Response of Red Hat, Inc. ("Red Hat")
to NIST's Request for Position Papers on Standards and Guidelines to Enhance Software Supply Chain Security
May 26, 2021

Red Hat appreciates the opportunity to comment on the above-referenced matter in anticipation of the Workshop scheduled for June 2 and 3. As the leading provider of open source software solutions (using a community-powered approach to deliver resilient and high-performing cloud, Linux, middleware, storage and virtualization technologies), Red Hat welcomes the release of the Executive Order on Improving the Nation's Cybersecurity. Red Hat looks forward to working with NIST to identify standards, tools, best practices, and other guidelines to enhance the software supply chain.

Red Hat plays a critical role in developing and supporting the full life cycle of our open source software offerings for our customers in the US government, critical infrastructures, and many mission-critical environments. We refer NIST to the Red Hat Risk Report for an understanding of how quickly vulnerabilities affecting our products are addressed.

To achieve the greatest degree of success, NIST should build on its foundation of work that touches on most of this inquiry's topics, relying on recognized global standards and best practices. Any proposed new (or changes to existing) guidelines, best practices, or standards must avoid technical, prescriptive or product-specific mandates, and must be consistent with a risk-based approach to develop and account for the risk level associated with a given software component.

It is also critical that the guidance and best practices are not framed as 'open source' vs 'proprietary', *per se*. As the Department of Homeland Security concluded, "Software can have low or high quality, regardless of whether it is OSS or not. … Actually, it's pretty easy to get malware into proprietary software."[1] The Department of Defense likewise cautions that "[t]he use of software with a proprietary license provides absolutely no guarantee that the software is free of malicious code. Indeed, many people have released proprietary code that is malicious. What's more, proprietary software release practices make it more difficult to be confident that the software does not include malicious code."[2]

As it undertakes its directives under the Executive Order, NIST's work should focus on how to enhance transparency, repairability, and resiliency that are essential to the trustworthiness of US government software assets.

1. The **definition of "critical software"** will determine the scope of the guidance NIST develops. Unfortunately, section 4(g) merely states that NIST "shall publish a definition of the term 'critical software' for inclusion in the guidance" without any requirement to get input from the private sector. It is essential

[1] Dr. David A. Wheeler and Tom Dunn, *Open Source Software in Government: Challenges and Opportunities*, Dept of Homeland Security, Aug 23, 2013, pp, 10,11.

[2] U.S. Dept of Defense, Chief Information Officer, *DoD Open Source Software (OSS) FAQL Frequently Asked Questions regarding Open Source Software (OSS) and the Department of Defense (DoD)*, 6.4 Q: Is there a risk of malicious code becoming embedded into OSS?, updated regularly, found at: https://dodcio.defense.gov/open-source-software-faq/#Q:_Is_there_a_risk_of_malicious_code_becoming_embedded_into_OSS.3F. "Such [proprietary] software does not normally undergo widespread public review, indeed, the source code is typically not provided to the public and there are often license clauses that attempt to inhibit review further (e.g., forbidding reverse engineering and/or forbidding the public disclosure of analysis results). Thus, to reduce the risk of executing malicious code, potential users should consider the reputation of the supplier and the experience of other users, prefer software with a large number of users, and ensure that they get the "real" software and not an imitator. Where it is important, examining the security posture of the supplier (e.g., their processes that reduce risk) and scanning/testing/evaluating the software may also be wise."

that this definition be narrowly tailored to address confidentiality, integrity, and availability, as directed in the Executive Order. We strongly recommend that the Secretary of Commerce, acting through NIST, seek public input on this fundamental element ***before*** the Secretary of Homeland Security, acting through the Director of CISA, provides agencies a list of categories of software and software products in use or in the acquisition process that meet this definition.

2. NIST should build an **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** from the foundation of work it already has in hand, e.g.: (a) Common Criteria (ISO/IEC 15408:2019), which includes requirements for the software development lifecycle as well as other topics related to this inquiry, which is recommended in the NIST Risk Management Framework, and reflected in Security and Privacy Controls for Information Systems and Organizations (SP 800-53 rev 5)[3]; (b) Secure Software Development Framework (SSDF) practices which are defined in the NIST Cybersecurity White Paper, Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF); (c) ISO 27001; (d) the Open Trusted Technology Provider Standard (ISO 20243:2015); (e) ISO/IEC 15408 (configuration management, change control, development security, flaw remediation (bug handling/vulnerability disclosure), lifecycle definition, tools, and techniques; and (f) ISO/IEC 27036 (managing supplier relationships).

3. To develop **Guidelines outlining security measures that shall be applied to the federal government's use of "Critical Software," including but not limited to, least privilege, network segmentation, and proper configuration**, NIST should utilize developed standards and guidance to draw on. These include, e.g., (a) ISO/IEC 27000 family of standards which include the basic requirements for an information management system and are designed for organizations of all sizes, as well as diverse technology environments; and (b) SP 800-53 Rev. 5, which provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks.

4. NIST will need to tread carefully to develop **initial minimum requirements for testing software source code** so as to avoid directly or indirectly prescribing specific technology, tools or proprietary solutions. We strongly urge NIST to focus on performance requirements and outcomes. In this regard, building on frameworks such as Common Criteria ISO/IEC 15408 as a well recognized standard outlining testing families (functional testing, coverage, and depth of testing) is a solid starting point.

5. Many of the above referenced standards and guidance are relevant to development of **Guidelines for software integrity chains and provenance**, as many of the Workshop topics are integrally related. The Open Trusted Technology Provider Standard (ISO/IEC 20243:2015), in particular, provides NIST with a set of guidelines, requirements, and recommendations that address specific threats to the integrity of hardware and software products throughout the product life cycle.

Contact:

Mark Bohannon
Vice President, Global Public Policy
& Associate General Counsel
Red Hat, Inc.
markb@redhat.com

Vince Danen
Senior Director, Product Security
Red Hat, Inc.
vdanen@redhat.com

[3] This reference to Common Criteria is only to the substantive elements found in the standard, especially those related to security testing. We do not recommend requiring more common criteria security evaluations, or pursuing higher assurance levels, to achieve the goals of the Executive Order.