Amazon Web Services, Inc. ▪ [redacted]

Amazon Web Services (AWS)
Response to the NIST Cybersecurity Framework 2.0
Draft and Implementation Examples

Introduction

As a leading cloud service provider (CSP), Amazon Web Services (AWS) is committed to improving security outcomes for our customers. AWS appreciates the opportunity to provide feedback to the National Institute of Standards and Technology's (NIST) *Cybersecurity Framework 2.0 Draft and Implementation Examples (CSF 2.0 Draft).* AWS has been engaged throughout NIST's process to update the Cybersecurity Framework, submitting comments to the initial Request for Information, and subsequently inputting through trades for the Concept Paper, and the Discussion Draft focused on the Core. We have been supportive of the overall direction of the updates to the CSF, and note that many of our initial inputs are reflected in the current draft. However, there are some areas, particularly related to the increased adoption of cloud computing, continuous monitoring, mapping to other frameworks, and international adoption of the framework that we believe could be improved in this draft.

As an initial point, we want to reiterate the five key recommendations AWS made during our initial response to NIST's RFI on the *CSF 2.0*:

- Highlight the increased adoption of cloud computing since the CSF was originally published through a greater focus on related concepts, including automation, infrastructure as code, and secure DevOps.
- Enhance focus on continuous improvement and resilience, through the addition of a new function.
- Ensure clear linkages between the NIST CSF and other resources, including in particular NIST's Secure Software Development Framework (SSDF) and Risk Management Framework (RMF).
- Underscore the importance of international awareness and potential adoption of the risk-based, voluntary approach underlying the CSF.
- Provide guidance on C-SCRM and incorporate core concepts into future version of the CSF.

Overall, we believe NIST has worked to integrate our initial feedback throughout the update process, and we offer a few suggestions below to support NIST in concluding its review of the CSF and publishing the updated final framework.

Recommendations

Expand on Explanation of Shared Responsibility Model

The *CSF 2.0 Draft* on page 3 notes that cybersecurity risk management activities can actually enable an organization's ability to achieve its mission, and gives the example of an organization

moving from an in-house data center to a hosting provider. This example at the outset is a strong acknowledgement of the increased role of cloud computing and the security benefits that cloud computing can offer compared to on-premises data hosting. The draft also notes one bullet under 3.4.2. *Improving Communication with External Stakeholders* that states the CSF can be used to help "define shared responsibility models with cloud service providers." We believe an additional narrative paragraph explaining the shared responsibility model in the context of cybersecurity risk management would be helpful to organizations, as many organizations that are implementing the CSF may be unfamiliar with this terminology.

We recommend adding a paragraph explaining that an organization can benefit from the services of a cloud service provider (CSP); CSPs are third-party providers offering infrastructure, application, storage, and other IT services, which allows an organization to delegate responsibility for implementation of a subset of security controls. This differentiation of responsibility is commonly referred to as the shared responsibility, wherein the CSP ensures Security "of" the Cloud and the organization is responsible for Security "in" the Cloud. CSPs can offer physically secure facilities and core functionality such as networking, storage, and compute services, as well as a variety of additional software services that often handle a large portion of security for the "stack" that organizations must otherwise manage for themselves. By using the services of a CSP, an organization can simplify its risk management through oversight of the CSP and other third parties, rather than having to implement full operational responsibility. In this model, a CSP is responsible for protecting the infrastructure that runs all of the services offered in the cloud, which includes the hardware, software, networking, and facilities delivered by the CSP. The organization (i.e. the CSP's customer) is responsible for choosing the appropriate services, and properly configuring and managing them to achieve the needed security outcomes. The organization's responsibility will vary based on the services they choose, the integration of those services into their IT environment, and applicable laws and regulations.

Clarify Continuous Monitoring of External Service Provider Activities

Continuous monitoring is a critical component of implementing an effective cybersecurity risk management strategy. However, we believe NIST should consider revising the language relating to continuous monitoring of an external service provider. Specifically, DE.CM 06, states that "external service provider activities and services are monitored to find potentially adverse events." The implementation example for DE.CM-06 further notes "Ex2: Monitor cloud-based services, internet service providers, and other service providers for deviations from expected behavior." The term "monitor" could be misconstrued as to asking organizations to have full visibility into a service provider's systems. Such access has the potential to increase cybersecurity risk and also may not be technically feasible. As noted above, in the context of a cloud service provider, monitoring and maintaining security "of the cloud" is the primary responsibility of the CSP, and the organization/customer should conduct an "outside-in" monitoring of the third party's service. We recommend changing the terminology in DE.CM-06 to reflect that organizations should "maintain awareness of external service providers activities to identify potentially adverse events." This language ensures that the organization focuses on

oversight of the CSP or other service provider, while clarifying that the organization cannot actually "monitor" the systems of an external party the same way that it can monitor its own.

Build Out Direct Mapping to Other Frameworks

We are pleased to see the significant effort to relate the CSF to other resources and frameworks, including new references to the NIST Privacy Framework, NICE Workforce Framework for Cybersecurity (SP 800-181), Secure Software Development Framework (SP 800- 218), Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (SP 800-161r1), Performance Measurement Guide for Information Security (SP 800-55), Integrating Cybersecurity and Enterprise Risk Management (NIST IR 8286) series, and the Artificial Intelligence Risk Management Framework (AI 100-1).

We note that it will be important to ensure direct mapping of controls between these frameworks and the updated CSF 2.0. For example, the following mapping of controls between the current NIST CSF to SP 800-53 rev 5 will need to be updated.

Reinforce International Adoption

As AWS noted in our initial filing on the CSF 2.0 update, we have seen governments, industry sectors, and organizations around the world increasingly recognize the CSF as a recommended cybersecurity baseline to help improve the cybersecurity risk management and resilience of their systems. The successful widespread use and adoption of the CSF beyond the United States and beyond critical infrastructure sectors demonstrates the value in its risk-based, flexible, voluntary, and stakeholder-driven approach.

We believe further articulation of the international adoption and use of the framework would support adoption of the framework in additional jurisdictions. The narrative does discuss how the CSF can be used with International Organization for Standardization (ISO) 31000:2018; ISO/International Electrotechnical Commission (IEC) 27005:2022; SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy; and the Electricity Subsector Cybersecurity Risk Management Process (RMP) guideline. We recommend further expansion of this section, including language on how ISO 27000 and NIST CSF are complementary to each other. Additionally, it may be useful to reference the international perspective page that NIST has developed in the CSF 2.0 document so that potential non-U.S. based organizations can easily identify other organizations outside the U.S. that have used the framework. Finally, as noted in our initial submission, we encourage NIST to expand translation of the CSF into additional languages to support broader use.

Conclusion

We appreciate NIST's collaborative process throughout this update. The CSF's risk-based, flexible, voluntary, and stakeholder-driven approach has proven to be a valuable resource since its initial development and we look forward to the final version of the *CSF 2.0* update, and to working with NIST to ensure its further adoption around the world.