CSA Response to NIST Regarding the CSF 2.0 Core Discussion Draft

Subject: Feedback on NIST Cybersecurity Framework 2.0 Core Discussion Draft
Date: May 25, 2023

Dear NIST Cybersecurity Framework Team,

The Cloud Security Alliance (CSA) appreciates the opportunity to provide feedback on the discussion draft of the NIST Cybersecurity Framework 2.0 Core. We recognize the importance of this framework in addressing current cybersecurity challenges faced by organizations and aligning with existing practices and available resources. After reviewing the draft, we would like to offer the following feedback and suggestions for improvement:

Cybersecurity Outcomes:
a. The proposed Functions, Categories, and Subcategories provide a comprehensive structure. However, we recommend further consideration of cloud-specific security challenges, such as data privacy, data residency, and supply chain risk management, to ensure broader applicability in cloud environments.

b. We encourage the inclusion of outcomes that specifically address emerging technologies and associated risks, including artificial intelligence, Internet of Things (IoT), and blockchain, to account for evolving threats.

Implementation Examples:
a. The provided Informative Examples are valuable in guiding organizations on practical actions. We suggest expanding the range of cloud-specific examples to showcase effective implementation of the framework in cloud environments as this is the core of most security issues in today's ecosystem.

b. Expand on the examples and publish an “Implementation Guide”. The guide will help users understand how to navigate through the CSF and to use it effectively and interpret and implement the category and subcategory control specifications. CSA developed a similar guide for the CCM and would be happy to lead this development initiative.

c. Suggest a collaboration with cloud service providers (CSPs) and cloud service users (CSC) as well as private sector enterprises to develop a repository of implementation examples tailored to different deployment models that include the cloud (e.g., public, private, hybrid) and CSP-specific security controls would greatly benefit organizations.

d. Include possible metrics or KPIs that organizations could consider in order to provide a “dashboard” to facilitate continuous monitoring for real-time feedback on complying with the organization’s implementation and effectiveness of the controls.

Format and Content:
a. We commend the effort to provide a machine-readable format through the online Cybersecurity and Privacy Reference Tool (CPRT). It would be beneficial to ensure that the CPRT is user-friendly, intuitive, and accessible to a wide range of organizations, including those with limited cybersecurity resources.

b. Consider incorporating crosswalks and mappings to other relevant resources and frameworks, such as cloud security standards and international cybersecurity guidelines, to enhance alignment and provide organizations with a holistic approach to cybersecurity.

Transition from CSF 1.1 to CSF 2.0:
a. A clear and concise mapping document highlighting the modifications from CSF 1.1 to CSF 2.0 would greatly assist organizations that have already implemented CSF 1.1. This will ease the transition process and help organizations understand the changes and their implications.

b. Providing a transition guide or toolkit that outlines practical steps, recommended timelines, and potential challenges during the migration process would support organizations in adopting CSF 2.0 effectively. It is critical that a specific date of when 1.1 will be "withdrawn" to ensure legacy environments are upgraded in a timely manner.

We appreciate the efforts made by NIST in developing the NIST Cybersecurity Framework 2.0 Core and its commitment to addressing current and future cybersecurity challenges. We hope that our feedback contributes to the refinement of the framework, ensuring its effectiveness and relevance in the coming years ahead.

Thank you for considering our suggestions.

Sincerely,
The Cloud Security Alliance
www.cloudsecurityalliance.org