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

NowSecure Response #1 - *“Criteria for designating critical software”*

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 recommends that “mobile applications” be addressed as a specific and distinct category of “critical software” in the standards definition process because:

- Mobile Applications now account for approximately 70% of ALL digital time spent online across web and mobile browsers and applications, according to research data from CommScore.
- Mobile Application architecture and risk profiles are very different from web and desktop applications. The security and testing standards must take into account their unique characteristics and mobile OS dependencies.
- Mobile Applications have significant risks with potential for sensitive data leakage including geolocation tracking, access/transmit/store PII, access to adjacent apps/services (SMS text messages, call logs, contact database, browsing history, and ability to manipulate data for negative outcomes.
- Other standards groups have recognized that mobile, web and desktop apps are different from security and risk perspectives and therefore created specific security standards for mobile apps, including MITRE with the MITRE Mobile ATT&CK Framework and OWASP with the OWASP Mobile Top 10 and OWASP MASVS, and NIAP with the Mobile App Protection Profile.
- Mobile applications are the primary interface for IOT devices, of which a subset are a part of critical software in use by Government agencies. The ioXt alliance certification standard for IoT-connected mobile apps and mobile VPNs have been built leveraging the OWASP MASVS with refinements as needed to fit specific IoT and VPN requirements.

In order to speed the creation, delivery, and adoption of new security standards based on the Executive Order, NowSecure recommends leverage the existing OWASP MASVS Standard with a focus on automation as foundation for any new security testing standards. Please see question #4 and Response #4 for deeper detail on an effective approach to address creation of new standards leveraging existing OWASP MASVS for the purposes of this project.