Mr. Kevin Stine
Chief Cybersecurity Advisor and Chief
Applied Cybersecurity Division
National Institute of Standards and Technology

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

International Business Machines Corporation (IBM) is pleased to provide the following comments to the National Institute of Standards and Technology (NIST) regarding its forthcoming Standards and Guidelines to Enhance Software Supply Chain Security (Guidance), as required by President Biden's *Executive Order on Improving the Nation's Cybersecurity (14028)*.

IBM has a deep and long-standing commitment to cybersecurity and supply chain integrity and welcomes the opportunity to collaborate with NIST on these important and timely topics. IBM encourages NIST to base its Guidance on existing NIST, global and industry-led standards, guidelines and best-practices.

Topic 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.

IBM urges NIST to derive this list from existing global standards, best practices and guidelines, rather than create new frameworks that might be duplicative of what already exists and impose additional burdens for both industry and government without improving cybersecurity protections in any meaningful way. Such an approach will drive consistency, and also allow organizations to focus resources on strengthening existing controls to enhance software security, rather than pursuing additional compliance exercises under new standards. Focusing resources on the consistent application of existing and common standards will result in better cybersecurity overall.

NIST already has done extensive work, partnering with industry, to develop the NIST Secure Software Development Framework (SSDF). IBM encourages NIST to leverage this and other commonly accepted global standards for cybersecurity, secure product development, and supply chain integrity. Widely adopted global standards such as the SDDF, NIST SP 800-53, ISO 27001 and ISO 20243 already provide meaningful guidance and a strong foundation for organizations to rely on when shaping their cybersecurity policies and practices. Notably, ISO 20243 already requires organizations to periodically attest to their conformance with secure software development practices and open source software practices. Rather than develop new certification requirements for suppliers and developers, NIST should leverage existing attestation schemes to facilitate increased transparency and accountability regarding secure software development.

Topic 3: Guidelines outlining security measures that shall be applied to the federal government's use of "Critical Software."

Guidance on the government's use of "Critical Software" should focus – as the plain text of the EO makes clear – on the use of Critical Software rather than impose additional requirements on the development and supply of Critical Software. Of course, Critical Software should comply with any software development lifecycle and supply chain risk management standards that NIST develops under other portions of the referenced Executive Order. Therefore, the requirements for Critical Software should logically focus on best practices for secure deployment and operations.

For private sector organizations operating Critical Software for the federal government (e.g., managed service providers), the Guidance should allow for reliance on existing cybersecurity frameworks, such as FedRAMP or System and Organizational Controls (SOC), and their respective audits, as evidence of appropriate practices. The Guidance also should reflect that cybersecurity is a shared responsibility between clients and service providers and thus should account for the desired level of control of, and division of responsibilities among, federal government agencies and service providers to implement cybersecurity best practices.

Topic 4: Initial minimum requirements for testing software source code.

Software providers should be required to demonstrate ongoing software testing and scanning practices. Industry standard audits are IBM's recommended mechanism for evidence of those practices (e.g., SOC2), as they confirm sustained execution of such practices. Software providers, however, should not be required to provide actual security scan test reports. Security scans, by design, identify many false positives, disclosure of which to the government would not be of material value (and, in fact, might be burdensome for both government and industry). They also only demonstrate security at a point in time, rather than an ongoing sustained security practice. The disclosure of security testing procedures, with industry standard audits confirming sustained execution of these procedures, should be the focus of any requirements in this area.

Topic 5: Guidelines for software integrity chains and provenance.

The ultimate goal in assessing integrity and provenance is trust - trust that software is secure and performs as expected. Multiple methods exist for assessing trust, depending on the nature and complexity of the software. For example, industry standards and their associated audits and compliance attestations, such as ISO 20243, can demonstrate trust that software was created in a secure manner. NIST guidelines focusing on integrity and provenance should draw upon these existing standards and best practices.

Furthermore, the Guidance should recognize that the provenance and integrity of any software source code, be it open source or proprietary, can best be established by automated or manual review and testing of the code itself. If source code is unavailable or proprietary, then other proxy tests - such as certifications of secure development practices or compliance with industry standards - can be useful.

IBM also recommends that the Guidance remains technology-agnostic. Dictating a specific technological solution might risk the federal government inadvertently favoring one platform or solution over others that provide comparable benefits, would limit the ever-evolving advancements in the software development field and unnecessarily hamper innovation.

Finally, NIST should work closely with software development experts to avoid seemingly simple but impractical-to-implement Guidance. For example, a requirement to "disclose where the software was developed" may seem straightforward. In reality, however, most software applications draw upon dozens or even hundreds or thousands of software libraries and modules, underlying components of which are often developed by companies, suppliers, and open-source communities over many years, involving the collective efforts of hundreds of contributors. Attempting to determine the location where any given contributor wrote any particular line of code is impossible. Furthermore, the location of the coder is of only minimal relevance when the code itself is available for review, or where it is subjected to automated or manual scanning and testing for security.

William Tworek
Vice President & Distinguished Engineer
Product Security
IBM
tworek@ibm.com

Frank V. Fontana
Associate General Counsel, Regulatory Compliance
IBM
ffontana@us.ibm.com