PUBLIC CONTRACTING INSTITUTE

Software Bill of Materials Requirements

Alexander W. Major, Esq.
Philip Lee, Esq.
May 4, 2023

PUBLIC CONTRACTING INSTITUTE

Who are we?

- Attorneys in the Government Contracts and Export Controls Group at McCarter & English
- Significant experience handling “bet the company” litigation, investigations and bid protests
- Clients range from Fortune 100 companies to small businesses
- Extensive experience in defense and civilian contracting across multiple industry sectors

Today's Agenda

- Introduction
- Executive Order 14028
- What is a Software Bill of Materials and what are its minimum elements
- Federal guidance regarding a Software Bill of Materials
- What is on the horizon for Software Bill of Materials

Introduction

What is a Software Bill of Materials (SBOM)?

"The term… means **a formal record containing the details and supply chain relationships of various components used in building software**… It is analogous to a list of ingredients on food packaging."

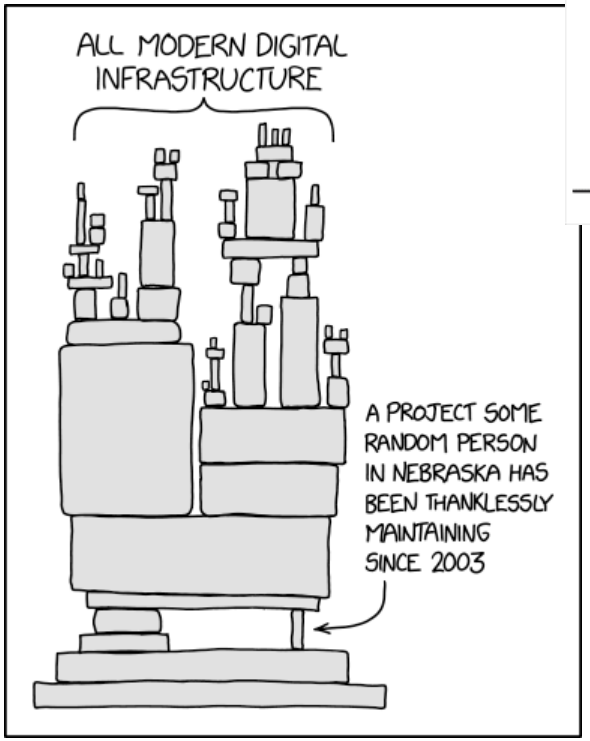
- *Improving the Nation's Cybersecurity*, Executive Order 14028, Section 10(j) May 12, 2021

Nutrition Facts

Serving Size 1 packet (28g)
makes 6-8 fl oz
Servings Per Container 10

Amount Per Serving	
Calories 110	Calories from Fat 10
	% Daily Value*
Total Fat 1g	**2%**
Saturated Fat 0.5g	**2%**
Cholesterol 0mg	**0%**
Sodium 150mg	**6%**
Total Carbohydrate 24g	**8%**
Dietary Fiber 1g	**3%**
Sugars 19g	
Protein 2g	

INGREDIENTS: SUGAR, NONFAT MILK, WHEY, PARTIALLY HYDROGENATED SOYBEAN OIL, COCOA PROCESSED WITH ALKALI, MARSHMALLOWS (SUGAR, CORN SYRUP, FOOD STARCH-MODIFIED, GELATIN, SODIUM HEXAMETAPHOSPHATE, ARTIFICIAL AND NATURAL FLAVORS, BLUE 1), CORN SYRUP SOLIDS, SODIUM CASEINATE, CARBOXYMETHYLCELLULOSE, SALT, ARTIFICIAL FLAVOR.



Bill of Material

Customer name: ABC Company
Customer adress: 10 Jane Avenue, New York
Date: 1/1/2010

Item #	Description	Vendor	Part Number	Quantity
1	FGHT sun model	MNF	GHY253	7
2	120 w photovoltaic module	Food FG	2543-I	14
3	Hardware	Mottle	1452-UKJ	2
4	4-module for GHN	IFS	256BN	1
5	822 air G	Mood plc	947673 IOL	4
6	SMA Model Sunny Boy Inverter	MNF	8 GH	2
7	9B, 700 GHT	IFS	f58	1
8	Fused Disconnect Switch	Food FG	56e	1

simplestudies.com

Improving the Nation's Cybersecurity, Executive Order (EO) 14028, May 12, 2021

Section 1, Policy: "The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors… Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. **The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace.**"

Improving the Nation's Cybersecurity, EO 14028, May 12, 2021 (Cont'd)

- **Section 2, Remove Barriers to Sharing Threat Information**: Remove barriers that exist in contract language and conditions and ensure service providers share cyber threats, incidents, and risks with appropriate agencies.
- **Section 3, Modernize Federal Government Cybersecurity**: Adopt security best practices, advancing toward a Zero Trust Architecture to secure cloud services.
- **Section 4, Software Supply Chain Security**: Increase transparency in commercial software development, focusing on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors, especially for ***"critical software"***. Federal Government must take action to rapidly ***improve the security and integrity of software supply chain, with a priority on addressing critical software.***
- **Section 5, Cyber Safety Review Board**: Establish a board that will review, assess, and provide recommendations on significant cyber incidents.

Improving the Nation's Cybersecurity, EO 14028, May 12, 2021 (Cont'd)

- **Section 6, Standardizing Federal Government's Playbook for Responding to Cybersecurity Vulnerabilities and Incidents**: Standardized response processes to ensure a more coordinated and centralized cataloging of incidents and tracking of Agencies' progress toward successful responses.
- **Section 7, Improve Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks**: Increase Federal Government's visibility into and detection of cybersecurity vulnerabilities by leveraging existing capabilities and the deployment of an Endpoint Detection and Response initiative.
- **Section 8, Improving the Federal Government's Investigative and Remediation Capabilities**: Improve the collection of information from network and system logs on Federal Information Systems and ensure its integrity to assist in responding to cyber incidents
- **Section 9, National Security Systems**: DoD shall adopt National Security Systems requirements equivalent to or exceeding the cybersecurity requirements in the EO.

Minimum Elements for an SBOM

Section 4(f), EO 14028: “Secretary of Commerce, in coordination with the Assistant Secretary for Communications and Information and the Administrator of the National Telecommunications and Information Administration, ***shall publish minimum elements for an SBOM***.”

Nutrition Facts

Serving Size 212 g

Amount Per Serving	
Calories 257	Calories from Fat 84
	% Daily Value*
Total Fat 9.4g	**14%**
Saturated Fat 1.1g	**6%**
Cholesterol 0mg	**0%**
Sodium 41mg	**2%**
Potassium 400mg	**11%**
Total Carbohydrates 39.8g	**13%**
Dietary Fiber 10.0g	**40%**
Sugars 2.1g	
Protein 8.0g	

Vitamin A 10% • Vitamin C 16%
Calcium 3% • Iron 14%

Nutrition Grade A

* Based on a 2000 calorie diet

Minimum Elements for an SBOM (Cont'd)

SBOM is a **formal record containing the details and supply chain relationships of various components used in building software**. The minimum elements for an SBOM consist of three broad inter-related areas:

- **Data Fields**: Baseline information of each component that should be tracked
- **Automation Support**: automatic generation and machine-readability to scale across the software ecosystem
- **Practices and Processes**: Define operations of SBOM requests, generation, and use

- The Minimum Elements for a Software Bill of Materials (SBOM), NTIA (Jul. 12, 2021).

Minimum Elements for an SBOM (Cont'd)

Data Fields – Baseline components include –

- **Supplier Name:** The name of an entity that creates, defines, and identifies components.
- **Component Name:** Designation assigned to a unit of software.
- **Version of the Component:** Identifier to specify a change in software from a previously identified version.
- **Other Unique Identifiers:** Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases.
- **Dependency Relationship:** Characterizing the relationship that an upstream component X is included in software Y.
- **Author of SBOM Data:** The name of the entity that creates the SBOM data for this component.
- **Timestamp:** Record of the date and time of the SBOM data assembly.

Minimum Elements for an SBOM (Cont'd)

Automation Support – data formats that are used to generate and consume SBOMs are:

- Software Package Data eXchange (SPDX)
- CycloneDX
- Software Identification (SWID) tags

The SBOM **must** be conveyed across organizational boundaries in one of these formats.

Minimum Elements for an SBOM (Cont'd)

Practices and Processes – To integrate SBOMs into the operations of the secure development life cycle, an organization should follow certain practices and processes that focus on the mechanics of SBOM use.

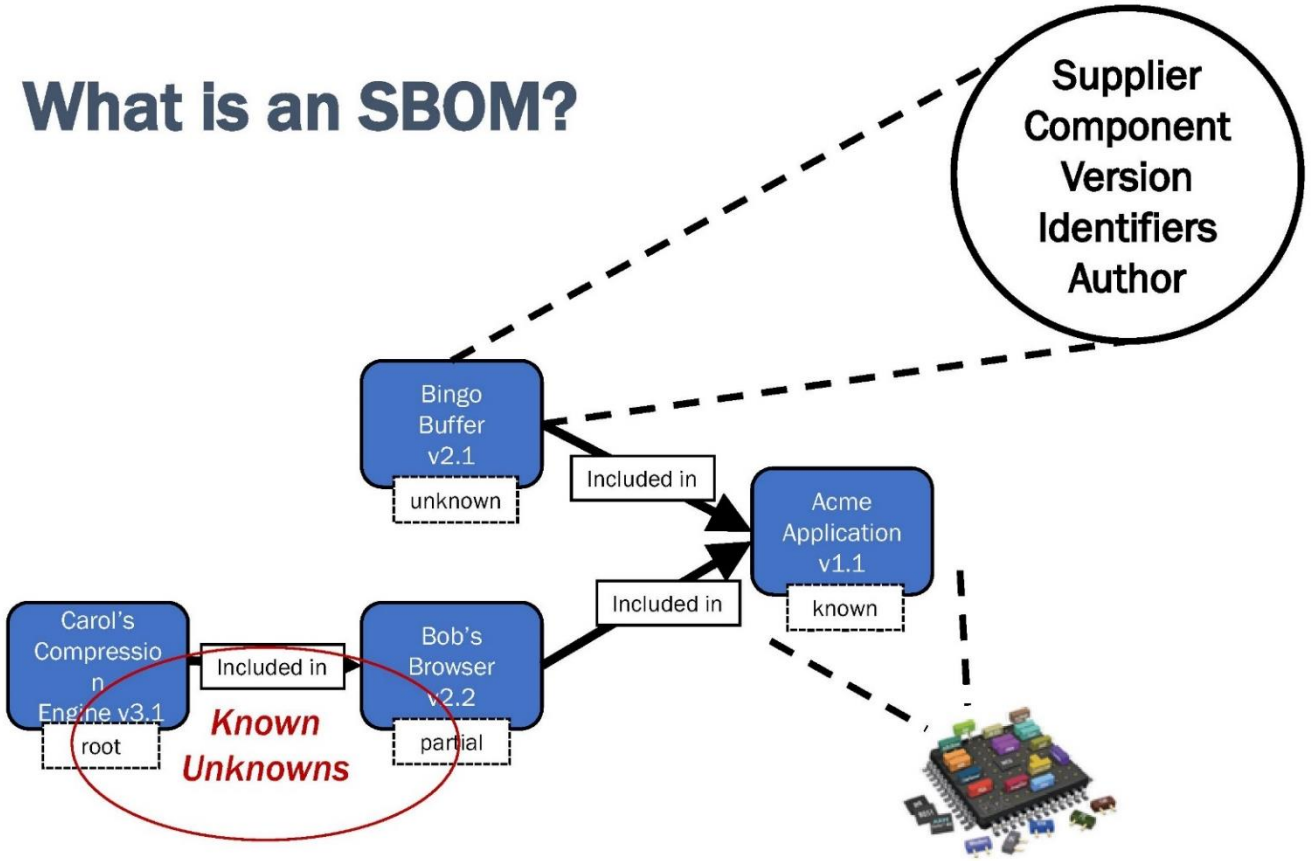
- **Frequency.** A new SBOM must be created to reflect the new version of the software
- **Depth.** An SBOM should contain all primary (top level) components, with all their transitive dependencies listed. Top-level dependencies must be listed with enough detail to seek out the transitive dependencies recursively.
- **Known Unknowns.** The SBOM author must explicitly identify "known unknowns" for instances in which the full dependency graph is not enumerated in the SBOM.
- **Distribution and Delivery.** SBOMs should be available in a timely fashion to those who need them and must have appropriate access permissions and roles in place.
- **Access Control.** Many suppliers, including open source maintainers, may feel their interests are best served by making SBOM data public.
- **Accommodation of Mistakes.** Should be built into the initial implementation phase of SBOM to allow for omissions and errors.

Minimum Elements for an SBOM (Cont'd)

How many SBOMs could a piece of software have (SBOMs for components of software)?

- "***A piece of software can be*** represented as a hierarchical tree, ***made up of components*** that can, in turn***, have subcomponents***, and so on. **Components** are often "third party," from another source, but might also be "first party," that is, from the same supplier but able to be uniquely identified as a freestanding, trackable unit of software. ***Each component should have its own SBOM listing their components, building the hierarchical tree***. The data fields apply to each component, which are, in turn, encoded with tools and formats for automation support following the defined practices and processes."

What is an SBOM?



1

FEDERAL GUIDANCE ON SOFTWARE BILL OF MATERIALS

"Critical Software" & EO 14028

Pursuant to Section 4 of EO 14028:

- Critical software is of particular concern and a priority to address.
- NIST directed to publish a definition of the term "critical software."
- CISA shall identify and make available to agencies a list of categories of software and software products in use or in the acquisition process meeting the definition of "critical software."
- NIST shall publish guidance outlining security measures for critical software including applying practices of least privilege, network segmentation, and proper configuration.

NIST, *Definition of Critical Software Under EO 14028* (July 8, 2021, updated Oct. 13, 2021)

NIST's definition of Critical Software:

- Applies only to the Government's ***management*** of software (per EO Sections 4i and 4j).
- Defines critical software in the context of the EO and provides a preliminary list of software that meets the definition of EO-critical and recommended to be included in the initial phase of implementation
- EO-critical definition is use-agnostic (*e.g.*, safety critical or critical infrastructure). Instead, definition focuses on the properties of a given piece of software that make it likely to be critical in most use cases.

NIST, *Definition of Critical Software Under EO 14028* (July 8, 2021, updated Oct. 13, 2021) (Cont'd)

NIST Definition: EO-critical software is any ***software that has, or has direct software dependencies upon, one or more components*** with at least one of these attributes:

- is designed to run with elevated privilege or manage privileges;
- has direct or privileged access to networking or computing resources;
- is designed to control access to data or operational technology;
- performs a function ***critical to trust***; or,
- operates outside of normal trust boundaries with privileged access.

The definition applies to software of all forms (*e.g.*, standalone software, software integral to specific devices or hardware components, cloud-based software) purchased for, or deployed in, production systems and used for operational purposes. Software solely used for research or testing that is not deployed in production systems, are outside of the scope of this definition.

NIST, *Definition of Critical Software Under EO 14028* (July 8, 2021, updated Oct. 13, 2021) (Cont'd)

NIST recommends initial EO implementation phase (phase 1) focus on standalone, on-premises software that has security-critical functions or poses similar significant potential for harm if compromised. Preliminary list includes:

- Identify, credential, and access management (ICAM)
- Operating systems, hypervisors, container environments
- Web browsers
- Endpoint security
- Network control
- Network protection
- Network monitoring and configuration
- Operational monitoring and analysis
- Remote scanning
- Remote access and configuration management
- Backup/recovery and remote storage

NIST, *Definition of Critical Software Under EO 14028* (July 8, 2021, updated Oct. 13, 2021) (Cont'd)

NIST anticipates that other categories of software, addressed in subsequent phases, may include:

- Software that controls access to data;
- Cloud-based and hybrid software;
- Software development tools such as code repository systems, development tools, testing software, integration software, packaging software, and deployment software;
- Software components in boot-level firmware; or
- Software components in operational technology (OT).

OMB Memorandum M-21-30, *Protecting Critical Software Through Enhanced Security Measures* (Aug. 10, 2021)

Overview:

Provides instructions for the implementation of measures required to secure the use of software falling within the definition of critical software and directs executive departments and agencies to implement measures in two phases:

1. Initial phase – Agencies should focus on standalone, on-premise software that performs security-critical functions or poses similar significant potential for harm if compromised.
2. Subsequent phases will address additional categories of software as determined by CISA.

OMB Memorandum M-21-30, *Protecting Critical Software Through Enhanced Security Measures* (Aug. 10, 2021) (Cont'd)

Critical Software for Agencies:

- Agencies must identify their critical software and adopt the required security measures for use of that software.
- Agencies must identify all agency critical software, in use or in the process of acquisition within 60 days of memorandum (Oct. 9, 2021).
- Agencies must implement the security measures designated by NIST for all categories of critical software included in initial phase within 1 year of the memorandum (Aug. 10, 2022).
- Agencies must incorporate security measures within 1 year of the publication of each guidance update from NIST, which will launch each subsequent phase of implementation.

OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (Sept. 14, 2022)

Overview:

- Requires agencies to comply with the NIST Guidance from EO 14028 and any subsequent updates when using any third-party software on the agency's information systems or otherwise affecting the agency's information.
- The term "software" includes firmware, operating systems, applications, and application services (*e.g.*, cloud-based software), as well as products containing software.
- Memorandum applies to agencies' use of software developed after the effective date of this memorandum, as well as agencies' use of existing software that is modified by major version changes after the effective date of this memorandum.

OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (Sept. 14, 2022) (Cont'd)

- The Memorandum's requirements do not apply to agency-developed software. However, agencies should take appropriate steps to adopt and implement secure software development practices for agency-developed software.
- An agency awarding a contract that may be used by other agencies (*e.g.*, GWACs) is responsible for implementing the requirements of this memorandum.
- Federal agencies must only use software provided by software producers who can attest to complying with the Government-specified secure software development practices, as described in the NIST Guidance.

OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (Sept. 14, 2022) (Cont'd)

For Contractors:

- Software producer's self-attestation (*i.e.*, conformance statement as described in NIST Guidance) from all third-party software used by an agency, including software renewals and major version changes.
- Software producers are encouraged to be product inclusive so the same attestation may be readily provided to all purchasing agencies.
- Agency shall retain the self-attestation document unless software producer posts it publicly and provides a link as part of its proposal response.

OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (Sept. 14, 2022) (Cont'd)

What if a software producer cannot attest to one or more practices from the NIST Guidance identified in the standard self-attestation form?

- The requesting agency shall require the software producer to identify those practices to which they cannot attest, document practices they have in place to mitigate those risks, and require a Plan of Action & Milestones (POA&M) to be developed.
- The agency shall take appropriate steps to ensure that such documentation is not posted publicly, either by the vendor or by the agency itself.
- If the software producer supplies that documentation and the agency finds it satisfactory, the agency may use the software despite the producer's inability to provide a complete self-attestation.

The above documentation, provided in lieu of a complete self-attestation, shall not be posted publicly by the vendor or the agency!!

OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (Sept. 14, 2022) (Cont'd)

What are the minimum requirements for an acceptable self-attestation a third-party software producer must provide?

1. The software producer's name;
2. A description of which product or products the statement refers to (preferably focused at the company or product line level and inclusive of all unclassified products sold to Federal agencies);
3. A statement attesting that the software producer follows secure development practices and tasks that are itemized in the standard self-attestation form;

NOTE: Self-attestation is the minimum level required! Agencies may make risk-based determinations that a third-party assessment is required due to the criticality of the service or product that is being acquired.

OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (Sept. 14, 2022) (Cont'd)

What is a third-party assessment?

- An assessment provided by either a certified FedRAMP Third Party Assessor Organization (3PAO) or one approved by the agency, including in the case of open source software or products incorporating open source software, provided the 3PAO uses the NIST Guidance as the assessment baseline.

Agencies are encouraged to use a standard self-attestation form, which will be made available to agencies. The Federal Acquisition Regulatory (FAR) Council plans to propose rulemaking on the use of a uniform standard self-attestation form.

OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (Sept. 14, 2022) (Cont'd)

SBOM in Government Requirements

1. Agencies may require SBOMs in solicitation requirements.
   a. Agency shall retain the SBOMs, unless the software producer posts it publicly and provides a link to that posting to the agency.
2. SBOMs must be generated in one of the data formats defined in the NTIA Report Minimum Elements for a SBOM or successor guidance published by CISA.
3. Agencies shall consider reciprocity of SBOM and other artifacts from software producers that are maintained by other Federal agencies.
4. Agency may require artifacts other than the SBOM (*e.g.*, automated tools and processes which validate the integrity of the source code and check for known or potential vulnerabilities).
5. Agency may require evidence that the software producer participates in a Vulnerability Disclosure Program.
6. Agencies are encouraged to notify potential vendors of requirements early in the acquisition process, including leveraging pre-solicitation activities.

OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (Sept. 14, 2022) (Cont'd)

Agencies To-Do's:

1. Inventory all software subject to the requirements of this memorandum, with a separate inventory for "critical software" within 90 days after publication of this memorandum (Dec. 13, 2022).
2. Develop a consistent process to communicate relevant requirements in this memorandum to vendors, and ensure attestation letters not posted publicly by software providers are collected in one central agency system within 120 days after publication of this memorandum (Jan. 12, 2023).
3. Collect attestation letters not posted publicly by software providers for "**critical software**" within 270 days after publication of this memorandum (June 11, 2023).
4. Collect attestation letters not posted publicly by software providers for **all software** within 365 days after publication of this memorandum (Sept. 14, 2023).
5. Agency CIOs, in coordination with agency requiring activities and agency CAOs, shall assess organizational training needs and develop training plans for the review and validation of full attestation documents and artifacts within 180 days after publication of this memorandum (March 13, 2023).

OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (Sept. 14, 2022) (Cont'd)

OMB To-Do's:

1. Post specific instructions for Agencies submitting requests for waivers or extensions to Max.gov. within 90 days after publication of this memorandum (Dec. 13, 2022).
2. Establish requirements for a centralized repository for software attestation and artifacts, with appropriate mechanisms for protection and sharing among Federal agencies within 180 days after publication of this memorandum (March 13, 2023).

CISA's To-Do's:

1. Establish a standard self-attestation "common form" within 120 days after publication of this memorandum (Jan. 12, 2023). **Published April 27, 2023!**
2. Establish a program plan for a government-wide repository for software attestations and artifacts with appropriate mechanisms for information protection and sharing among Federal agencies within 1 year from OMB's establishment of the requirements.
3. Demonstrate an Initial Operating Capability of the repository within 18 months from OMB's establishment of the requirements.
4. CISA will evaluate requirements for the Full Operating Capability of a Federal interagency software artifact repository through traditional OMB processes within 24 months from OMB's establishment of the requirements.
5. CISA will publish updated guidance on SBOMs for Federal agencies, as appropriate.

NIST Special Publication 800-218, *Secure Software Development Framework*, Ver. 1.1 (Feb. 2022)

- Identifies a core set of high-level secure software development practices to integrate into each software development lifecycle implementation.
- Practices should help reduce vulnerabilities and address the root causes of vulnerabilities.
- Secure software development practices organized in four groups:
  - **Prepare the Organization**: People, processes, and technology are prepared to perform secure software development at the organizational level.
  - **Protect Software**: Organizations should protect all components of their software from tampering and unauthorized access.
  - **Produce Well-Secured Software**: Produce well-secured software with minimal security vulnerabilities in software releases.
  - **Respond to Vulnerabilities**: Identify residual vulnerabilities in software releases and respond appropriately to address those vulnerabilities and prevent similar occurrences.

NIST, *Software Supply Chain Security Guidance Under EO 14028 Section 4e* (Feb. 4, 2022)

- Defines guidelines for federal agency staff who have software procurement-related responsibilities and helps federal agency staff know what information to request from software producers regarding their secure software development practices.
- When acquiring software or products containing software, Federal agencies should:
  - Use the SSDF's terminology and structure to organize communications about secure software development requirements.
  - Require attestation to cover secure software development practices performed as part of processes and procedures throughout the software life cycle.
  - Accept first-party attestation of conformity with SSDF practices unless a risk-based approach determines that second or third-party attestation is required.
  - Request high-level artifacts if artifacts of conformance are required.

NISTIR 8397, *Guidelines on Minimum Standards for Developer Verification of Software* (Oct. 2021)

Section 4(r) of EO 14028 directed NIST to publish guidelines recommending minimum standards for vendors' testing of their source code.

Eleven minimum standards identified in NISTIR 8397:

1. Threat modeling to look for design-level security issues.
2. Automated testing for consistency and to minimize human effort.
3. Code-based, or status, analysis to look for bugs.
4. Using heuristic tools to look for possible hardcoded secrets (passwords and private encryption keys)
5. Use of built-in (programing language-provided) checks and protections.
6. "Black box" test cases based on functional specifications or requirements, negative tests, and testing of what software should not do.
7. Code-based, or structural, test cases.
8. Historical test cases such as regression tests specifically designed to show presence of a bug.
9. Fuzzing (automated active testing where huge numbers of inputs are created during testing).
10. Web app scanners if the software provides a web service, using a Dynamic Application Security Testing tool.
11. Check included code (libraries, packages, services) from software components.

WHAT'S ON THE HORIZON?

GSA Acquisition Letter MV-23-02, *Ensuring Only Approved Software is Acquired and Used at GSA* (Jan. 11, 2023)

- Letter highlights current GSA acquisition policy and GSA IT policy work to ensure only approved software is acquired and used at GSA.
- In accordance with OMB M-22-18 and the GSA Acquisition Letter, GSA IT will update its policy or policies by June 12, 2023 to reflect GSA's process for collecting, reviewing, retaining, and monitoring attestation information.
- Until FAR rules are issued, GSA contracting activities will continue adhering to GSA internal policies on the use of approved and unapproved software as it pertains to:
  - Existing Contracts that Include the use of Software
  - New Contracts that Include the use of Software

GSA Acquisition Letter MV-23-02, *Ensuring Only Approved Software is Acquired and Used at GSA* (Jan. 11, 2023) (Cont'd)

For GSA-Administered Governmentwide Vehicles and Assisted Acquisitions:

- GSA-administered indefinite delivery vehicles (IDVs) (*e.g.*, Federal Supply Schedule, Government-wide Acquisition Contracts, Multi-Agency Contracts (MACs)) must be updated to allow, but not require, contractors to provide attestations, responsive to the requirements of OMB M-22-18, at the base IDV contract level and make such information available to ordering activities to the extent possible.
- Attestations must utilize the forthcoming CISA attestation common form and must not include Plan of Action & Milestones (POA&M) or Software Bill of Material (SBOM) information.
- The ordering agency is responsible for complying with OMB M-22-18.
- Relevant GSA acquisition policy specific to GSA-administered IDVs may be updated to further implement the FAR rule once issued.
- For assisted acquisitions, GSA contracting activities must follow the policy of the requesting agency.

Status of CISA Self-Attestation Common Form?

On April 27, 2024, CISA released the draft *Secure Software Development Attestation Common Form* (88 FR 25670)

- Self-attestation is required for:
  - Software developed after September 14, 2022;
  - Existing software modified by major revision changes after September 14, 2022; and
  - Software to which the producer delivers continuous changes to the software code (*e.g.*, software-as-a-service products)
- Self-attestation is not required for:
  - Software developed by Federal agencies; and
  - Software freely obtained directly by a Federal agency

Draft form available for public comment until June 26, 2023

Open FAR Case

FAR Case No. 2023-002 (April 28, 2023), Supply Chain Software Security, to implement section 4(n) (FAR language to require supplier of software available for purchase by agencies to comply with, and attest to complying with, any requirements issued pursuant to subsection g through k of section 4) of EO 14028

- FAR Case No. 2023-002 would propose changes to:
  - FAR Part 1;
  - FAR Part 39; and
  - FAR Part 52.

Current Status? Proposed FAR rule currently being drafted. Report due date May 3, 2023!

QUESTIONS?

Bonus Tip: Don't Be Afraid to Seek Guidance or Ask for Help!

Contact Information

Alexander W. Major, Esq.
Partner, McCarter & English LLP

www.mccarter.com
amajor@mccarter.com
O: 202-753-3440
M: 410-935-0037

Philip Lee, Esq.
Associate, McCarter & English LLP

www.mccarter.com
plee@mccarter.com
O: 202.741.8209