Andrew van der Stock

Executive Director, OWASP Foundation

c/- 401 Edgewater Place, Suite 600, Wakefield, MA

The OWASP Foundation is responding to NIST's request for a position paper on secure software supply chains for four elements: criteria for designating critical software; an initial list of secure software requirements; Initial minimum testing requirements; Guidelines for software integrity chains and provenance. Andrew van der Stock, Executive Director, and Brian Glas, OWASP Top 10/OWASP SAMM co-lead, have registered for the workshop and are willing to speak on behalf of OWASP. Contact details are at the end of this document.

The Open Web Application Security Project (OWASP) is unique in the industry as a vendor-neutral non-profit. For 20 years, OWASP has promoted software security improvement by developing hundreds of projects, the participation of thousands of members, regular meetings at 270 chapters worldwide, and several regional and global events. Our Education and Training Committee is developing free industry and tertiary curriculums, and eventually, certification. OWASP has mature, accessible, and open-source standards, guidance, evidence-based data, and tools ready for immediate adoption by NIST to fulfill many parts of the Executive Order and its short deadlines.

This position paper is written in concert with Steve Springett, who leads the OWASP Dependency Track Project, CycloneDX (a Software Bill Of Materials SBOM standard); Jeremy Long (OWASP Dependency Check project); Sebastien Deleersnyder and Bart De Win from the OWASP Software Assurance Maturity Model (SAMM) project, Andrew van der Stock, Josh Grossman, Jim Manico, and Daniel Cuthbert from the OWASP Application Security Verification Standard (ASVS); and finally Andrew is also a co-leader of the OWASP Top 10 project with Brian Glas, Neil Smithline, and Torsten Gigler. Our leaders bring decades of experience as practitioners and leaders in the application security field worldwide.

Criteria for designating "critical software."

OWASP's view on designating critical software and systems is that it should be simple, objective, and repeatable. One of our leaders has a 20-25 point questionnaire that models risk factors and is difficult to game to get a lower result. Additionally, there will be systems on the cusp that should be protected as well, in the case of those who might try to game the system to lower the risk inappropriately. The OWASP ASVS defines three security verification levels, with each level increasing in depth. Three levels are a good start for a working definition. We encourage NIST to keep the levels clear and limited in complexity to prevent confusion and promote voluntary compliance. The biggest enemy of security is complexity, and by joining forces, NIST can ensure everyone understands each level.

An initial list of secure software development lifecycle standards, best practices, and other guidelines

We encourage NIST to consider, adopt, and improve any of our essential standards, guidelines, and tools, such as OWASP SAMM, OWASP ASVS, OWASP SCVS, OWASP Web Testing Guide, OWASP Threat Dragon, OWASP Cheat Sheet Series, and more. Access to standards, guidelines and tools should be free and easy to adopt. The ASVS has been adopted by several governments and is under consideration by the UK financial regulator.

Software Assurance Maturity Model (SAMM) provides an effective and measurable way for all types of organizations to analyze and improve their secure software development lifecycle. SAMM is a prescriptive model, an open framework that is simple to use, fully defined, and measurable. Our community-built SAMM is meant to be evolutive and risk-driven in nature, as there is no single recipe that works for all organizations. SAMM 1.5 was mapped to the NIST Secure Software Development Framework (SSDF). SAMM v2 is a core component of the new RABET-V process that has been piloted with non-voting election software.

We are working on certification to ensure training materials and body of knowledge are of high standards in individuals and organizations. We would like to gather NIST's requirements to validate that consultancies and practitioners have adequate skills to implement the EO's requirements.

Initial minimum requirements for testing software

As the EO has extremely short timelines, we would recommend that for the initial minimum requirements, NIST consider OWASP's flagship Testing Guides and the Application Security Verification Standard, which contains standards for architecture, unit and integration testing, code review, and penetration testing. OWASP promotes building security in, along with validating the controls are in place and effective.

The OWASP Top 10 project recently completed the forthcoming OWASP Top 10 2021's data collection and analysis, with data on over 495,000 applications. We strongly believe in evidence-based security. This data set will assist with both protecting and testing systems using evidence-based controls. OWASP is willing to share this data set with NIST and the rest of the world. Incidence rate data is used to help order the OWASP Top 10 and the ASVS control levels. There is no point in mandating controls or testing with little to no impact or likelihood.

Guidelines for software integrity chains and provenance

OWASP encourages interoperable SBOM standards, allowing rapid developer consumption and resolution of results. Security teams should consume those same results to assist in the rapid elimination of vulnerable components. OWASP Dependency-Check, OWASP Software Component Verification Standard, OpenSSF's SLSA, and the CycloneDX SBOM standard are significant real world implementations. OWASP would encourage NIST to work with leading experts from the OWASP community to improve the integrity and security of software security.

OWASP is ready to assist in the rapid implementation of the Executive Order using our mature flagship standards, guidelines, and tools, and subsequently improve them with NIST, and share our expertise, data, and vendor neutrality.

Andrew van der Stock, Executive Director - andrew.vanderstock@owasp.com +510 697 9315
Brian Glas, Co-lead OWASP Top Ten/SAMM - brian.glas@owasp.org