From: **Joseph Pidala**
Date: Mon, Apr 10, 2017 at 3:46 PM
Subject: NIST CSF Draft 1.1 | Cybernance
To: cyberframework@nist.gov
Cc: Charlie Leonard

Hello,

Cybernance composed feedback and comments addressing the NIST CSF Draft 1.1. These comments are attached as a PDF.

Kind regards,
Joseph

Joseph A. Pidala, GSEC

Product Manager

www.cybernance.com

Cybergovernance Journal

[Attachment Copied Below]

NIST CSF Draft 1.1 Response
Cybernance Corporation
April 10, 2017

Introduction
Cybernance employs the NIST CSF as the foundation of our automated SaaS cyber assessment and monitoring platform, which enables corporate directors and non-technical stakeholders to engage in cyber risk and resilience oversight. We have spent many hours in considering what areas are most important to address as the Framework evolves, and we appreciate this opportunity to offer our perspective.

Are there any topics not addressed in the draft Framework Version 1.1 that could be addressed in the final?

Organizations who do an effective job managing cyber risk take a collaborative approach that spans the entire enterprise. Board members, executives, and managers who are led by intuition that tells them "cyber is an IT issue" are likely to preside over an organization with myriad gaps in cyber risk controls. On the other hand, leaders who display far more maturity around risk management foster a collaborative approach to cybersecurity that draws on talents from internal auditors, general counsel, risk managers, and human resources. We believe this principle is embodied within NIST CSF, and that it would be beneficial to make it even more explicit. When we engage with executives, they often place responsibility for NIST implementation squarely on the shoulders of the CIO, CISO, or other IT function. This approach usually leads to less than adequate control implementations and can in fact increase the risk of a negative outcome.

Cyber risk can be addressed most effectively by a team of leaders who represent different areas of the enterprise. Extending this idea further, we encounter the reality that risk controls are most effective when their implementation considers the dependencies between them. We see some limited recognition of this concept in the C2M2 framework, in which the authors identify critical dependencies between individual controls. This concept has merit and can be extended into what might be called "sub-critical dependencies" or "interactive" control relationships. Exploration of this concept may lead to creating a more tangible understanding of how the five NIST Functions are interrelated. Such an understanding might be used to frame examples of who should be involved in certain areas. An outcome would be to convey the message that this issue is larger than information technology.

The NIST CSF "risk-based approach" is key in making the framework adaptive rather than prescriptive. Furthermore, it is helpful to create content that addresses the risk associated with failure to implement controls in each of the Functions, Categories, and Sub-Categories. For example, if a company has inadequate capabilities in the Detect Function (or specific failings at

the Category or Sub-Category level), then the Framework could describe the potential risk associated with not implementing improved capabilities.

How do the changes made in the draft Version 1.1 impact the cybersecurity ecosystem?

With continued cyber breaches often resulting from poor supply chain management, emphasizing SCRM controls is very important. While NIST 800-161 succeeded as an interim reference document, we have found organizations using supply chain controls as a side project. It has been proven time and time again that organizations are only as secure as their weakest link. Now that SCRM controls are integrated into the NIST CSF, we expect to see the controls being more widely adopted in commercial industries. These controls are an excellent step toward codifying the genetic structure of cyber supply chain risk. To take this farther, implementing SCRM controls as a part of a recognized standard could be useful in quantifying risks by sharing anonymized data across industries, and eventually, globally. Vendors have an inherent risk that can affect most of their buyers and partners. If information about specific vendors were shared across the many buyer organizations, the ecosystem as a whole could improve.

For those using Version 1.0, would the proposed changes impact your current use of the Framework? If so, how?

Since the NIST CSF lives at the core of our platform, all our software functions would be impacted, but in a good way. These updates, especially in SCRM and metrics/measures, are what our customers are requesting. Version 1.1 will allow us to build out improved supply chain functionality in our platform. Along with software functionality, the other impact to our platform is in the crosswalks with other frameworks, such as HIPAA, ISO 27001, and C2M2. To align NIST with industry and international standards, the crosswalks also need to be updated.

The integration of metrics and measurements is very compelling. The concept helps better delineate the relationship between quantitative and qualitative measures. That said, the wording and description of metrics and measures is not precisely clear in Table 1 Section 4.2. One of the best characteristics about the NIST CSF is it gives non-technical leaders the ability to determine cause-and-effect relationships between cyber and the business.

Further, non-technical examples of metrics and measures can help non-technical stakeholders better understand how these can be used in their organization. CIO.gov at https://cio.gov/performance-metrics-and-measures/ provides an excellent description of the distinction between metrics and measures:

> "There is overlap between measures and metrics. Both can be qualitative or quantitative, but what distinguishes them is important. Measures are concrete, usually measure one thing, and are quantitative in nature (e.g. I have five apples). Metrics describe a quality and require a measurement baseline (I have five more apples than I did yesterday)."

Incorporating such terminology may improve the widespread adoption of metrics and measures.

For those not currently using Version 1.0, does the draft Version 1.1 affect your decision to use the framework?

While we heavily use the NIST CSF internally and with our customers, we see Version 1.1 as an improvement with minimal downsides.

Does this proposed update adequately reflect advances made in the Roadmap areas?

The "NIST Roadmap for Improving Critical Infrastructure Cybersecurity" speaks deeply to "Automated Indicator Sharing." Cooperation across industries is essential to protecting the critical infrastructure cybersecurity. There is a great opportunity for NIST CSF 1.1 to emphasize the idea of information sharing to a greater degree. Efforts by NIST to promote anonymized information sharing have not gone unnoticed (e.g. the collaboration with CIDAWG/CIDAR), and these efforts should be incorporated in the NIST CSF. This issue is currently growing exponentially as the federal government continues to advocate for the NIST CSF to be the standard across the United States. Analytics to gauge alignment with the NIST CSF would significantly improve the critical infrastructure and resilience across verticals.

Is there a better label than "Version 1.1" for this update?

Version 1.1 is the correct name and standard across frameworks.

Based on this update, activities in Roadmap areas, and activities in the cybersecurity ecosystem, are there additional areas that should be added to the Roadmap? Are there any areas that should be removed from the Roadmap?

With increasing regulation, particularly in the EU, adding additional privacy guidance as sub-categories could help the NIST CSF grow into the internationally accepted "gold standard" for cybersecurity frameworks. While Section 3.6, "Methodology to Protect Privacy Policy and Civil

Liberties," provides a good process for relating privacy to cybersecurity, incorporating frameworks such as GDPR as informative references could enhance international acceptance. We agree with NIST's consideration to address privacy and civil liberty implications as a part of the Framework Core (as mentioned in Appendix A) and "to efficiently operate globally and to manage new and evolving risks."

Submission By

Charles F. Leonard, COO, Cybernance Corporation
Joseph A. Pidala, Product Manager, Cybernance Corporation