April 25, 2022

National Institute of Standards and Technology
100 Bureau Drive, Gaithersburg, MD 20899

Re: Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management
[Docket Number: 220210-0045]

Dear NIST,

BlackBerry appreciates the opportunity to provide input on the evaluation and improvement of the NIST Cybersecurity Framework as well as NIST's new effort to improve the cybersecurity of supply chains. For over 35 years, BlackBerry has invented, created, and built security solutions to give people and businesses the ability to stay secure and productive. Today, BlackBerry continues to put that trusted security protection everywhere, from cars, to mobile devices, to laptops, based on our industry proven secure software development practices. We recently gained company-wide OpenChain ISO/IEC 5230:2020 conformance and collaborated with OSS Consultants to achieve accreditation, demonstrating BlackBerry's ability to manage the use of open source software across our Cybersecurity and IoT product portfolios[1].

BlackBerry strongly supports NIST's leadership in advancing the Framework and supply chain security in order to address the changing landscape of cybersecurity risks and technologies. Below, we provide our detailed views and inputs to the questions raised in the NIST RFI. In short, we recommend that **NIST preserve the Framework as a flexible, comprehensive and voluntary cybersecurity risk management guidance. We recommend, as a potential first step towards this end, NIST developing a best practice guide based on real use cases that successfully address evolving threat landscapes with emerging cybersecurity concepts, principles and technologies -- for example, Zero Trust tenets and AI/ML powered threat prevention, detection and response.**

For the alignment or integration with other risk management resources, we believe it is imperative to **keep the Framework backward compatible and avoid unnecessary inter-dependency with other resources**. Instead of merging or integrating these resources, NIST should clearly illustrate the intended alignment (commonalities and differences) between them, as well as how organizations can take advantage of them to successfully build and advance risk management systems suiting their organizations' business goals. BlackBerry encourages **NIST to promote the Framework's mutual recognition, where appropriate, with other well-adopted global and regional standards** to advance its adoption by wider industries.

With regard to cybersecurity supply chain risk management, BlackBerry recommends NIST lead the nation by **setting long-term goals and a roadmap to advance supply chain cybersecurity**, whilst continuing its effort to **enhance the guidance supporting Executive Order (EO) 14028**

[1] https://www.blackberry.com/us/en/company/newsroom/press-releases/2022/blackberry-strengthens-software-supply-chain-with-corporate-wide-openchain-conformance

-- for example, the attestation and verification of vendor's secure software development practices.

Use of the NIST Cybersecurity Framework

1. *The usefulness of the NIST Cybersecurity Framework for aiding organizations in organizing cybersecurity efforts via the five functions in the Framework and actively managing risks using those five functions.*

The five functions provide helpful guidance to organizations that are establishing their cybersecurity risk management systems from scratch. At the same time, the flexible design of the functions enables organizations that have already established and been managing their own risk management systems to overlay the Framework Core to review and improve their existing risk management process. The Framework can work with widely adopted risk management standards and guidelines including NIST SP 800-37r2 (Risk Management Framework), ISO/IEC 27001 (Information Security Management), or AICPA's Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

2. *Current benefits of using the NIST Cybersecurity Framework. Are communications improved within and between organizations and entities (e.g., supply chain partners, customers, or insurers)? Does the Framework allow for better assessment of risks, more effective management of risks, and/or increase the number of potential ways to manage risks? What might be relevant metrics for improvements to cybersecurity as a result of implementation of the Framework?*

For those organizations whose cybersecurity risk management is based on the Framework, the use of common vocabulary defined in the Framework significantly improves the efficiency of communications on cybersecurity (e.g., risks and requirements) between them. BlackBerry suggests NIST develop key terminology mapping between the Framework and other widely adopted risk management resources (e.g., Framework Tiers) to improve cybersecurity risk communications with organizations using other frameworks or resources.

With regard to the relevant metrics for improvements, organizations should determine the best metrics and measurements to evaluate the effectiveness of their own cybersecurity management systems. A number of cybersecurity KPIs are available, such as risk register entry count, control count (% assessed, % effective), remediation status of risk treatment plan, vulnerability scan and traffic trends, incident trends, and work volume. Organizations need to select and tailor the KPIs to suit their needs.

3. *Challenges that may prevent organizations from using the NIST Cybersecurity Framework or using it more easily or extensively (e.g., resource considerations, information sharing restrictions, organizational factors, workforce gaps, or complexity).*

In BlackBerry's view, the key value of the Framework is its flexibility and comprehensiveness. It can be overlayed with existing risk management systems organizations have in place. However, it may require additional expertise (and cost) to identify and implement the best approach to integrating the Framework into an organization's existing risk management practices. Without a clear ROI, an organization's management may choose to reject the cost associated with such an effort.

4. *Any features of the NIST Cybersecurity Framework that should be changed, added, or removed. These might include additions or modifications of: Functions, Categories, or Subcategories; Tiers; Profile Templates; references to standards, frameworks, models, and guidelines; guidance on how to use the Cybersecurity Framework; or references to critical infrastructure versus the Framework's broader use*.

BlackBerry supports the evolution of the Framework to meet the changing landscape of cybersecurity risks. At the same time, we would highlight the importance of preserving the key values of the current Framework as a voluntary, flexible, and comprehensive guidance. As the current Framework has already been widely adopted and tailored by entities across critical infrastructure sectors, the structure of the Framework Core should be preserved to the extent possible. We support NIST enhancing the information references by updating and adding resources that address evolving cybersecurity risks, e.g., NIST SP 800-161 (C-SCRM guidance), and developing new profiles to address emerging cybersecurity risks.

5. *Impact to the usability and backward compatibility of the NIST Cybersecurity Framework if the structure of the framework such as Functions, Categories, Subcategories, etc. is modified or changed.*

Considering the Framework's widespread adoption, BlackBerry urges NIST to avoid significant changes impacting its backward compatibilities. Many critical industries and private sector entities have voluntarily adopted and tailored the Framework to their needs in establishing their cybersecurity management systems. In this regard, we stress the importance of preserving the voluntariness and flexibility of the Framework. Introducing significant changes or adding to the Framework language specific to a certain application or sector should be avoided to the extent possible to minimize impacts to the current implementation and use cases of the Framework.

6. *Additional ways in which NIST could improve the Cybersecurity Framework, or make it more useful*.

BlackBerry believes that a further explanation on the Framework Core, Tiers and Profiles, reflecting the Framework's current use cases and the changing cybersecurity landscape would be helpful. As a first step in any effort to update and improve the Framework, we recommend NIST develop a best practices guide for using the Framework based on real use cases that successfully address the evolving threat landscape applying emerging cybersecurity concepts, principles and technologies. As demonstrated below, Zero Trust tenets and AI/ML powered threat prevention, detection and response enhances the Framework's outcomes.

- Continuous authentication based on user and entity behavior analytics (UEBA) utilizing AI/ML models significantly improves Identity Management, Authentication and Access Control (PR.AC).

- AI/ML powered endpoint protection, detection and response can prevent, detect and remediate zero-day attacks, thus enhancing Anomalies and Events (DE.AE), Analysis (RS.AN) and Mitigation (RS.MI).

<u>Relationship of the NIST Cybersecurity Framework to other Risk Management Resources</u>

7. *Suggestions for improving alignment or integration of the Cybersecurity Framework with other NIST risk management resources. As part of the response, please indicate benefits and challenges of using these resources alone or in conjunction with the Cybersecurity Framework. These resources include:*

   - *Risk management resources such as the NIST Risk Management Framework, the NIST Privacy Framework, and Integrating Cybersecurity and Enterprise Risk Management (NISTIR 8286).*

   - *Trustworthy technology resources such as the NIST Secure Software Development Framework, the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline, and the Guide to Industrial Control System Cybersecurity.*

The NIST risk management resources mentioned above were developed and evolved with specific goals in mind. For example, the Framework was developed pursuant to the February 2013 Executive Order 13636, Improving Critical Infrastructure Cybersecurity, and the Cybersecurity Enhancement Act of 2014.

As the Framework is already widely adopted by both the public and private sectors, BlackBerry would stress the importance of maintaining its independence from the other risk management resources and avoid creating unnecessary inter-dependencies when considering such alignment or integration. Rather, we propose NIST develop a high-level guidance document illustrating the intended alignment of the Framework with other NIST resources by delving into how the goals of each resource relate to each other and how the resources can most effectively be applied as building blocks to achieve an organization's cybersecurity goals.

We appreciate the progress NIST has made thus far to demonstrate the relationship of the Framework to other risk management resources and to clarify its alignment to them. For example:

- NIST SP 800-37r2 (Risk Management Framework (RMF)) shows the relationship mapping from the RMF tasks to the Framework, and the NIST Online Informative Reference (OLIR) catalog includes the reverse mapping.

- NIST OLIR catalog includes the relationship mapping from the Framework Core to SP 800-53 and SP 800-171 controls.

- NISTIR 8269 series (Cybersecurity risks for enterprise risk management) explain how to integrate the Framework to Enterprise Risk Management (ERM), and the NIST OLIR catalog includes the relationship mapping from the Framework Core to ERM.

- NIST 800-213A (IoT Device Cybersecurity Guidance for the Federal Government) shows the relationship mapping from the Framework Core to the IoT device cybersecurity requirements, and the NIST OLIR catalog covers the mapping.

BlackBerry supports NIST continuing OLIR development and refining the existing relationship mappings, as doing so will contribute to the improved alignment of the Framework with other NIST resources. For example, NIST may consider developing relationship mapping from the Framework Core to the Secure Software Development Framework's practices, tasks and implementation examples. We recommend NIST avoid the addition of software development specific descriptions to the Framework to the extent possible due to the importance of preserving the Framework as a flexible, and comprehensive cybersecurity risk management guidance.

8. *Use of non-NIST frameworks or approaches in conjunction with the NIST Cybersecurity Framework. Are there commonalities or conflicts between the NIST framework and other voluntary, consensus resources? Are there commonalities or conflicts between the NIST framework and cybersecurity-related mandates or resources from government agencies? Are there ways to improve alignment or integration of the NIST framework with other frameworks, such as international approaches like the ISO/IEC 27000-series, including ISO/IEC TS 27110?*

With regard to the ISO/IEC 27000-series standards, the Framework shares commonalities including the layered management structure, continuous improvement and outcome-oriented requirements. However, ISO/IEC 27001 follows the harmonized structure to facilitate integration with other ISO management system standards -- which is different from the Framework.

BlackBerry commends NIST's effort in establishing the Framework as an international information security management system standard and technical specification. ISO/IEC 27002:2022, updated this year, assigns each of its security controls with the cybersecurity concepts, i.e., the Framework functions. ISO/IEC 27110 defines the cybersecurity concept based on the Framework Core functions. We recommend NIST continue its active participation in ISO and refine the cybersecurity concepts at the Framework category or subcategory level in a new publication, e.g., a revision of TS 27110 or a new publicly available specification.

9. *There are numerous examples of international adaptations of the Cybersecurity Framework by other countries. The continued use of international standards for cybersecurity, with a focus on interoperability, security, usability, and resilience can promote innovation and competitiveness while enabling organizations to more easily and effectively integrate new*

technologies and services. Given this importance, what steps should NIST consider to ensure any update increases international use of the Cybersecurity Framework?

BlackBerry acknowledges the importance of evolving international cybersecurity standards to enable organizations to continue to integrate innovative technologies and services into their risk management system. To this end, future international cybersecurity standards must remain technology agnostic and focus on the attributes mentioned above (e.g., interoperability) and backward compatibility.

We would also stress the importance of recognizing other widely adopted global or regional cybersecurity risk management standards, e.g., the ISO/IEC 27000 series of standards, as it is not practical to unify the existing risk management standards. In this regard, we recommend NIST promote mutual recognition of the Framework and other existing widely adopted standards by developing or refining the vocabulary and relationship mapping. Mutual recognition of the Framework and its counterparts could expand the market for cybersecurity products and services developed according to the Framework, thus promoting wider adoption of the Framework.

10. *References that should be considered for inclusion within NIST's Online Informative References Program. This program is an effort to define standardized relationships between NIST and industry resources and elements of documents, products, and services and various NIST documents such as the NIST Cybersecurity Framework, NIST Privacy Framework, Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53), NIST Secure Software Development Framework, and the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline*

BlackBerry supports NIST's commitment to its Online Informative References (OLIR) program and defining standardized relationships between NIST and other key risk management resources. As mentioned in our response to question 7, we appreciate the OLIR catalogs NIST has made available, and suggest that mappings shown below would help clarify the Framework's alignment to the following NIST resources:

- The Framework to NIST Secure Software Development Framework
- The Framework to NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline

We also recommend NIST provide opportunities for public review of the OLIR catalogs to refine the relationship mapping. For the standardization of relationship, the refined mapping can be included in the relevant risk management resources, as already accomplished in SP800-37r2.

As a long-term goal, BlackBerry encourages NIST to consider developing common control requirements shared by all the risk management resources NIST has developed. The relationship of a newly introduced risk management resource can be specified to the common control requirements, rather than defining its relation against all the existing resources. This would reduce the OLIR program resource required and help organizations understand the goals of the new resource and make finding the best approach to utilize it easier.

Supply Chain Risk Management

11. *National Initiative for Improving Cybersecurity in Supply Chains (NIICS). What are the greatest challenges related to the cybersecurity aspects of supply chain risk management that the NIICS could address? How can NIST build on its current work on supply chain security, including software security work stemming from EO 14028, to increase trust and assurance in technology products, devices, and services?*

BlackBerry thinks that the greatest challenge NIICS could address would be development of long-term actionable goals and a roadmap to achieve the trust and assurance of the supply chains involved in technology products and services. Such a roadmap would need to address the cybersecurity measures necessary to increase the transparency of supply chains from federal agencies and final product assemblers to the most upstream suppliers.

With regard to EO 14028, we commend NIST's commitment and progress thus far in providing guidance covering key issues including the critical software definition, testing and verification, secure software development framework and attestation. While this guidance increases transparency and trust across the software supply chain, NIST in collaboration with stakeholders must continue updating and refining the guidelines to keep improving supply chain cybersecurity. For example:

- <u>Attestation and verification of secure development practices</u>
  Further improvement of efficient and sustainable verification of the vendor attestation can include architecture or a model to support secure discovery and exchange of artifacts between the interested parties, and the clarification of high-level artifacts introduced by the NIST guidance on EO Section 4(e)[2].

- <u>Critical software definition for embedded systems</u>
  As mentioned in NIST's guidance pursuant to the EO Section 4(g), critical software has taken a phased approach. NIST can review and refine the existing definitions based on stakeholder feedback, and extend its scope to firmware and embedded systems in the second phase.

12. *Approaches, tools, standards, guidelines, or other resources necessary for managing cybersecurity-related risks in supply chains. NIST welcomes input on such resources in narrowly defined areas (e.g. pieces of hardware or software assurance or assured services, or specific to only one or two sectors) that may be useful to utilize more broadly; potential low risk, high reward resources that could be facilitated across diverse disciplines, sectors, or stakeholders; as well as large-scale and extremely difficult areas.*

There are evolving standards for managing cybersecurity related risks in supply chains. These include, for example, OWASP's recently published Software Component Verification Standard

[2] https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.pdf

(SCVS), and OpenSSF's development of a Supply Chain Level of Software Artifacts (SLSA) standard.

BlackBerry would highlight the importance of high-level architecture and tools integration to enable the automation of processes assisting supply chain risk assessment and integrity verification – this would help to achieve prevention as well as faster detection and remediation of threats inherent in supply chains. We recommend that NIST develop such common architecture and models that are agnostic to specific implementations, as the logical Zero Trust architecture was defined in SP 800-207. Meanwhile, an NCCoE project to validate and verify the evolving standards and develop best practices would inform future approaches to take the EO effort to the next level.

In narrowly defined areas including software and service assurance, BlackBerry stresses the importance of utilizing widely adopted, industry proven frameworks as the baseline for managing supply chain cybersecurity to avoid re-inventing a wheel. We recommend NIST consider AICPA's Trust Services Criteria and rigorous third-party audit standards such as International Standard on Assurance Engagements (ISAE) 3000 to assure a supplier's ability to deliver trustworthy products and services. BlackBerry has witnessed a high level of demand from critical industries, including the financial and healthcare sectors, for compliance reports according to these standards.

13. *Are there gaps observed in existing cybersecurity supply chain risk management guidance and resources, including how they apply to information and communications technology, operational technology, IoT, and industrial IoT? In addition, do NIST software and supply chain guidance and resources appropriately address cybersecurity challenges associated with open-source software? Are there additional approaches, tools, standards, guidelines, or other resources that NIST should consider to achieve greater assurance throughout the software supply chain, including for open-source software?*

The February 25, 2022 report "Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry" issued by the Department of Commerce and the Department of Homeland Security identifies many of the risks inherent within hardware, firmware, software (including open-source software) and extended supply chains.

Compared to the domain of IT cybersecurity, BlackBerry notes a much wider variety of hardware designs found among embedded devices deployed in the IoT domain. This, in addition to the associated diversity in file formats and architectures, make accurate composition analysis of these devices far more challenging. A trusted, well understood hardware bill of materials (HBOM) would help with risk assessment, including cybersecurity vulnerabilities and supplier source identification. Considering CISA's leadership on advancing the security and resilience of industrial control systems (ICS), NIST should closely collaborate with CISA and develop technical guidance and best practices to support their vision and plan.

Concerning open-source software, BlackBerry commends both the Office of National Cyber Director (ONCD)'s line of effort and OpenSSF's initiatives to boost the security posture of open-source software. It is imperative to identify and secure critical open-source projects whose vulnerabilities can impact a large span of society, as well as to ensure that consumers of open-source software uptake improvements made by the initiative. To this end, we encourage NIST, in collaboration with OpenSSF and other open-source communities, to develop guidance and best practices for software suppliers to take advantage of open-source community efforts (e.g., open-source project score cards, dependencies identified within open-source packages) to help software suppliers achieve greater assurance of their software products.

14. *Integration of Framework and Cybersecurity Supply Chain Risk Management Guidance. Whether and how cybersecurity supply chain risk management considerations might be further integrated into an updated NIST Cybersecurity Framework – or whether and how a new and separate framework focused on cybersecurity supply chain risk management might be valuable and more appropriately be developed by NIST.*

As explained in our response to question 7, BlackBerry recommends that NIST preserve the Framework as voluntary, flexible, and comprehensive guidance for cybersecurity risk management to avoid disruptive impacts to public and private sector entities who have adopted the Framework. In this regard, we think the framework and Cybersecurity Supply Chain Risk Management (C-SCRM) Guidance should evolve separately. The Framework can reference the C-SCRM Guidance and the OLIR program can develop detailed relationship mapping from the Framework Core to the C-SCRM controls.

Summary

BlackBerry strongly supports NIST's leadership for improving NIST Cybersecurity Resources: he Cybersecurity Framework and Cybersecurity Supply Chain Risk Management. Takashi Suzuki (email: tsuzuki@blackberry.com) is pleased to address any questions or comments you may have regarding BlackBerry's response.

Respectfully submitted,

Takashi Suzuki

Takashi Suzuki
Senior Director, Standards