DVMS Institute Response to the NIST-CSF 2.0. Concept Paper

For the past seven years, The DVMS Institute, in collaboration with governments and industry across the globe, has focused on creating Accredited Learning Systems and Resources designed to teach institutions of any size how to engineer, implement, audit, and innovate a Digital Value Management System™ (DVMS) to protect its digital business value across an enterprise and its supply chain. The Institute teaches organizations how to deliver the outcome the NIST Cybersecurity Framework was designed to deliver.

This DVMS overlay system leverages the NIST Cybersecurity Framework and existing digital service Creation (Planning), Protection (GRC), and Delivery (Implementation & Operations) systems to build an enterprise-wide, adaptive, cyber-resilient risk management program that is fit for use, auditable for purpose, and compliant with government cybersecurity mandates.

More information on the DVMS Institute and its CPD overlay model (including explainer videos) can be found at www.dvmsinstitute.com

Main Question Responses

1. Do the proposed changes reflect the current cybersecurity landscape (standards, risks & technologies)?

Yes. The Institute has included additional detail in each section.

2. Are the proposed changes sufficient and appropriate? Are there other elements that should be considered under each area?

Yes

3. Do the proposed changes support different use cases in various sectors, types, and sizes of organizations (and with varied capabilities, resources, and technologies)?

Yes

4. Are there additional changes not covered here that should be considered?

No

5. For those using CSF 1.1, would the proposed changes affect the continued adoption of the Framework, and how?

No

6. For those not using the Framework, would the proposed changes affect the potential use of the Framework?

Yes

Section Responses

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

Section 1.1, Change the CSF's title and text to reflect its intended use by all organizations.

The NIST Cybersecurity Framework brand is well established in the marketplace, so changing its name at this point may create confusion in the market, let alone a lot of documentation updates for governments and corporations that have included the NIST-CSF in government and corporate strategy documents etc.

However, the Institute recommends that NIST explore new naming options that expand the scope of the framework to include all aspects of a business (i.e., Digital Enterprise Cyber Framework, Digital Enterprise Value Framework, etc.)

Section 1.2, CSF Scope to ensure it benefits organizations regardless of sector, type, and size.

The current NIST-CSF scope works well when implemented and operationalized using an overlay model that leverages existing business systems as it enables organizations of any size to benefit from the framework not only in the context of managing its cyber risks but also in terms of cost to do so.

Section 1.3, Increase international collaboration and engagement.

The current NIST-CSF model is already widely adopted internationally, either by name or incorporated into other policy and program documents. The Institute agrees that having international translations, adaptations, and other resources for the CSF will expand its international footprint.

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

Section 2.1, Retain CSF's current level of detail

The Institute agrees with retaining the current Framework level of detail as it is easy to map to what other frameworks call capabilities (functions), practices (categories & subcategories), etc.

The Institute recommends changing references from "implementation" to "adoption" or "adaptation" as appropriate to the context. A framework is not "implementable," it serves as a guide.

Section 2.2, Relate the CSF clearly to other NIST frameworks.

The Institute supports NIST's position on keeping the NIST Cybersecurity Framework as a standalone publication and not integrated into other NIST Publications. The overlay model we mentioned earlier in our response, views each area (privacy, supply chain, workforce, etc.) as a separate business risk that can be factored into an organization's cybersecurity risk management program and managed using the informative references supplied by NIST or other standard bodies.

Section 2.3, Leverage Cybersecurity and Privacy Reference Tool for online CSF 2.0 Core

The Institute agrees that the CPRT tool will bring great value to organizations adopting and adapting the NIST-CSF.

Section 2.4, Use updatable, online Informative References

The Institute agrees that having updatable, online informative references will bring great value to organizations adopting and adapting the NIST-CSF.

The Institute recommends preserving the published references consistent with Table 1 and Table 2 in CSF 1.1. We also recommend adding a statement that links to the National Online Informative References Program (OLIR) Catalog to get the latest mappings from the Core to the selected informative reference(s).

Section 2.5, Use Informative References to provide more guidance in implementing the CSF

The Institute agrees that having more mappings to other standards, guidelines, and frameworks is a good idea. However, having these references as standalone PDF documents will bring limited value to the community, requiring an additional workforce to tie everything together in the program context. There are platforms available in the market today that do everything described in this question automatically, including cross-walking between standards, guidelines, and frameworks.

The Institute recommends using language that suggests each cybersecurity control represents a set of implementation requirements – it is the control requirements that are implemented, not the Framework. The additional examples should focus on the implementation of control requirements to achieve an organizational risk-based posture.

Section 2.6, Remain technology- and vendor-neutral, but reflect changes in cybersecurity

The Institute supports NIST's position on keeping the NIST-CSF technology vendor-neutral as the framework is centered around managing an organization's risk and resiliency in which any technology (old or new) is just another risk that needs to be factored into an organization's cybersecurity risk management program.

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

Section 3.1, Add implementation examples for CSF Subcategories

The Institute's position is that implementation examples be listed in the CSF Resource section and linked back to an actual cybersecurity control requirement(s) designed to deliver specific outcomes; otherwise, some may view what is listed in the NIST-CSF as practical guidance, which we believe is not part of the NIST charter.

Section 3.2, Develop a CSF Profile Template

The Institute agrees that using templates to map profiles to Categories and sub-categories is a valuable tool for organizations with a limited budget to adapt the framework to their business. Another option is to provide organizations with guidance on how to quickly adapt a minimum set of controls to stabilize their environment and then work from there to adapt additional controls to expand their defensible perimeter.

Section 3.3, Improve the CSF website to highlight implementation resources

The Institute views this as the most important update to the NIST-CSF. It would be great to have a resource website that presented organizations with a listing of FREE and FOR FEE NIST-CSF resources and services (i.e., training, mentoring, etc.) available to help organizations adopt and adapt the framework. This builds on the public/private partnership organized to create the framework.

Four working examples of this are the DHS-CISA-NICCS model, the NICE Workforce Framework job locater, the Department of Energy C2M2 for assessments, and the Linkedin NIST Cybersecurity Professional Community of Practice.

Section 4 - CSF 2.0 will emphasize the importance of cybersecurity governance

Section 4.1, Add a new Govern Function

The Institute supports the addition of a new Governance function for the NIST-CSF. We agree with the wording in the Concept paper to make this a crosscutting (or “wrapper”) function around the existing Core Functions. Approached in this way should alleviate the perceived serial nature of the current Core.

We also recommend changing the language from “…[implementing] each current Function” to “implementing appropriate the cybersecurity control requirements associated with each Function.”

Section 4.2, Improve the discussion of the relationship to risk management

The Institute recommends that governance be the “wrapper” around the other core functions and establish the basis for measurement. Governance in the CSF should be described as an extension of existing organizational governance versus governance for cybersecurity.

Section 5 - CSF 2.0 will emphasize the importance of cybersecurity supply chain risk management.

Section 5.1, Expand coverage of supply chain

The Institute overlay model, described in the opening paragraph, looks at the organizational supply chain as another risk it must mitigate and manage. Regarding the detail behind that risk, NIST has done a great job creating NIST publications 800-161, which organizations can use as their Informative Reference to deal with Supply Chain risks.

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

Section 6.1, Clarify how leveraging the CSF can support the measurement and assessment of cybersecurity programs

The Institute recommends that assessment and measurement should stem from governance and be included in every core function, cognizant of organizational strategic and operational intent. Note: this should be done in the context of the selected informative reference control requirements.

Section 6.2, Provide examples of measurement and assessment using the CSF

The Institute supports NIST's position to provide examples of measurement and assessment as a guide for organizations to adopt and adapt a model that works best for them in the context of the NIST-CSF. This should be in the context of the cybersecurity control requirements, not something in the Framework.

One example might be instead of aligning with assessment and measurement, consider aligning cybersecurity control requirement implementation phases with revised tiers and profiles to adapt the CSF.

Section 6.3, Update the NIST Performance Measurement Guide for Information Security

The Institute supports NIST's position on pointing those looking to measure NIST-CSF performance back to NIST Performance Measurement Guide for Information Security (800-55r2)

Section 6.4, Provides additional guidance on Framework Implementation Tiers

The Institute supports shifting the focus of Tiers to goals and objectives in the context of governance. The "Implementation Tiers" should be restructured to be "Adaptation Tiers" based on the selected informative reference control requirements.