Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e
February 4, 2022

Introduction

Executive Order (EO) 14028 on Improving the Nation's Cybersecurity, May 12, 2021, directs the National Institute of Standards and Technology (NIST) to publish guidance on practices for software supply chain security. Section 4e begins with the following text, which is followed by ten numbered items omitted here for brevity.

> *(Section 4e) Within 90 days of publication of the preliminary guidelines pursuant to subsection (c) of this section, the Secretary of Commerce acting through the Director of NIST, in consultation with the heads of such agencies as the Director of NIST deems appropriate, shall issue guidance identifying practices that enhance the security of the software supply chain. Such guidance may incorporate the guidelines published pursuant to subsections (c) and (i) of this section.*

The EO also directs the Office of Management and Budget (OMB) to require agencies to comply with the published guidance.

> *(Section 4k) Within 30 days of issuance of the guidance described in subsection (e) of this section, the Director of OMB acting through the Administrator of the Office of Electronic Government within OMB shall take appropriate steps to require that agencies comply with such guidelines with respect to software procured after the date of this order.*

To gather input on possible practices for the guidance, NIST solicited position papers from the community, hosted a virtual workshop in June and a second virtual workshop in November, consulted with other federal agencies, and reviewed existing federal guidance.

This document starts by explaining NIST's approach for addressing Section 4e. Next, it defines guidelines for federal agency staff who have software procurement-related responsibilities (e.g., acquisition and procurement officials, technology professionals). These guidelines are intended to help federal agency staff know what information to request from software producers regarding their secure software development practices. This document concludes with Frequently Asked Questions (FAQ) offering additional information.

Guidance Purpose and Scope

EO 14028 emphasizes that "the security of software used by the Federal Government is vital to the Federal Government's ability to perform its critical functions," and "there is a pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended." Accordingly, secure software development practices should be integrated throughout software life cycles for three reasons: 1) to reduce the number of vulnerabilities in released software, 2) to reduce the potential impact of the exploitation of undetected or unaddressed vulnerabilities, and 3) to address the root causes of vulnerabilities to prevent recurrences. [SP 800-218]

EO 14028 Section 4e contains 10 subsections or items. Each of them specifies actions or outcomes for *software producers*, such as commercial-off-the-shelf (COTS) product vendors, government-off-the-shelf (GOTS) software developers, and contractors and other custom software developers. Before EO 14028's release, NIST had published the initial Secure Software Development Framework (SSDF), which defined outcome-based secure software development practices and tasks for software producers to follow. Most of the Section 4e items were already addressed by the original SSDF. NIST has since revised the SSDF to address all Section 4e items, resulting in SP 800-218, *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities*. FAQ #7 contains a mapping of each Section 4e item to the SSDF practices and tasks that help address it.

SP 800-218 addresses Section 4e from a **software producer viewpoint**. The software producers are the ones who implement SSDF practices. Section 4k explains that federal agencies will need to comply with NIST guidelines addressing Section 4e. In this context, federal agencies are *software purchasers*, not software producers, so additional guidance is needed to address Section 4e from a **software purchaser viewpoint**. This document defines that guidance.

This document provides recommendations to federal agencies on ensuring that the producers of software they procure have been following a risk-based approach for secure software development throughout the software life cycle. These recommendations are intended to help federal agencies get the information they need from software producers in a form they can use to make risk-based decisions about procuring software. These recommendations address all items within Section 4e from a software purchaser (federal agency) viewpoint. They involve software producers indicating conformity with secure software development practices as part their internal processes by providing artifacts to federal agency purchasers and/or attesting to conformity.

The **scope** of this guidance is limited to **federal agency procurement** of software, which includes firmware, operating systems, applications, and application services (e.g., cloud-based software), as well as products containing software. The location of the implemented software, such as on-premises or cloud-hosted, is irrelevant. **Software developed by federal agencies is out of scope, as is open-source software freely and directly obtained by federal agencies. Open-source software that is bundled, integrated, or otherwise used by software purchased by a federal agency is in scope.**

Terminology

Section 4e uses several terms, including "conformity," "attestation," and "artifacts." Because EO 14028 does not define these terms, this guidance presents the following definitions from existing standards and guidance:

- ***Conformity assessment*** is a "demonstration that specified requirements are fulfilled." [ISO/IEC 17000] In the context of Section 4e, the requirements are secure software development practices, so conformity assessment is a demonstration that the software producer has followed secure software development practices for their software.

- ***Attestation*** is the "issue of a statement, based on a decision, that fulfillment of specified requirements has been demonstrated." [ISO/IEC 17000]

    - If the software producer itself attests that it conforms to secure software development practices, this is known by several terms, including ***first-party attestation***, ***self-attestation***, ***declaration***, and ***supplier's declaration of conformity (SDoC)***.
    - If the software purchaser attests to the software producer's conformity with secure software development practices, this is known as ***second-party attestation***.
    - If an independent third-party attests to the software producer's conformity with secure software development practices, this is known as ***third-party attestation*** or ***certification***.

- An ***artifact*** is "a piece of evidence." [adapted from NISTIR 7692] ***Evidence*** is "grounds for belief or disbelief; data on which to base proof or to establish truth or falsehood." [NIST SP 800-160 Vol. 1] Artifacts provide records of secure software development practices.
    - Low-level artifacts will be generated during software development, such as threat models, log entries, source code files, source code vulnerability scan reports, testing results, telemetry, or risk-based mitigation decisions for a particular piece of software. These artifacts may be generated manually or by automated means, and they are maintained by the software producer.
    - High-level artifacts may be generated by summarizing secure software development practices derived from the low-level artifacts. An example of a high-level artifact is a publicly accessible document describing the methodology, procedures, and processes a software producer uses for its secure practices for software development.

The following subsections of EO 14028 Section 4e use these terms:

> *(ii) generating and, when requested by a purchaser, providing artifacts that demonstrate conformance to the processes set forth in subsection (e)(i) of this section;*
>
> *(v) providing, when requested by a purchaser, artifacts of the execution of the tools and processes described in subsection (e)(iii) and (iv) of this section, and making publicly available summary information on completion of these actions, to include a summary description of the risks assessed and mitigated;*
>
> *(ix) attesting to conformity with secure software development practices;*

In other words, when a federal agency (purchaser) acquires software or a product containing software, the agency should receive attestation from the software producer that the software's development complies with government-specified secure software development practices. The federal agency might also request artifacts from the software producer that support its attestation of conformity with the secure software development practices described in Section 4e subsections (i), (iii), and (iv), which are listed here:

> *(i) secure software development environments, including such actions as:*
>
> > *(A) using administratively separate build environments;*
> >
> > *(B) auditing trust relationships;*

(C) establishing multi-factor, risk-based authentication and conditional access across the enterprise;

(D) documenting and minimizing dependencies on enterprise products that are part of the environments used to develop, build, and edit software;

(E) employing encryption for data; and

(F) monitoring operations and alerts and responding to attempted and actual cyber incidents;

(iii) employing automated tools, or comparable processes, to maintain trusted source code supply chains, thereby ensuring the integrity of the code;

(iv) employing automated tools, or comparable processes, that check for known and potential vulnerabilities and remediate them, which shall operate regularly, or at a minimum prior to product, version, or update release;

Attesting to Conformity with Secure Software Development Practices

NIST has defined the following minimum recommendations for federal agencies as they acquire software or a product containing software. These recommendations are intended to assist federal agencies and software producers in communicating clearly with each other regarding secure software development artifacts, attestation, and conformity.

1. **Use the SSDF's terminology and structure to organize communications about secure software development requirements.** This enables all software producers to use the same lexicon when attesting to conformity for federal agencies. Software producers can map their secure development methodology to the SSDF's secure software development practices or associated informative references.
2. **Require attestation to cover secure software development practices performed as part of processes and procedures throughout the software life cycle.** With the highly dynamic nature of software today, attesting to how things were and are done on an ongoing basis (processes and procedures) is typically more valuable than attesting to how things were done for a specific software release generated by one instance of those processes. This is especially true for post-release practices such as vulnerability disclosure and response, where processes might not yet have been performed for the latest release.
3. **Accept first-party attestation of conformity with SSDF practices unless a risk-based approach determines that second or third-party attestation is required.** First-party attestation is recommended for meeting the EO 14028 requirements. This is consistent with the guidance in NIST SP 800-161 Rev. 1 (Second Draft), which states in Section 3.1.2: "There are a variety of acceptable validation and revalidation methods, such as requisite certifications, site visits, third-party assessment, or self-attestation. The type and rigor of the required methods should be commensurate to the criticality of the service or product being acquired and the corresponding assurance requirements."
4. **When requesting artifacts of conformance, request high-level artifacts.** The software producer should be able to trace the practices summarized in the high-level artifacts to the corresponding

low-level artifacts that are generated by those practices. Asking for low-level artifacts for a particular software release is not recommended for meeting the requirements of EO 14028, but may be needed to meet other agency requirements. Reasons for avoiding low-level artifacts include the following:

- Low-level artifacts provide a snapshot in time of only a small aspect of secure software development, whereas high-level artifacts can provide a big-picture view of how secure software development is performed.
- Artifacts should address the needs of the audience receiving them, thus providing the necessary information in a usable format for that audience. Understanding low-level artifacts requires the agency to expend considerable technical resources and expertise in analyzing them and determining how to consider them within the context of the broader secure software development practices.
- Low-level artifacts often contain intellectual property or other proprietary information, or details that attackers could use for hostile purposes, so accepting low-level artifacts gives the agency additional sensitive information to protect.

These minimum recommendations apply to attestation for all software within the scope of this guidance procured by federal agencies, and they should be part of each agency's processes. The recommendations are not intended to replace more stringent requirements for secure software development that federal agencies may have.

These minimum practices will not be sufficient in some cases. For example, an agency may need greater visibility into the practices for a particular product so that it can better understand how the product would affect the agency's cybersecurity risk. As discussed in Section 1.4.2 of SP 800-161 Rev. 1 (Second Draft), agencies requiring greater visibility into practices may increase costs for software producers, and thus may increase product prices. See SP 800-161 Rev. 1 for more information on these considerations.

FAQs

The following FAQs provide additional information on the guidance.

1. **Where can I learn more about conformity assessment?**

   For more detailed information on conformity assessment, see NIST SP 2000-01, ABC's of Conformity Assessment; NIST SP 2000-02, Conformity Assessment Considerations for Federal Agencies; and ISO/IEC 17000:2020 – Conformity assessment – vocabulary and general principles. NIST SP 2000-01 and SP 2000-02 reference ISO/IEC 17000 and cite several of its definitions, including "conformity assessment."

2. **Where can I learn more about first-party attestation and supplier's declaration of conformity?**

   Additional information is available from NIST SP 2000-01, ABC's of Conformity Assessment and ISO/IEC 17050-1:2004, Conformity assessment – Supplier's declaration of conformity – Part 1: General requirements.

3. **Does NIST have additional resources on cybersecurity supply chain risk management (C-SCRM)?**

Yes, see NIST's C-SCRM project website for links to all the resources. An example is the Federal C-SCRM Forum, which NIST hosts; the Forum fosters collaboration and the exchange of C-SCRM information among federal agencies to improve the security of federal supply chains. Examples of NIST C-SCRM guidance include SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations and SP 800-161 Rev. 1 (Second Draft), Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.

4. **Are any other parts of EO 14028 related to this guidance?**

   Yes. Section 4n references section 4k, which was discussed in the introduction to this guidance. Here is the text of Section 4n:

   > *(Section 4n) Within 1 year of the date of this order, the Secretary of Homeland Security, in consultation with the Secretary of Defense, the Attorney General, the Director of OMB, and the Administrator of the Office of Electronic Government within OMB, shall recommend to the FAR Council contract language requiring suppliers of software available for purchase by agencies to comply with, and attest to complying with, any requirements issued pursuant to subsections (g) through (k) of this section.*

5. **Can agencies apply this guidance to software developed by federal agencies?**

   Yes, agencies can choose to implement the recommendations with agency-based software developers in order to help assess the security risks associated with their software and make risk-based decisions about its implementation and use.

6. **Can agencies apply this guidance to open-source software they freely and directly obtain?**

   Yes, agencies can choose to use attestations and artifacts from open-source software producers who make such content available. This may help agencies to assess the security risks associated with the software and make risk-based decisions about its implementation and use.

7. **How does the SSDF help address Section 4e of EO 14028?**

   The following table maps each Section 4e subsection to the SSDF practices and tasks that help address each subsection. See SP 800-218 for more information on each SSDF practice and task.

SSDF Practices Corresponding to EO 14028 Subsections

EO 14028 Subsection	Subsection Summary (Refer to the next column for a complete list)	SSDF Practice and Task Reference Numbers
4e(i)	Have secure software development environments, including:	*[See rows below]*
4e(i)(A)	administratively separate build environments;	PO.5.1
4e(i)(B)	trust relationship auditing;	PO.5.1
4e(i)(C)	multi-factor, risk-based authentication and conditional access;	PO.5.1, PO.5.2
4e(i)(D)	minimized dependencies on enterprise products in development environments;	PO.5.1
4e(i)(E)	data encryption; and	PO.5.2
4e(i)(F)	operational monitoring and incident detection and response.	PO.3.2, PO.3.3, PO.5.1, PO.5.2

EO 14028 Subsection	Subsection Summary (Refer to the next column for a complete list)	SSDF Practice and Task Reference Numbers
4e(ii)	Provide artifacts from 4e(i) upon request.	PO.3.2, PO.3.3, PO.5.1, PO.5.2
4e(iii)	Maintain trusted source code supply chains.	PO.3.1, PO.3.2, PO.5.1, PO.5.2, PS.1.1, PS.2.1, PS.3.1, PW.4.1, PW.4.4
4e(iv)	Check software for vulnerabilities and remediate them.	PO.4.1, PO.4.2, PS.1.1, PW.2.1, PW.4.4, PW.5.1, PW.6.1, PW.6.2, PW.7.1, PW.7.2, PW.8.2, PW.9.1, PW.9.2, RV.1.1, RV.1.2, RV.2.1, RV.2.2, RV.3.3
4e(v)	Provide artifacts from 4e(iii) and 4e(iv) upon request, and make a summary description of risks assessed and mitigated publicly available.	PO.3.2, PO.3.3, PO.4.1, PO.4.2, PO.5.1, PO.5.2, PW.1.2, PW.2.1, PW.7.2, PW.8.2, RV.2.2
4e(vi)	Maintain provenance data for internal and 3rd party components.	PO.1.3, PO.3.2, PO.5.1, PO.5.2, PS.3.1, PS.3.2, PW.4.1, PW.4.4, RV.1.1, RV.1.2
4e(vii)	Provide a software bill of materials (SBOM) for each product.	PS.3.2
4e(viii)	Participate in a vulnerability disclosure program.	RV.1.1, RV.1.2, RV.1.3, RV.2.1, RV.2.2, RV.3.3
4e(ix)	Attest to conformity with secure software development practices.	All practices and tasks consistent with a risk-based approach
4e(x)	Attest to the integrity and provenance of open-source software components.	PS.2.1, PS.3.1, PS.3.2, PW.4.1, PW.4.4

8. I have software procurement-related responsibilities (e.g., acquisition and procurement officials, technology professionals) for my agency. To conform with Section 4e of EO 14028, what should I request from software producers regarding their secure software development practices?

Software purchasers from a federal agency should ask software producers to provide a conformance statement attesting that their software development processes follow SSDF practices, including those specifically called out in Section 4e as presented in FAQ #7. The conformance statement should include:

- *Software producer's name*
- *A description of which product or products the statement refers to. (Note: it is preferable to address this at the company or product line level rather than per product.)*
- *A statement attesting that the software producer follows secure development practices and tasks as specified in FAQ #7 that are appropriate and applicable*
- *Name and title of individual who is the main point of contact and can provide, if requested by the purchasers, the artifacts generated by the secure software development activities related to EO 14028 Sections 4e(i), 4e(iii), and 4e(iv)*

9. I am a software producer and I want to sell my product to federal agencies. What information about secure software development do I need to provide to them?

You should provide a conformance statement, which is described in FAQ #8.

Additionally, you can choose to exceed the EO 14028 Section 4e requirements by providing a reference or URL to a summary of secure software development activities related to the SSDF *practices and tasks, including risk-based and mitigation actions. A sample template is posted here for reuse in documenting the activities.*

10. **I am a software reseller. How do I show purchasers that the software I am reselling meets the requirements of EO 14028 Section 4e?**

    You should ensure that you can provide a reference to the software producer's conformance statement, as described in FAQ #8, for each software you resell to software purchasers.