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

Executive Order 14028 on Improving the Nation's Cybersecurity

Issued May 12, 2021 by President Biden

Key Areas Covered by this Executive Order:

1. Policy – Federal Government must
   - Bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid.
   - Must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).
2. Sharing Threat Information
3. Cyber Incident Reporting
4. **Enhancing Software Supply Chain Security**
5. Standardizing the federal government's playbook for responding to cybersecurity vulnerabilities and incident
6. Improving detection of cybersecurity vulnerabilities and incidents on federal government networks
7. Improving the federal government's investigative and remediation capabilities

Executive Order on Improving the Nation’s Cybersecurity - Update

Current Status

- On February 04, 2022 NIST released the following documents supporting the execution of this Executive Order:

Software Security Practices

- **Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e** (https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-cybersecurity-producers-and)
- NIST Special Publication 800-218, Secure Software Development Framework (SSDF) Version 1.1:Recommendations for Mitigating the Risk of Software Vulnerabilities (https://csrc.nist.gov/publications/detail/sp/800-218/final)

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

- EO 14028 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.*
- NIST issued NIST Special Publication 800-218, Secure Software Development Framework (SSDF) Version 1.1:Recommendations for Mitigating the Risk of Software Vulnerabilities to partially address Section 4e, but NIST Special Publication 800-218 is from a software producer perspective
- Purpose of this particular guidance is to address Section 4e from the prospective of a Federal Agency procuring software – i.e., how can a Federal Agency ensure "that the producers of software they procure have been following a risk-based approach for secure software development throughout the software life cycle"

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

Scope

- 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
- 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

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

Terminology

- ***Conformity assessment***: a "demonstration that specified requirements are fulfilled"
- ***Attestation***: the "issue of a statement, based on a decision, that fulfillment of specified requirements has been demonstrated"
    - If the software producer itself attests that it conforms to secure software development practices, this is known by several terms, including ***first-party attestation***, ***selfattestation***, ***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***
- ***Artifact***: "a piece of evidence."
- ***Evidence***: "grounds for belief or disbelief; data on which to base proof or to establish truth or falsehood"

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

Terminology

- **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.

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

Guidelines

- 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
  - Essentially this means that the software producer should attest that it is following the Secure Software Development Framework documented in NIST SP 800-218 (or something similar)
- 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)

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

<u>Guidelines</u>

Prescribed software practices in Section 4e are:

- *(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;*

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

Guidelines for Attesting to Conformity with Secure Software Development Practices

- 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
- When requesting artifacts of conformance, request high-level artifacts