March 17, 2023

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

RE: NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework

Dear NIST,

BlackBerry appreciates the opportunity to provide input on the structure and direction of the Cybersecurity Framework (CSF or Framework). For nearly 40 years, BlackBerry has invented, created, and built security solutions to give people and businesses the ability to stay secure and productive. Today, BlackBerry's trusted security protection can be found everywhere – from cars, to mobile devices, to laptops, based on our industry proven secure software development practices. BlackBerry develops credible, secure solutions, which e.g. are certified against ISO/IEC standards including 27001, have adopted OpenChain ISO/IEC 5230:2020, and include FedRAMP authorized products[1].

We believe the Framework can be 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 to review and improve their existing risk management process.

Below, you will find our responses to questions posed in Concept Paper. We have retained the original numbering of the questions in their headings.

1. CSF 2.0 will explicitly recognize the CSF's broad use to clarify its potential applications

Increase (international) collaboration and engagement (1.3)

Various standards developing organizations have mapped their standards to the Framework. Unfortunately, often these mappings cannot be obtained via the National Online Informative References (OLIR). Other mappings, available via the OLIR, are published several years after the latest version (1.1) of the Framework became available. Finally, widely adopted risk management standards and guidelines, including ISO TR 27103, appear not to have been mapped. Finally, ISO TS 27110 may need to be aligned with a future version of the Framework.

Many organizations have made it clear that international use of the Framework would improve the efficiency and effectiveness of their cybersecurity efforts. NIST should further prioritize its participation in international standards activities that leverage the Framework as part of a broader effort and prioritize engaging strategically in the work of (international) standards developing organizations. In this regard, we recommend NIST promote 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.

[1] BlackBerry Certifications, https://www.blackberry.com/us/en/company/certifications

While BlackBerry notes NIST's call to action: "*Call to Action – Provide Mappings: NIST welcomes submissions of mappings to the CSF*", we also recommend that NIST takes the initiative. To improve the efficiency and effectiveness of cybersecurity efforts by the industry, BlackBerry supports NIST prioritizing increasing connections by participating in and/or encouraging mapping efforts.

2. CSF 2.0 will remain a framework, providing context and connections to existing standards and resources

Retain CSF's current level of detail (2.1) & relate the CSF clearly to other NIST frameworks (2.2)

We stress the importance of preserving the voluntariness and flexibility of the Framework. Many (critical) industries and private sector entities have voluntarily adopted and tailored the Framework to their needs in establishing their cybersecurity management systems. Furthermore, the National Cybersecurity Strategy[2] leverages the Framework when setting necessary cybersecurity requirements; states and independent regulators are recommended to leverage the Framework for the same, significantly increasing its adoption. Any discrepancies between the present version of the Framework and a future version may cause disruptive impacts to public and private sector entities who have adopted the Framework.

Additionally, when subjects like supply chain security[3] or secure software development[4] are incorporated into a future version of the Framework, we recommend they be incorporated by reference (i.e. references to existing NIST frameworks or practices).

Leverage Cybersecurity and Privacy Reference Tool for online CSF 2.0 Core (2.3)

BlackBerry finds that the Cybersecurity and Privacy Reference Tool (CPRT) is a valuable resource and commends NIST for making it available. We recommend that NIST continue to enhance the CPRT, adding additional mappable standards.

Remain technology- and vendor-neutral, but reflect changes in cybersecurity practices (2.6)

We recommend that NIST develop common architecture and models that are agnostic to specific implementations e.g., like the logical Zero Trust architecture as defined in SP 800-207[5].

3. CSF 2.0 (and companion resources) will include updated and expanded guidance on Framework implementation

General

BlackBerry highlights the importance of preserving the key values of the current Framework as a voluntary, flexible, and comprehensive guidance. Any profiles, updated or expanded guidance should remain informative and continue to permit integration with other widely adopted risk management standards and guidelines or already established risk management systems.

---

[2] 2023 National Cybersecurity Strategy, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[3] Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf
[4] Secure Software Development Framework (SSDF) Version 1.1, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf
[5] Zero Trust Architecture, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Add implementation examples for CSF Subcategories (3.1)

BlackBerry supports inclusion of implementation examples, for example demonstrating how to leverage other NIST efforts in order to achieve Subcategory outcomes. We demonstrate below how Zero Trust tenets and AI/ML powered threat prevention, detection and response can enhance the outcomes:

- Continually authenticating 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).

For example BlackBerry notes the Subcategory PR.AC-7, recommending authentication using single-factor or multi-factor authentication procedures. This fails to highlight the option to judiciously – when warranted by changes in a risk score – initiate re-authentication procedures: "*[c]ontinually prompt[ing] a subject for reauthentication against behavior that is consistent with historical trends and norms for their mission function and role within the organization*" [NIST TS 800-207, p.20].

4. CSF 2.0 will emphasize the importance of cybersecurity governance

Add a new Govern Function (4.1)

BlackBerry recommends that NIST avoid disruptive impacts to public and private sector entities who have adopted the Framework (e.g., due to guidance in the 2023 National Cybersecurity Strategy).

5. CSF 2.0 will emphasize the importance of cybersecurity supply chain risk management (C-SCRM)

Expand coverage of supply chain (5.1)

BlackBerry recommends that NIST aim to avoid disruptive impacts to public and private sector entities who have adopted the Framework (e.g., due to guidance in the 2023 National Cybersecurity Strategy). In this regard, we think the framework and Cybersecurity Supply Chain Risk Management (C-SCRM) Guidance should evolve separately.

6. CSF 2.0 will advance understanding of cybersecurity measurement and assessment

Provide examples of measurement and assessment using the CSF (6.2)

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. The Framework can include example measurement and assessment.

7. Conclusion

BlackBerry has compared the Framework with our existing risk management process, which includes national and international standards, including the aforementioned ISO/IEC standards, etc. The Framework is a helpful guidance and can serve to review and improve existing risk management processes. BlackBerry recommends close alignment between the Framework and standards, where they may exist. We believe this is the surest path to wide adoption of the Framework.

We appreciate the opportunity to offer our input. Mr. John-Luc Bakker [redacted] is available to respond to any questions concerning BlackBerry's response.

Respectfully submitted,

J.H.L. Bakker

John-Luc Bakker
Director, Standards

BlackBerry Corporation
3001 Bishop Drive, Suite 400, San Ramon, California, 94583 USA. tel: +1 (925) 242-5660 fax: +1 (925) 242-5661