Executive Order – NIST workshop position paper #2

(Secure software development lifecycle)

Microsoft Corporation

Focus Area

Initial list of secure software development lifecycle standards, best practices, and other guidelines acceptable for the development of software for purchase by the federal government. This list of standards shall include criteria and required information for attestation of conformity by developers and suppliers. See EO Section 4(e)(i, ii, ix, and x).

Microsoft Response

Microsoft supports international standards which are created in open global standards development organizations, such as the International Standards Organization / International Electrical Committee (ISO / IEC). International standards are especially important in situations where there are multiple national or industry-specific standards that could apply to commodity products, such as operating systems, applications, and cloud services. The benefit of adopting international standards is that product suppliers can implement to one standard for world-wide use instead of being required to satisfy multiple standards per region or industry, some of which may have conflicting requirements. We suggest NIST consider aligning to applicable ISO / IEC standards related to secure software development and supply chain in a similar manner as NIST has adopted ISO/IEC cryptographic module conformance and testing standards for the United States federal IT systems.

Recommendations

1. Adopt ISO/IEC 27034, "Security Techniques – application security" and ISO/IEC 27036, "Security Techniques – information security for supplier relationships" as the initial foundation for secure development lifecycle standards, best practices, guidelines, and assessment. Both ISO standards are published, with ISO/IEC 27034 part 4 under development and ISO/IEC 27036 entering a scheduled periodic revision, so the U.S. has an opportunity to provide input to the worldwide community for acceptable software security and supply chain relationships. Naturally, these perspectives would include NIST's existing work on software security. There is also a regular cadence of updating these standards, providing a critical opportunity to continue evolving and maturing practices.

2. Adopt an updated version of the NIST Secure Software Development Framework (SSDF) as an initial foundation for secure development lifecycle standards, best practices, and guidelines. These updates would be based on experiences learned from utilizing the SSDF and aligned with relevant international standards.

   There are many development lifecycles, and no single development lifecycle is used to develop software anywhere. Different approaches are taken across industries, within industries and even within single development organizations. Given this diversity, evolving threats, and the fast pace of innovation, no single standard has emerged for secure software development. An integral part of the software development process at Microsoft since 2004 and first shared with industry in 2008, Microsoft’s Secure Development Lifecycle (SDL) has been constantly improved and demonstrates a practical approach that has proven to be effective across an organization developing diverse products using different technologies. It offers generalized practices broad enough to apply to all development organizations and technologies, flexible enough to allow for the creation of specific processes and tools aligned to the specific requirements of specific development organizations, and open enough to allow of innovation and evolution as the environment changes. Microsoft notes a strong correlation between the practices we've used for many years and the practices defined in NIST Secure Software Development Framework (SSDF). We believe the SSDF provides an excellent initial foundation to build upon for use as the Secure Development Lifecycle required by the Executive Order.

3. Should the SSDF be adopted, we recommend updating of some of the implementation examples for more practical implementation. Automation considerations and principles should be integrated for standards and best practices to scale.

Request to participate on panel

Microsoft would appreciate the opportunity to participate on the panel that will lead the discussion on secure software development lifecycle standards and best practices at the June 2 – 3, 2021 NIST workshop. For this discussion, we will share lessons learned and experiences and provide expertise on the security development lifecycle.