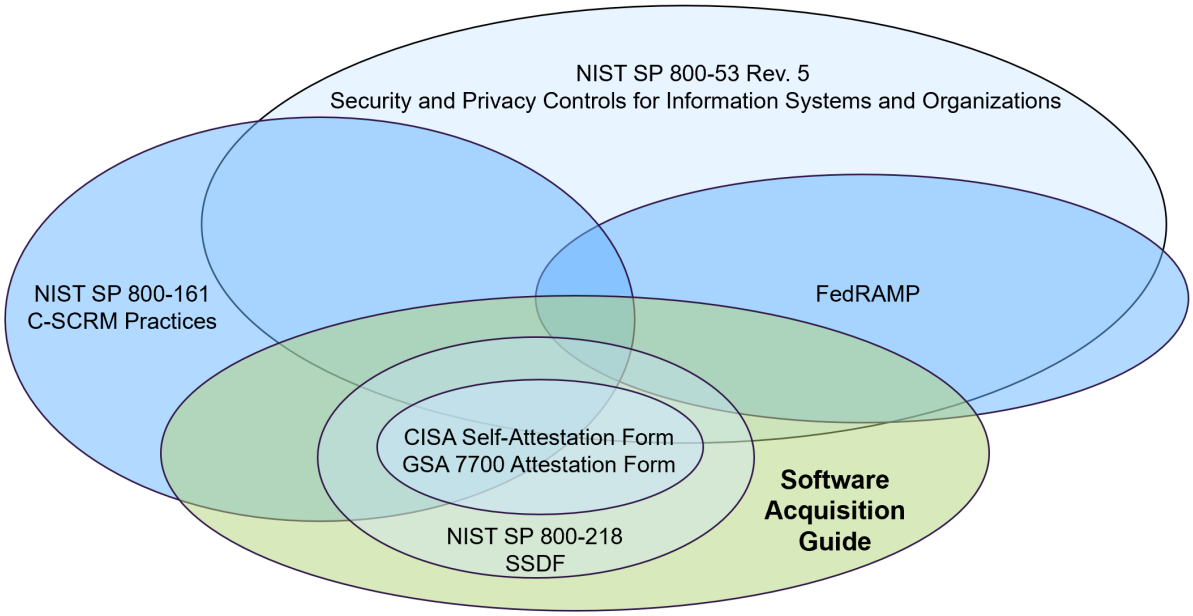
Prime contractors and system integrators could use the Software Acquisition Guide to help them determine if the software included in their solutions follows secure software development processes, and to help validate that their suppliers follow similar practices as those the contractor or integrator follow. Prime government contractors must still comply with the terms and clauses of each contract and flow-down clauses to their subcontracts as required by each government contract.

While marketplace resellers might not typically set any cybersecurity attestation or questionnaire requirements for software they resell, the Software Acquisition Guide could help resellers encourage integration of more mature SwA programs in their supplier communities.

Ultimately, it will be up to the parties to decide how they will use the Software Acquisition Guide questionnaire.

11. How does the Software Acquisition Guide relate to other software assurance guidance?

The ICT SCRM Task Force's Software Assurance Working Group leveraged existing guidance from NIST and CISA to influence the Software Acquisition Guide. This was done to create uniformity and reliability. The Task Force did not want to reinvent the wheel, but rather to build upon existing standards to foster consistency and compliance.



***Notional – Not to scale**

Figure 1: Notional Overlap of Major Cybersecurity Control Efforts

12. How does the Software Acquisition Guide relate to future Federal Acquisition Regulation (FAR) requirements?

Section 4(o) of EO 14028 instructs the FAR Council to require suppliers of software available for purchase by agencies to comply with, and attest to complying with, applicable secure software development requirements. These rules have yet to be published.

The scope of this guidance in the Software Acquisition Guide is broader than secure software development requirements. This guidance covers SwA during the design, development, deployment, and operational lifecycle of the software product that both software suppliers and customers can apply.

13. How does the Software Acquisition Guide relate to CISA Secure Software Development Attestation Form?

The CISA Secure Software Development Attestation Form identifies requirements from the NIST SSDF that are addressed in the Software Acquisition Guide. Entities that submit an attestation form to CISA may answer "yes" to CONTROL.GOV.01 within the Software Acquisition Guide, which then enables them to skip 25 additional control questions. Appendix E of the Software Acquisition Guide provides a mapping of all governance control questions and the control group questions that can be skipped based on affirmative answers to governance questions.

14. How does the Software Acquisition Guide align to OMB memos M-22-18 and M-23-16?

Careful consideration has been made to align to existing work from CISA, NIST, and requirements from OMB and GSA.

15. How does the Software Acquisition Guide relate to the Secure by Demand Guide?

Customer organizations can use both guides in procurement discussions with third-party resellers or service providers. Both guides can be used by software customers to generate the demand for more secure technology products. The Software Acquisition Guide covers the use of the CISA Secure Software Development Attestation Form, the use of a software bill of materials (SBOM), and all of NIST's Secure Software Development Framework plus additional measures that customers can leverage during procurement. The Secure by Demand Guide has some overlap with the Software Acquisition Guide, addressing Software Supply Chain Security with coverage for SBOMs and vetting security of open-source software, and it offers additional detailed questions not in the Software Acquisition Guide that should be considered by staff supporting U.S. government agencies and those incorporating third-party components in their software.

16. Does the use of a memory safe language change any recommendation in the Software Acquisition Guide?

No. The use of a memory safe language to create an application may address some element of risk within that application's development and lifecycle, but the programming language used is only one part of the SwA process. The use of a memory safe language in one application does not imply that one has a memory safe system.

17. What is the effort to complete the Software Acquisition Guide's questionnaire for small and medium-sized businesses (SMBs)?

It is conceivable that a small supplier with a small number of parties contributing to the Software Development Lifecycle (SDLC) process and a small software product could answer the entire set of governance questions within 10 staff hours, including research per product sold to the U.S. government. Some products will require more time and effort due to multiple factors including the number of third-party suppliers and products used, the total number of externally acquired components that contribute to the final product distributed to customers, and the number of SDLC teams involved in product manufacturing, design, development, and maintenance/distribution.

18. How does the completion effort for a larger organization compare to SMBs?

Larger organizations tend to have a significant quantity of applications. They also tend to standardize on development practices. For any organization that has reduced the number of independent development practices and policies, filling out the Software Acquisition Guide's questionnaire should not be any more significant than that of a medium-sized organization.