[redacted] [redacted]
Subject: EXT :FW: CISA/CSD/CB comments to NIST in response to the CSF v2.0 Concept Paper
Date: Thursday, March 9, 2023 1:23:33 PM
Importance: High

CAUTION: This email originated from outside your organization. Exercise caution when opening attachments or clicking links, especially from unknown senders.

FYI

-----Original Message----[redacted]
Sent: Friday, March 3, 2023 9:26 AM
To: cyberframework <cyberframework@nist.gov>
[redacted]
Subject: CISA/CSD/CB comments to NIST in response to the CSF v2.0 Concept Paper
Importance: High

Good Morning,

Thank you for the opportunity to provide feedback on the CSF v2.0 Concept Paper. Tom Hallewell from the CISA/CB Performance & Accountability Team participated in the 2/15 virtual workshop. We look forward to collaborating with NIST on the journey to CSF 2.0.

CISA/CB realizes and acknowledge that the concept paper "does not cover all potential changes that may be made to the Framework structure, format, and content, especially specific changes to Categories and Subcategories of the CSF Core." We appreciate this advanced view into the topics being discussed. This team is pleased to provide specific thoughts about the potential changes described in the Concept Paper and would be happy to follow up directly if we can be of assistance. Each point includes a reference to the original section number from NIST's concept paper.

* [Concept Paper Section 1.1] While CISA certainly places great importance on critical infrastructure, we understand that making the title more general (i.e., removing critical infrastructure and renaming to simply Cybersecurity Framework) will ensure that a broader audience sees value in applying the framework, regardless of industry sector, entity type, or size. Also note that in most use cases to date, the Framework is already simply referenced as "the CSF" so this formal change seems completely appropriate.
* [Concept Paper Section 2.1] We feel that the current level of detail is appropriate, recognizing that CSF is intended to be paired with actual control-based solutions. Further, the implementation examples proposed by NIST will help to improve specificity.
* [Concept Paper Section 2.4] CISA will monitor progress and explore opportunities to use NIST's Online Informative References (OLIR) model. For example, it may be helpful to develop a mapping between federal directives (OMB M- memos, CISA Binding Operational Directives) and NIST reference/focal documents.
* [Concept Paper Section 2.6] We support the concept of "Remaining technology- and vendor-neutral, but reflecting changes in cybersecurity practices". Our team recognizes that this may be a balancing act, at times, and looks forward to working with NIST on how that would occur.
* [Concept Paper Section 3.1] As mentioned above, the implementation examples are likely to be very valuable. There may be an opportunity for CISA to provide federal-specific implementation examples for use by agencies.
* [Concept Paper Section 3.2] A federal CSF Target Profile that reflects federal goals and strategy might be useful for the broader FCEB community and might support future cybersecurity measurement.
* [Concept Paper Section 4.1] We recognize the value of separating strategy and expectations from

operations/implementation, though the line between governance and management is sometimes challenging to draw. We support the general approach described and look forward to additional details in the CSF 2.0 draft.

* [Concept Paper Section 5.1] CISA recognizes the importance of cyber-supply chain risk management and appreciates the inclusion of supply chain considerations in the CSF. CISA/CSD/CB concurs that NIST should not develop a separate Framework to address these risks.
* [Concept Paper Section 6.1] CISA/CSD/CB, in particular our Performance & Accountability Section, takes great interest in measurement and assessment topics. We support efforts to improve consistent models for performing and reporting assessment results.
* [Concept Paper Section 6.1] Many public- and private-sector organizations are stressing the need for maturity models. CISA/CSD/CB encourages discussion about what constitutes maturity, especially in light of federal initiatives to measure "cybermaturity". There are many existing criteria for measuring maturity, including the U.S. Inspectors General (IG) Evaluation Maturity Levels and the widely-adopted Capability Maturity Model Integration (CMMI) model. The community should examine what maturity means in a cybersecurity context, keeping in mind that such maturity should reflect improvement in people, process, and technology, but also that such improvement should be consistently implemented, consistently managed, and consistently measurable. Perhaps some of these considerations could be integrated into governance aspects.
* [Concept Paper Section 6.1] Where maturity/measurement are covered, CISA/CSD/CB supports additional mappings to key directives, along the lines of recent NIST work (e.g., mapping CISA ZTMM v1/v2 to the ZTA functions/CSF subcategories mapping as in NIST 1800-35E).
* [Concept Paper Section 6.3] CISA supports NIST's ongoing work for the Performance Measurement Guide for Information Security, SP 800-55r2, and will continue to participate in public draft reviews and comments.

Thank you for your team's continued work to update this framework and please feel free to contact us if we can be of assistance.

V/r,
Kim Isaac
Section Chief, Performance and Accountability