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

In response to the EO on Improving the Nation's Cybersecurity of 12th May 2021

Mastercard appreciates the opportunity to submit comments to NIST on Standards and Guidelines to Enhance Software Supply Chain Security. Mastercard as the world's premier payment network provider, and part of the PCI council, has a rich history of creating and nurturing security and cybersecurity standards which protect digital payment networks while facilitating a rich ecosystem of innovation and entrepreneurship within the companies who provide software to banks, merchants and payment providers. Mastercard has also invested significantly in small businesses, committing $250m to provide SMB cybersecurity solutions to help during Covid-19, and foundational payment systems to support B2B payments.

Please find below our comments tracking the areas of inquiry posted by NIST

1. Criteria for designating "critical software."

With the definition of critical software, we encourage NIST to consider the ramifications of software concentration within a multi-level supply chain. Software not deemed as critical by one entity directly doing business with the groups subject to the EO may be indeed critical to the downstream supply chain, or may be common, ubiquitous or essential within "suppliers of suppliers". Concepts such as downstream supply chain visibility should be included in NISTs response when determining the criticality of software, or the tools, libraries and third parties required to create such software.

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

Mastercard through its membership of the PCI Council collaborates and publishes the following standards related to secure software development

a. PCI Software Security Framework – **Secure Software Lifecycle Requirements and Assessment Procedures** which expand traditional Software Development Lifecycle processes with baseline security requirement and corresponding assessment procedures. This document guides software vendors in the design, development and release of secure software and encompasses topics such as authority and accountability, access to code, correct sensitive data handling, release control, vulnerability management, versioning and change management, methodology, use of open source and third party components, and other topics related to the lifecycle management of software to ensure integrity, authenticity, and discipline within the software lifecycle.

b. PCI Software Security Framework – **Secure Software Requirements and Assessment Procedures** which provides a baseline of security standards with corresponding assessment procedures for building secure software, guiding developers of software to use strong principals to ensure correct implementation of security controls, definition of critical and mission-critical functions and assets, elimination of unused functionality, cryptography, key management and data leakage prevention, elimination of "developer accounts" and back door access, concepts of zero trust and least privilege access, correct retention, deletion and handing of sensitive data, authentication, attack mitigation, and other topics related to the development of robust software with minimal opportunity for misuse or exploitation.

The PCI Software Security Framework was developed in partnership with a global community of contributors across the payment ecosystem landscape and has wide interest within the fintech community and also a vibrant ecosystem of companies able to assess and audit software and the software development lifecycle of companies providing it. These audits are known to be fair and to ensure that payment related software remains one of the most robust categories of software. This framework will become a required standard in late 2021 as the predecessor PA-DSS sunsets.

> "With the exception of the Secure Software Lifecycle (Secure SLC) standard developed by PCI Security Standards Council, few software development life cycle models explicitly address software security in detail."
> Kevin Stine, Chief of the Applied Cybersecurity Division at NIST

The PCI Software Security Framework is well aligned with NIST Secure Software Development Framework (SSDF), with common expectations and objectives. Both cover fundamental security principles and objectives that support secure software, regardless of the type of software or the industry. The alignment is significant enough to facilitate joint engagements between the PCI Council and NIST, including a recent publication with Kevin Stine (Chief of the Applied Cybersecurity Division at NIST) and Troy Leach (SVP Chief Engagement Officer at PCI Council) titled *NIST and PCI SSC Find Common Ground in Development of Software Frameworks.*

4. Initial minimum requirements for testing software source code including defining types of manual or automated testing

We would caution NIST in requiring or mandating certain tools or practices to be used in manual or automated testing – given such a wide range of development languages, processes and environments, creating an exhaustive list of processes would be perpetually out of date and ineffective. Rather, we recommend NIST express the desired objective, risk, or outcome of testing and enable the industry to seek the most appropriate way to measure and demonstrate such through an auditable process. We would recommend that attempts to automate risk elimination through technologies such as source code scanning may have the unintended consequence of increasing risk as software developers focus on "clean reports" rather than exploitable functionality which is not related to coding mistakes. The PCI standards mention above encompass testing methodologies based on risk assessment and functional testing, combined with auditable automation and test strategies.

We would encourage NIST to consider the needs of software vendors both in terms of strong guidance in creating secure software, but also the burden of third-party audits on both software and software development processes. The PCI standards have wide global adoption and a capable community of recognized auditors able to qualify adherence with minimal business disruption to diligent adherers.