Thank you for the opportunity to participate in NIST CSF 2.0. The NIST Cybersecurity Framework has been foundational to good cybersecurity practice across industries and around the globe. It occupies a unique place in the cybersecurity landscape for its scalability, ease of use, and holistic approach.

The Concept Paper's Call to Action specifically requests examples of how organizations are using the CSF to measure and assess their cybersecurity. I would like to proffer one approach that I have found helpful, as well as to suggest some direction on measurement, assessment, and metrics in the development of NIST CSF 2.0.

A key characteristic of the NIST CSF, highlighted in section 2 of the Concept Paper, lies precisely in that it is a framework and not a standard. Organizations of any size, in any industry, and at any maturity level may align to the NIST CSF to improve their cybersecurity posture. I believe that an overly detailed or quantitative approach to measurement, assessment, and metrics could undermine the framework's status as a framework, and that we should proceed cautiously.

There are many compliance standards which an organization may use for detailed metrics and third-party certification. Some, such as PCI-DSS, are industry-specific. Others, like the Center for Internet Security (CIS) Benchmarks, are technology-specific. Still others, including AICPA and ISO, provide clear criteria that can be verified by a third party for compliance. I believe an overly quantitative approach to measurement, assessment, and metrics in the NIST CSF runs the risk of making the NIST CSF just one more standard in fact if not in name.

To guard against this, I would suggest an assessment rubric aligned to the Capability Maturity Model Integration (CMMI) and oriented toward next steps for continuous improvement. An assessor can review each element of the CSF and record the People, Process, and Technology solutions currently employed before making a net assessment of maturity based on regular CMMI scoring. Based on the specific threats facing the organization, its risk tolerance, and its maturity score, logical next steps for People, Process, and/or Technology can be defined and planned.

Rubric:

1- Initial (characterized by ad-hoc and reactive processes)
2- Managed (characterized by repeatable processes)
3- Defined (characterized by well-defined, documented processes that are continually improved)
4- Capable (well-defined, documented and quantitatively tracked processes, tools, and standards)
5- Optimizing (processes that are continually monitored and improved).

CSF Element	People	Process	Technology	Maturity Level	Next Steps
Identify					
Protect					
Detect					
Respond					
Recover					
Govern					

I believe an approach like this would enable any organization, regardless of its size, industry, or maturity, to assess itself against the NIST CSF with an orientation toward continual improvement.   If a more detailed quantitative model is desired, an organization could assess against standards published for that purpose, such as the CIS benchmarks or ISO 27001.   But a lightweight approach such as proposed would ensure that the Framework remains a Framework, whose primary purpose is to drive strategy and to prioritize continual improvement actions.

The NIST CSF has been invaluable in my professional journey.   Thank you for allowing me to provide feedback on the Concept Paper and to participate in the workshops.

Sincerely yours,

Stephen Danckert
Senior Director, Enterprise Architecture & Data Protection Officer
Haemonetics

The opinions expressed here do not necessarily reflect those of Haemonetics or its officers.