NFPPC NATIONAL FORUM FOR PUBLIC PRIVATE COLLABORATON

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

10 March 2017

Dear Edwin,

Please find our comments related to the NIST Cybersecurity Framework Draft 1.1 attached.

Public and private organizations are under pressure to identify, understand, and respond to a multitude of federal, state, and local regulations. The role of the framework must stay above regulation and stay in the realm of enablement.

Continual effective public and private internal and external collaboration will be required to find effective ways to determine measurable approaches that are both "reasonable" and "prudent". Cyber resilience/security must be tightly coupled with and support business value. These approaches are found by including collaboration in each organizations strategy to support their missions.

It is not reasonable or prudent for Michael Phelps's swim coach to protect his shoe size at the same level of his doctor for his medical care records, or a swim fin manufacturer protecting the intellectual property of a new line of Michal Phelps signature training fins. Therefore, we must not rush into this document being the source of how things are measured.

We suggest NIST stays out of the swim lane of prescribing how organizations set up metrics to use relating to the framework. If this document gets too prescriptive it could unintentionally inhibit organizational effectiveness.

Each sector is unique. Sectoral and cross-sectoral collaboration is required as we look for reasonable and prudent approaches that work for all.

Traditional risk management tends to look at the negative side of risk which often leads to no. A more holistic view of risk management would better enable us to take advantage of existing common investments in people, processes, and technology as well as leveraging new opportunities.

Thank you.

Warm Regards,

Charles Tupitza
Chief Executive Officer
National Forum for Public Private Collaboration
www.nfppc.org
202 839-4096
charlie.tupitza@nfppc.org

CYBERSECURITY FRAMEWORK DRAFT 1.1 COMMENTS

Page 1: Second Paragraph

"The resulting Framework, created through collaboration between 75 government and the private sector, uses a common language to address and manage 76 cybersecurity risk in a cost-effective way based on business needs without placing additional 77 regulatory requirements on businesses."

If you are reading this document you are utilizing a common language. This document seems to be attempting to provide a common lexicon. Care should be given with the lexicon used when describing activities outside the documents purpose. This can create confusion and may limit many existing effective approaches to achieve organizational resilience and security.

Beyond this we need a common basic lexicon so we understand each other because all parts of the business need to be involved.

What happened to this collaboration between 1.0 and 1.1?

There was a great deal of interest from the participants in each session about sharing best practices at last year's Cybersecurity Framework event at NIST. What is the definition of a best practice?

Practices are contextual; what works in one context may be dangerous in another context. (David Marquet's *Turn the Ship Around* is an example)

It is not appropriate for the government to be the caretaker of "best practices". The term is inappropriate. "Best" is not "Best" for significant portions of public and private sectors effectiveness changes. There is danger in using this term and sharing without appropriate discipline. We will continue to operate with a changing threat landscape including different architectures, capabilities, and capacities to recognize respond and recover from all internal and external, intentional, and unintentional threats against the value of our business and customers. Any "practices", a preferred term, must have a disciplined continual improvement lifecycle associated with it. Measurements must be in place to identify increasing or degrading value over time.

Page 2: Second Paragraph

"The Framework is a living document and will continue to be updated and improved as industry provides feedback on implementation. NIST will continue coordinating with industry as directed in the Cybersecurity Enhancement Act of 2014"

NIST will participate in public/private collaboration coordinated by others as invited.

Page 2: Last Paragraph

"Use, evolution, and sharing of best practices of this voluntary Framework are the next steps to improve the cybersecurity of our Nation's critical infrastructure – providing guidance for individual organizations, while increasing the cybersecurity posture of the Nation's critical infrastructure as a whole."

What is the definition of a best practice?

Page 10: Tier 1 - Partial

- *External Participation – An organization may not have the processes in place to participate in coordination or collaboration with other entities.*

Page 10: Tier 2 - Risk Informed

- *External Participation – The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally.*

Page 11: Tier 3 - Repeatable

- *External Participation – The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.*

Page 12: Tier 4 - Adaptive

- *External Participation – The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.*

Collaboration is touched on in this document lightly. There is great value to an organization to have disciplined collaboration throughout. This document skips the value of internal and external public as well as public private collaboration. It seems to address collaboration in terms of threat sharing like the roles of ISAC's and ISIO's. This is valuable collaboration but collaboration should be expanded to other common interests and needs among participants.

Page 11: Tier 4 - Adaptive

*The organizational budget is based on understanding of current and predicted risk environment and future **risk appetites**.*

Risk appetite is not defined here use "organizational risk tolerance" from NIST SP 800 39.

Page 12: Paragraph three

Paragraph three is confusing.

Page 14: Paragraph Three

The Framework can be applied in design, build/buy, deploy, operate, and decommission system lifecycle phases."

Where did this "life cycle" come from? It fails to address the value of Strategy before Design, Transition, Operation, and Continual Improvement throughout an IT Service Management Lifecycle. This is one of the times in the life-cycle where stakeholders would consider buy or build depending on the organizations capabilities and capacities. How you manage internal or external resources are different and should not be considered the same.

Page 17: First Paragraph

"The practice of communicating and verifying cybersecurity requirements among stakeholders is one aspect of cyber supply chain risk management (SCRM). A primary objective of cyber SCRM is to identify, assess and mitigate "products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the cyber supply chain."

This is a good point. Along with this we need to articulate the importance of risk management in determining opportunities identified. We need to be more inclusive.

Page 17: Figure 3 - Cyber Supply Chain Relationship.

This is a confusing graphic. The supplier may be external to the organization, or an internal resource. They should not be considered the same. There are advantages and disadvantages of internal and external sources. SCRM may be addressed differently.

Page 18: First Paragraph

"Whether considering individual Subcategories of the Core, or the comprehensive considerations of a Profile, the Framework offers organizations and their partners a method of ensuring the new product or service meets security outcomes that are prioritized. By first selecting outcomes that are relevant to the context (PII transmission, mission critical service delivery, data verification services, product or service integrity, etc.) the organization can then evaluate partners against those criteria. For example, if a particular system is being purchased that will monitor OT, availability may be a particularly important cybersecurity objective to achieve and thus will drive Subcategory selection (ID.BE-4, ID.SC-3, ID.SC-4, ID.SC-5, PR.DS-4, PR.DS-6, PR.DS-7, PR.DS-8, PR.IP-1, DE.AE-5, etc.)."

Please clarify this in context.

Page 18: Identifying Opportunities for New or Revised Informative References

*"To address that need, the organization **might** collaborate with technology leaders and/or standards bodies to draft, develop, and coordinate standards, guidelines, or practices."*

The organization would benefit from collaboration among private and public organizations including standards bodies to draft, develop, and coordinate standards, guidelines and/or practices.

Page 18: Methodology to Protect Privacy and Civil Liberties

"Consistent with Section 3.4, technical privacy standards, guidelines, and additional best practices may need to be developed to support improved technical implementations."

Be careful with the phrase "best practice" without it being defined.

Page 31: = ID.SC-3

Strike "required".

*** END ***

Charles Tupitza

Lawrence Cooper and Jon Bradley assisted in this document.