NIST Cybersecurity Framework

Rebellion Defense, Inc.'s Comments regarding NIST Cybersecurity RFI[1]

Use of the NIST Cybersecurity Framework

3. Challenges that may prevent organizations from using the NIST Cybersecurity Framework or using it more easily or extensively (e.g., resource considerations, information sharing restrictions, organizational factors, workforce gaps, or complexity).

Comment from Rebellion Defense: NIST CSF is a very broad framework that deliberately does not specify particular control requirements (how controls should be implemented). Other, more specific requirements exist across other regulatory frameworks like SOC, ISO, NIST 800-53, etc. A perennial challenge, however, has been mapping control requirements across frameworks. With a revamp to CSF, attention should be paid to how requirements from the new framework map to other major frameworks. Canonical/definitive mappings will save the industry countless hours of analyst time and make "interoperability" across frameworks more viable.

NIST CSF has a limited concept of maturity measurement. CSF control tiers (partial, risk informed, repeatable, adaptive) exist but little guidance is provided for assessing/assigning a maturity score to control implementation.

4. Any features of the NIST Cybersecurity Framework that should be changed, added, or removed. These might include additions or modifications of: Functions, Categories, or Subcategories; Tiers; Profile Templates; references to standards, frameworks, models, and guidelines; guidance on how to use the Cybersecurity Framework; or references to critical infrastructure versus the Framework's broader use.

Comment from Rebellion Defense: CSF was rolled out prior to widespread adoption of cloud. Framework is becoming increasingly challenging, particularly as it pertains to who owns what portion of the framework. Control responsibility is no longer clear and is typically shared across organizations and their IaaS/PaaS/SaaS vendors. CSF doesn't really deal well with shared control responsibilities.

How does the move to Zero Trust relate back to CSF which is more focused on things like role based access control and managing user permissions rather than on focus on least privilege.

---

[1]https://www.federalregister.gov/documents/2022/02/22/2022-03642/evaluating-and-improving-nist-cybersecurity-resources-the-cybersecurity-framework-and-cybersecurity

5. Impact to the usability and backward compatibility of the NIST Cybersecurity Framework if the structure of the framework such as Functions, Categories, Subcategories, etc. is modified or changed.

Comment from Rebellion Defense: It will be important to provide mappings from old to new. Many organizations have embedded CSF into their risk and security programs and understanding how existing programs map to the new framework will be important. Having to figure this out themselves would be very burdensome. Not just NIST CSF (Old) to NIST CSF (New) but NIST CSF to lots of other regulatory frameworks.

Cybersecurity Supply Chain Risk Management

12. Approaches, tools, standards, guidelines, or other resources necessary for managing cybersecurity-related risks in supply chains. NIST welcomes input on such resources in narrowly defined areas (e.g. pieces of hardware or software assurance or assured services, or specific to only one or two sectors) that may be useful to utilize more broadly; potential low risk, high reward resources that could be facilitated across diverse disciplines, sectors, or stakeholders; as well as large-scale and extremely difficult areas.

Comment from Rebellion Defense: Encourage standards of reporting from supply chain vendors. It would be useful were vendors held to provide standard, ideally automated visibility into system security.

14. Integration of Framework and Cybersecurity Supply Chain Risk Management Guidance. Whether and how cybersecurity supply chain risk management considerations might be further integrated into an updated NIST Cybersecurity Framework—or whether and how a new and separate framework focused on cybersecurity supply chain risk management might be valuable and more appropriately be developed by NIST.

Comment from Rebellion Defense: Preference for separate framework focused on cybersecurity supply risk management. Inclusion in the core CSF framework would seem overly specific in a framework intended to be as generic as possible. Yet for vendors who are part of supply chains, having a standard framework to follow would be useful. For organizations assessing their supply chain, having a common standard/benchmark to apply cross vendors would be valuable.

Other

Comment from Rebellion Defense:The move to remote workforce accelerated by COVID creates a very different cybersecurity ground truth than that CSF was intended to address. The security standards that need to be followed (e.g. focus on physical security) per frameworks like CSF and the actual security challenges experienced on the ground are quite different. Increasingly companies are spending resources to meet outdated standards that aren't actually making them more secure.