Office of Management and Budget
Office of the Federal Chief Information Officer

Implementation of Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4(k)
March 7, 2022

Introduction

The security of software used by the Federal Government is vital to the Federal Government's ability to perform its critical functions. In order to implement more rigorous and predictable mechanisms for ensuring that software products function securely, and as intended, the National Institute of Standards and Technology (NIST) has issued a Secure Software Development Framework (SSDF) and related guidance. Agencies should begin integrating the NIST Software Supply Chain Security Guidance under Executive Order 14028[1] Section 4e into their existing software lifecycle management and acquisition practices to ensure purchase of only secure and trustworthy products. Following SSDF practices should help software producers reduce the number of vulnerabilities in released software, reduce the potential impact of the exploitation of undetected or unaddressed vulnerabilities, and address the root causes of vulnerabilities to prevent recurrence.

Background

NIST developed guidelines[2] based on consultations with and input from the Federal Government, private sector, academia, and other appropriate actors to identify existing or develop new standards, tools, and best practices for complying with the standards, procedures, or criteria for secure software development environments.

The Office of Management and Budget (OMB) is seeking feedback through a set of structured implementation questions. The questions are focused on best practices for implementing the SSDF, and approaches for attesting to secure software development practices. OMB will incorporate feedback into its guidance as appropriate. Responses should be no longer than 5 pages in length and sent to OFCIO@omb.eop.gov no later than **5:00pm Friday, March 18, 2022**. Responses do not need to address every question below. For technical questions on NIST's Secure Software Development Framework (SSDF) and related guidance, please contact NIST: swsupplychain-eo@nist.gov.

[1] See EO 14028 Federal Register :: Improving the Nation's Cybersecurity

[2] See NIST 4e guidelines Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e (nist.gov)

Implementation Questions

1. How would you describe the ideal process for Federal agencies to obtain and retain secure software development attestation documents[3] for software being procured?

2. Are there examples of successful systems, tools and procedures for assessing compliance that should be examined for applicability to the SSDF? What characteristics of other established processes are most important to emulate? Do you recommend any particular standard format(s) for attesting to compliance?

3. Are there elements of the framework for which there are alternate and potentially more effective ways (e.g., conformity assessments[4]) of demonstrating adoption than attestation?

4. What risk-based factors should be considered to determine when third party attestation is most appropriate for affirming adequate SSDF practices are in place?

5. How should vendors articulate the products and the boundaries of the products covered within the attestation?

6. What information do vendors need in advance in order to comply with implementation guidance?

[3] NIST defines an attestation as the "issue of a statement, based on a decision, that fulfillment of specified requirements has been demonstrated." (See Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e, p.2)

[4] NIST defines a conformity assessment as a "demonstration that specified requirements are fulfilled" (See Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e, p.2)