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

NowSecure Response #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."*

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 simple, effective standards and best practices to enable maximum adoption across software developers building apps for use by the federal government.

- Commercial software vendors, systems integrators and internal federal software development teams will more rapidly incorporate standards and best practices that are clear and concise and easy to implement.
- Consider optimizing for speed and ease of use for faster adoption (vs depth of 'perfect security') in whole or in the first phase, then if needed over time potentially incorporate more complex security requirements based on context.
- For consideration, a lesson learned from NIAP compliance is that the requirement for deep security testing that requires non-automated, manual attestation slows down the process and has reduced speed of app releases and delayed ATO certifications for federal use.
- To help drive understanding and adoption to all software developers, create a set of easy to access reference guidelines available online and promoted across the industry.

NowSecure recommends that standards and best practices incorporate support for Agile and DevSecOps methodologies, enabling speed with security built in.

- All organizations use a variety of pipeline tools to build software including IDEs, CI/CD platforms, build systems, code repositories, ticketing systems, and more where integration and automation are used to enable team productivity
- To drive adoption, scalability, efficiency and repeatability, focus on standards and best practices that leverage automation and integration across these tools. Building security automation into each phase of the development lifecycle and toolchain will enable teams to more easily deliver secure code at low friction and high scale.

- Ultimately the best practice goal should be to integrate “continuous security testing” throughout the development process as the best way to reduce risk and ensure high quality, secure code production.
- Encourage creation of secure internal code repositories inside software development teams with pre-secured, pre-vetted code. A national tracking system for secure code libraries, SDKs, and third party components may serve to secure the software supply chain.
- Specify a simple standard SBOM in human and machine readable formats that can be generated throughout the development process and be shared easily upon completion to all stakeholders.
- The USAF BESPIN program is an example of development and security teams running an effective, scalable DevSecOps Program.

NowSecure suggests the creation of a shared repository for application development best practices and common vulnerabilities available to all software developers.

- Similar to the MITRE ATT&CK framework, a platform enabling broad access to proper application coding (minimum crypto) and security concerns (faulty APIs, proper use of SSL, etc) may be created as a shared resource for mobile application developers.
- Resources could be provided by NIST and the federal government or through industry partnership and contribution. The OWASP Web and Mobile Projects for example have substantial resources that could be leveraged.

NowSecure suggests a national software developer engagement program.

- Create a program to engage the world’s largest and most prominent software vendors and development companies to leverage the new resources and standards, and as importantly, encourage them to speak and promote the use of the new standards and resources across the industry
- Engage with large vendors such as Microsoft, Google, IBM, Amazon, and Apple, and trailblazers like Netflix, Uber, and Instagram to use and speak publicly about the standards.
- Engage with application development tools, IDE, SDK and framework vendors to build in security features, secure code, and security capabilities into their tools and speak publicly about them such as JetBrains, Jenkins, node.js, and Xamarin.

Consider a multi-level badge or labelling program for software developers to use in their materials that certifies the use of or compliance with new standards. A badge or labelling system can help drive visibility for the program and encourage wider developer adoption.