NIST Request: Position Papers on Standards and Guidelines to Enhance Software Supply Chain Security

NowSecure Response #5 - *"Guidelines for software integrity chains and provenance."*

NowSecure, Inc. (parent company viaForensics, LLC)
1608 Spring Hill Rd, Ste 200, Vienna VA, 22182
NowSecure has 12 years in mobile app forensics, mobile app security testing, test automation, mobile pen testing and mobile security standards development.

Date Submitted: Wednesday, May 26, 2021 Submitted by: Jeff Miller, Director US Public Sector - jmiller@nowsecure.com Gentry Sims, Director Fed Bus Dev - gsims@nowsecure.com	Contributors: Alan Snyder, CEO - asnyder@nowsecure.com Andrew Hoog, Founder - ahoog@nowsecure.com Brian Reed, CMO - breed@nowsecure.com Brendan Hann, PMM - bhann@nowsecure.com

NowSecure recognizes the criticality of addressing software integrity chains for securing mobile apps and reducing risk for all organizations

- Specify the use of predefined standardized SBOMs that includes key identifying information such as source provider, version, etc.
- Consider the creation and use of standardized labelling and establish credentialing system to identify proper, valid sources of supply chain code with corresponding certifications
- For consistency and ease of adoption, consider leveraging the application software standards to be defined in the project and how to apply those standards and requirements for software components themselves in the supply chain.

Regarding open source provenance, NowSecure recommends DevSecOps environment with shared code repositories and automated continuous security testing:

- Enables the 'prior tested and repeatedly reviewed' content for frequent use by the Federal community.
- In order to meet this requirement, organizations will have to implement multiple assessment types, and disparate tools become hard to manage.