Comments of Arceo Labs Inc. (D.B.A. Resilience)
To the Department of Commerce, National Institute of Standards and Technology
Re: Request for comments and feedback on the NIST Cybersecurity Framework 2.0 Concept Paper

March 17, 2023

Resilience submits the following comments in response to the Department of Commerce, National Institute of Standards and Technology Cybersecurity Framework 2.0 Concept Paper.[1] We appreciate the opportunity to provide input to this important process.

Resilience provides cyber risk management solutions through two separate entities that support purchasing both cyber insurance and cyber risk visibility products. Together these solutions help organizations bridge the internal silos between finance, risk management, and IT security to build resilience to cyber threats. This new approach for managing cyber risk holistically, while relatively novel today, has the opportunity to become the best-in-class approach for organizations that seek to mature their cyber defense capabilities. Approaches like the NIST Cybersecurity Framework (the Framework) also promote this more holistic approach to cyber risk management. We believe that NIST can make significant improvements in version 2.0 by further incorporating some of the approaches we have developed to build cyber resilience in our client base.

Resilience has been supportive of promoting the Framework by working to incorporate it into the presentation of cyber risk data to our clients. Additionally, Resilience's founding employees were involved in the initial development and launch of the Framework and believe this tool has tremendous value for organizations working to optimize how they assess and invest against their cyber risk. The current version of the Framework acknowledges the role that cyber risk management plays in securing enterprises, noting:

Implementation of risk management programs offers organizations the ability to quantify and communicate adjustments to their cybersecurity programs. Organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery

[1] https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf

of critical services. The Framework uses risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity. [2]

However, since the initial drafting of the latest version of the Framework, there have been significant improvements in the cyber risk management space. NIST appears to recognize the importance of updating the Framework's guidance on cyber risk management. Section 4.2 ("Improve Discussion of Relationship to Cyber Risk Management") of their 2.0 Concept Paper notes:

Revising the CSF offers an opportunity to clarify the relationship among governance and cybersecurity risk management... CSF 2.0 will describe how an underlying risk management process is essential for identifying, analyzing, prioritizing, responding to, and monitoring risks, how CSF outcomes support risk response decisions (accept, mitigate, transfer, avoid), and various examples of risk management processes (e.g., Risk Management Framework, ISO 31000) that can be used to underpin CSF implementations.

Resilience would suggest examining how harmonizing cyber risk quantification and prioritization, cyber threat visibility, and cyber risk transfer can benefit organizations' cyber risk management. The synchronization of these three areas provides a more holistic approach to building cyber resilience that the NIST should further explore in the upcoming version 2.0 of the Framework.

Cyber Risk Quantification & Prioritization:

Section 6.2 of the CSF 2.0 Concept Paper calls for organizations to "share information with NIST about how they are using the CSF to measure and assess their cybersecurity." Resilience greatly appreciates this increased interest in measuring cyber risk and believes there is significant value in further exploring the topics of cyber risk quantification and prioritization of investment in security controls.

Version 1.1 of the Framework begins with identifying cybersecurity risks to an organization's systems, people, assets, data, and capabilities. Resilience has found that this process is significantly enhanced by quantitative modeling around the probability of realistic cyber incident scenarios impacting an organization's ability to operate. Instead of jumping straight to a discussion of assets, organizations should start by aligning on key business objectives and what cyber incident scenarios may impact operations most. Once all executive stakeholders understand and agree upon these scenarios, an

[2] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

organization can begin identifying systems, people, assets, data, and capabilities that impact or are impacted by, those scenarios.

As an organization understands its systems, people, assets, data, it can then begin building out quantitative models to understand how investments in controls affect organizational operations. Quantitative analysis helps forecast not only the value-at-risk, but also their cost and effectiveness at controlling losses. This understanding can drive prioritization of the security controls discussed throughout the Framework. The acts of quantification and prioritization should be a key first step in utilizing the Framework, thus deserving of significantly greater exploration by NIST.

Cyber Threat Visibility:

Section 2.6 of the CSF 2.0 Concept Paper focuses on reflecting changes in cybersecurity practices while remaining technology neutral. One area of cybersecurity practice that has evolved dramatically in practice and technology since version 1.1 of the Framework is managing data that provides cyber threat visibility.

Technical visibility into threats is a foundational goal for any cyber defense effort. Understanding an organization's ability to identify and manage new and existing vulnerabilities is critical to limiting the attack surface for adversaries to access critical systems. However, as organizations' digital footprints have grown and expanded to SaaS vendors, along with digital dependencies of upstream and downstream supply chains, the volume of "doors and locks" that need to be routinely checked has become a Sisyphean task.

As with other aspects of Cyber Resilience, organizations, and the security vendors supporting them, need to prioritize threats and vulnerabilities based on their actual risk to business operations. This means limiting the scope of what is deemed critical enough to warrant investigation based on its context to overall risk. When Resilience provides threat notifications, we utilize a simple three-level requirement. All notifications to clients must be:

- Critical: The vulnerability must be of such a critical nature that it could lead to direct access to or control of a client's environment.
    - *Example: A remote code exploit (RCE) that provides access to operationally critical systems.*

- Relevant: The threat from the vulnerability must be relevant to the client's infrastructure or industry.
    - *Example: A vulnerability present in deployed IT infrastructure or common across their region, industry, or organization size.*

- Actionable: The outreach must come with remediation guidance that is specific enough to enable independent action.
    - *Example: The vulnerability is resident in commonly used infrastructure and can be patched using an update by the vendor through a trusted distribution chain.*

Cyber Risk Transfer:

Section 4.2 of the CSF 2.0 Concept Paper calls for an improved focus on, "how CSF outcomes support risk response decisions (accept, mitigate, transfer, avoid)." A cyber resilience approach to managing cyber risk requires holistic management of all four principles. However, security practitioners often overlook risk transfer products, such as insurance, as a tool for addressing cyber risk. We believe NIST has an opportunity to correct this and drive a better understanding of how to transfer cyber risk alongside mitigation strategies.

A critical component of holistic cyber management is the collaboration within an organization on their level of risk tolerance and the associated availability of financial risk transfer. To adequately manage cyber risk, it is important to determine what risks are acceptable as is, if risk mitigation is required, or if transferring the risk through insurance is the appropriate course of action. Emphasizing the role of risk transfer and the collaboration between security, finance, and risk management supports NIST's approach of analyzing cyber risk holistically. In many cases, the risk transfer product may also encourage organizations to pursue operational and technological advances to meet insurance requirements. Resilience believes this balance between risk identification, transfer, and mitigation deserves significant attention in future analysis by NIST.

In the current cyber risk transfer climate, insurance organizations are not solely financial risk transfer entities but rather partners that work collaboratively with their customers to advance cyber maturity and reduce cyber risk in a mutually beneficial way. Resilience hopes that its input will be helpful to NIST as it develops version 2.0 of the Framework. Should you have any questions, or if we can assist in any other way, please contact Davis Hake [redacted]

Respectfully submitted,

Arceo Labs Inc. (D.B.A. Resilience)