Public Draft: The NIST Cybersecurity Framework 2.0 National Institute of Standards and Technology

Released August 8, 2023

Cloud Security Alliance Comments/Suggestions

Summary of selected Framework changes from version 1.1 to this draft with comments

Recognize broad use of the Framework:

CSA Comments: The name change to “Cybersecurity Framework” from the original title is a welcome move as it reflects the broader applicability and user base of the framework.

The modified scope to encompass organizations of all sizes and nature, beyond just critical infrastructure, is commendable. This reflects the reality that cybersecurity is a concern for all entities, regardless of their scale or sector.

Internationalizing the framework further strengthens its relevance in a globalized world. Cybersecurity threats are borderless, and so should be the strategies to combat them.

Relate CSF to other Frameworks and resources:

CSA Comments: The integration and referencing of the newly introduced NIST guidelines and frameworks provide organizations with a cohesive and comprehensive set of resources. This could help streamline cybersecurity efforts and reduce potential overlaps or gaps.

The initiative to provide an online tool hosting CSF 2.0 Core in both human- and machine-readable formats can be instrumental in enhancing accessibility and usability for different stakeholders. CSA supports leveraging OSCAL (and/or JSON) as they are available models for Cloud Control Matrix as well.

Increase guidance on CSF implementation:

CSA Comments: Implementation examples are essential for organizations that may struggle to translate framework directives into practical actions. These notional examples can serve as starting points for companies to customize based on their unique requirements.

The revamped guidance on Framework Profiles is likely to enhance its application. Offering templates is a great way to facilitate quicker adoption.

While we know that the CSF is “voluntary” it would be advisable to publish guidelines on evaluating the level of compliance for internal auditors. This would provide an internal mechanism for evaluating, monitoring and maintaining an effective CSF and also provides a way of providing evidence of due diligence. CSA Created a similar guide for the Cloud Control Matrix. This can be developed through workshops with private industry.

We realize that there is a section on Assessing and Prioritizing Cybersecurity Outcomes with the Framework, but this section in our opinion, can be a bit confusing in how it is written. A formal compliance evaluation guide would clarify the process and formality of due diligence by providing an authoritative document that brings consistency and allows for an internal auditor calibration route.

Along these same lines, prioritization and assessment guidance related to different maturity levels would also be useful and provide organizations with an incremental enhancement roadmap for evolving enterprise cybersecurity.

Several appropriate implementation example references to Zero Trust were noted. These could potentially be expanded further, particularly in the context of securing critical infrastructure, including OT/IoT/ICS where in-built security capabilities are often limited and supporting micro segmentation controls are warranted.

Accordingly, the CISA Zero Trust Maturity Model V2 and the NSTAC Report to the President on Zero Trust and Trusted Identity Management (as well as other NIST and ZT (e.g. 207A) and NSA ZT and device protection guidance documents) would be useful additional references for both the Implementation Examples and core CSF the Next Steps section.

Emphasize cybersecurity governance:

CSA Comments: The introduction of the 'Govern' function is a significant step forward. Organizational context and an emphasis on governance are crucial for embedding cybersecurity deep within the organizational culture.

Bridging the Cybersecurity Framework with the NIST Privacy Framework can provide organizations with a holistic approach, especially when dealing with data protection, governance, and privacy issues.

The reiterated focus on people, process, and technology ensures a balanced approach to cybersecurity, ensuring no area is neglected. Bravo! There are too many solutions that throw technology at every problem.

Emphasize cybersecurity supply chain risk management:

CSA Comments: Given the increasing interdependencies in today's digital ecosystems, emphasizing supply chain risk management is timely. The integrated approach ensures that vulnerabilities in the supply chain do not become weak points for the organization.

The emphasis on secure software development is a positive step, considering the frequency of software-based vulnerabilities exploited by adversaries.

Clarify understanding of cybersecurity measurement and assessment:

CSA Comments: Regular assessment is essential to gauge the efficacy of cybersecurity measures. Directing users to NIST SP 800-55 offers clarity and standardization.

Refining the Tiers to concentrate on governance, risk management, and third-party considerations aids in sharpening the framework's focus and utility. We still believe the Tiers serve as a maturity status and should be treated as such.

If justification was required, it would be interesting to see a justification for a certain level with a possible action plan to improve over time.

Highlighting the importance of continuous improvement ensures that cybersecurity remains dynamic, adapting to evolving threats and challenges.

Conclusion:

The draft for NIST Cybersecurity Framework 2.0 appears to be a well-thought-out and comprehensive update. It embraces the dynamic nature of cybersecurity, emphasizing the importance of continuous improvement while also providing clearer guidance and actionable steps for organizations. The international scope and broadened application further increase its potential to benefit a wider range of stakeholders.