ITI Promoting Innovation Worldwide

ITI Position Paper on Standards and Guidelines to Enhance Software Supply Chain Security

May 26, 2021

The Information Technology Industry Council (ITI) appreciates the opportunity to submit comments to NIST on Standards and Guidelines to Enhance Software Supply Chain Security. ITI is the premier global advocate for technology, representing 80 of the world's most innovative companies. Our diverse membership and expert staff provide policymakers the broadest perspective and thought leadership from technology, hardware, software, services, and related industries. ITI welcomes the release of the *Executive Order on Improving the Nation's Cybersecurity*, which delegates NIST to consult with stakeholders to identify standards, tools, best practices, and other guidelines to enhance software supply chain security. ITI emphasizes that ICT products/services and our knowledge about risks and vulnerabilities are always evolving; therefore, standards and best practices, including those developed pursuant to the EO, should be reviewed regularly. Please find below our comments tracking the five areas of inquiry posed by NIST:

1. Criteria for designating "critical software."

Overall, ITI recommends that the definition of "critical software" be narrowly scoped and should not encompass every software element that might pose a security risk should it contain a vulnerability, which could capture potentially any and every piece of software connected to a government network. The definition should focus on software elements critical to maintaining confidentiality, integrity and availability (CIA triad), focusing primarily on identification/authentication, authorization, and non-repudiation. We recommend the definition of "critical software" be risk-based and narrowly focus on the purpose or use of the software, and the potential impact to the organization if software is compromised, leveraging existing frameworks to assess the criticality of the system.

2. 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.

ITI recommends leveraging the Common Criteria (ISO/IEC 15408:2009) framework, an internationally recognized product evaluation and certification scheme for software that is referenced in the NIST Risk Management Framework (SP 800-53) and well understood among the vendor stakeholder community. However, we caution against converting Common Criteria into a set of requirements for the software development lifecycle in the commercial space due to several challenges, including: significant costs and a lengthy and bureaucratic process heavily weighted to government needs. ITI emphasizes that references to Common Criteria should pertain only to substantive elements of the standard, not expanding the levels of Common Criteria evaluations. NIST could also work with technical communities to accelerate and enhance Protection Profile development, including to refine Common Criteria Protection Profiles designed to meet the USG's requirements, while allowing flexibility for vendors in the commercial space and avoiding fragmentation with existing broadly-adopted approaches. Further, as technology and consumer needs constantly change, NIST should continue to work with industry to consider and adapt to new developments in software engineering and service delivery, such as agile methodologies and secure dev/ops techniques. ITI also notes the importance of the NIST Software Security Framework, OWASP Software Assurance Maturity Model (SAMM), and Building Security In Maturity Model (BSIMM) as effective frameworks.

Other useful standards include: ISO/IEC 15408 [covers configuration management (change control), secure delivery (of the product), development security (i.e., the development environment), flaw remediation (bug handling/vulnerability disclosure), lifecycle definition, tools, and techniques][1]; ISO/IEC 30111, 29147, 27001 and 27035, which are more broadly applicable in this domain; and ISO/IEC 27036 (guidance for managing supplier relationships to secure information systems. These documents cover ICT products and services as well as cloud services.

Any secure development recommendation must be based on a process-centric approach such as SAFECode Fundamental Practices for Secure Software Development or ISO 27034 (also applicable in the context of secure supply chain).

[1] Supplements also cover patch management, as well as topics guidance documentation, vendor testing, and vulnerability analysis.

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

Proposed guidelines, best practices, or standards adopted pursuant to the EO must also be technology-agnostic and focus on risk-based practices, procedures and architecture guidelines to secure development and account for the risk levels associated with software components. This approach will help companies tailor the guidelines, best practices or standards to the type of software.[2] Additionally, we emphasize that "best practices" are not one-size-fits-all; some companies have made significant investments in security-first approaches using secure development standards honed over many years. A reference list of useful practices mapped to standards is a helpful tool, but companies should ultimately be afforded the latitude to determine which mix is most appropriate.

3. Guidelines outlining security measures that shall be applied to the federal government's use of critical software

Although the ISO/IEC 27000 family of standards are not specific to software, they contain basic requirements for an information management system. Uptake in U.S. government agencies is low due to U.S. regulation requiring the use of the control set defined in FISMA (SP 800-53). However, SP 800-53 does map between the two, and it is often used by suppliers to government agencies, especially cloud providers. ITI recommends that the U.S. continue building on existing programs such as FedRAMP instead of introducing something new. For cloud services, it is not useful set different requirements for the security of the software inside the service; holistic appraisals of overall cloud security, such as those provided by FedRAMP, are more appropriate than considering only software-specific elements. Additionally, ISO/IEC 27001 is designed for organizations of all sizes in a variety of technology areas, and it is well respected internationally. Since the NIST Cybersecurity Framework (CSF) maps to ISO/IEC 27001/2 controls, ITI recommends continuous improvement of the NIST CSF. Therefore, if a supplier has built an ISMS using ISO 27001 instead of NIST SP800-53, it should be recognized as a valid control framework. Security Technical Implementation Guides (STIGs), Security Content Automation protocol (SCAP) and Viewer Tools, and the macOS Security Compliance Project also provide some tools on configuration. In general, ITI recommends that critical software deployed by the government not utilize traditional network-level access systems for use, management, or support. Critical systems must be deployed in a manner that ensures a Zero Trust Architecture to support the function of the relevant software or system.

4. Initial minimum requirements for testing software source code

Overall, ITI members caution against the use of mandatory source code testing, particularly when such mandates require the sharing or disclosure of source code to government authorities or other third parties. Enshrining source code testing as a tool or panacea would require significant resources to triage and explain the results, should the customer demand them, and could detract from overall security gains. While these tools may identify issues, they are not without their limitations, as they do not indicate whether any of the issues identified by the tools are in fact exploitable, as there could be a check elsewhere in the code that prevents exploitation. Relying on source code testing runs the risk of a high return of false positives and requires unnecessary resource expenditures, which is not a risk-based approach. In addition, most organizations develop internal testing guidelines; however, these are often classified as IP, since they can refer to build instructions, compiler settings, etc. Disclosure of this sensitive information could also be used by malicious actors. If NIST pursues minimum requirements for source code testing, ITI recommends exploring what can be leveraged from the Common Criteria ISO/IEC 15408 standard for the specification of testing families (functional testing, coverage, and depth of testing) and the Tools and Techniques family and other ISO/IEC standards. SP 800-63 Rev1: *Vetting the Security of Mobile Applications* is a relatively new endeavor promulgated by NIST and could have value either for vendor standards or as standard measures for the government before it deploys software. As mentioned above, any secure development recommendation must be based on a process-centric approach such as SAFECode Fundamental Practices for Secure Software Development or ISO 27034.

5. Guidelines for software integrity chains and provenance

We encourage NIST to leverage and align with existing international standards for software integrity chains and provenance, including: ISO/IEC 20243:2018 Open Trusted Technology Provider (O-TTPS), ISO/IEC 30111 (2019), and 29147 (2018) for coordinated vulnerability disclosure (CVD) and ISO/IEC 27035 in the domain of incident management. As NIST looks to develop guidelines pertaining to vulnerability disclosure, NIST should ensure that guidelines do not require companies to unnecessarily disclose information that, if exposed, could put customers at risk.

[2] For example, firmware, which is software embedded in hardware, is developed differently than other software and thus a different approach may be needed.