Amazon Web Services, Inc. ▪ 410 Terry Avenue N. ▪ Seattle, WA 98109

**Amazon Web Services (AWS)**
**Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management**
**Docket Number: 220210-0045**

## Introduction

As a leading cloud service provider (CSP), Amazon Web Services (AWS) is committed to excellence in security and security outcomes for our customers. AWS appreciates the opportunity to provide feedback to the National Institute of Standards and Technology (NIST) as it evaluates whether to update the Cybersecurity Framework (CSF) as well as how to take forward the National Initiative for Improving Cybersecurity in Supply Chains (NIICS) to address cybersecurity risks in supply chains. We believe this review is timely given the evolution of the regulatory and threat landscape since the CSF was initially published, as well as increased attention on cybersecurity supply chain risk management (C-SCRM) and need for alignment on related efforts.

In our response to this Request for Information (RFI), we highlight a number of key concepts that we believe should be taken into account in NIST's review and should be considered in any future iteration of the CSF. We hope that this process will continue in the same spirit as the development of the CSF as well as this RFI. This will ensure an opportunity for broad stakeholder engagement, review, and input. AWS welcomes the opportunity to discuss our views in more detail and to contribute to any process that NIST undertakes to update the CSF and take forward the NIICS.

## Priorities for Review of the CSF

We appreciate that governments, industry sectors, and organizations around the world have increasingly recognized the CSF as a recommended cybersecurity baseline to help improve the cybersecurity risk management and resilience of their systems. We have evaluated the CSF and the many AWS Cloud offerings public and commercial sector customers can use to align to the NIST CSF to improve their cybersecurity posture. The successful widespread use and adoption of the CSF beyond critical infrastructure sectors demonstrates the value in its risk-based, flexible, voluntary, and stakeholder-driven approach. We believe these four fundamental grounding principles should be carried forward in any substantive updates to the CSF to ensure it continues to serve as a critical resource to enhance cybersecurity in the United States (U.S.) and globally.

In addition to these principles, we believe certain measures could be taken to improve the CSF to reflect relevant changes since it was first developed and updated and to grow its effectiveness and adoption. Accordingly, we offer the following key recommendations for updating the CSF:

- 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.

## Recommendations

AWS has observed positive outcomes from the use of the CSF as a guide for our broad range of customers to manage risk. The CSF provides a structure to categorize and catalog security services by function, which allows CSP customers to more easily identify and invest in services to support each of the CSF functions. The CSF was designed to be more accessible to a broader audience than other NIST technical standards, particularly for users who are not security professionals. The CSF thus serves an important role in the cybersecurity ecosystem by helping bridge communication gaps across disparate organizations.

The CSF also provides a construct that allows users to categorize their risk management efforts in an evolving landscape. The CSF takes an approach that assumes breach, preparing organizations for an approach to risk management that keeps pace with the dynamic threat environment.

We recommend that NIST retain these positive attributes inherent to the CSF as it reviews and considers updates to the Framework.

**Highlight increased adoption of cloud computing.** A future version of CSF should include concepts that highlight the increased adoption of cloud computing since the CSF was originally published. This could include references to practices such as "infrastructure as code" and secure DevOps that can provide significant advantage in implementing multiple CSF functions. Teams practicing secure DevOps invest in automating and scaling their software delivery pipeline which reduces time to publish new software artifact or deployment in production environment (for cloud services). Automated delivery software pipeline enables development/service teams to not only deliver new functionality (and security fixes) faster, but also enables continuous security assessment of software, accounting for 3rd party/open source software used in addition to 1st party code written by the team.

Secure DevOps is founded on Agile Software Development principles that expects teams to

reflect on how to become more effective on a continuous basis. This includes setting an expectation that learnings from security events will be considered on a regular basis and then teams will be empowered to tune and adjust their ways-of-working for constant improvement and enhanced resilience.

**Enhance focus on continuous Improvement and Resilience.** We recognize that both the CSF Respond and Recover Functions include a Subcategory on improvement; however, we believe that this activity should be further elevated and emphasized as a stand-alone core function.

The CSF would benefit from a focus on the concept of continuous improvement and resilience and we therefore recommend adding IMPROVE as a new top-level function to the Framework Core. The focus of this step is to ensure that the CSF implementation is not a static model and that each event is also an opportunity for an organization to deliberately take stock of what may have occurred and to consciously consider how to IMPROVE their overall cybersecurity posture and enhance resilience. We believe this step is important to develop independently and fund fully to ensure that it does not get overlooked or delayed. This function would seek to ensure that reflection on learnings and implementing intentional adjustments following any security issues is done in a deliberate manner, by focusing on post event analysis and incorporating lessons learned to reduce and prevent future incidents. While that is technically part of the current Respond and Recover function, the intent is to not only consider a return to normal operations, but also forward-looking improvements and actions that may follow. It also helps elevate continuous improvement as a core function in the mind of business leaders, and understood to be a function that must be fully staffed and funded, and not just a "best efforts" or "spare time" function for already highly-burdened security and compliance teams.

**Ensure clear linkages between the NIST CSF and other resources.** Since the CSF was originally developed and published, there has been a proliferation of additional related resources. In order to assist with improving clarity and explaining how they fit together, the CSF should include a traceability matrix that shows how the elements of the CSF align to the other resources, standards, guidance, etc. This will help to ensure not only that those different documents are in alignment with the CSF, but will also serve as a kind of index to help organizations identify complementary and supplementary resources available.

We specifically want to highlight the need for alignment with the NIST SSDF. References to practices such as secure DevOps can provide significant advantage in implementing multiple CSF functions. The NIST CSF should map its core functions to SSDF practices, instead of adding development environment related guidelines in core CSF functions.

Further, all new NIST resources should include a mapping to NIST 800-53 baselines and a gap analysis. Having this information will allow security compliance stakeholders to rapidly determine their alignment with the CSF or any new guidance that adopts this model. This could provide at-a-glance analytics to show the degree of alignment an organization has with a given framework by virtue of being compliant with various NIST baselines. Specifically, we recommend creating a stronger alignment between the CSF and the NIST RMF. It is important

for organizations that are required to comply with the NIST RMF to understand that the CSF is a complementary set of requirements to enhance related risk management efforts. For example, enhancing the existing mapping in Table 2: Framework Core, Informative References column to include the NIST SP 800-53/FedRAMP Security Baseline that the controls belong to would support this goal.

**Underscore the importance of international awareness and potential adoption of approach underlying the CSF.** We are encouraged to see NIST's focus on international adoption of the CSF as part of the RFI. We recommend that NIST consider a range of options to accelerate international adoption of the CSF. We urge NIST to continue to engage in international standards bodies and advance its related work in ISO/IEC with respect to *Cybersecurity Framework Development Guidelines* and build on those efforts to support a broader international consensus on CSF concepts and approaches. NIST should also ensure that it extends its stakeholder consultations to those in the international community, to include government officials, academics and other relevant subject matter experts. Not only will this input enrich the next version of the CSF, but it will also support greater adoption in the future. We recommend that NIST work with others in the U.S. government to promote the CSF and its fundamental risk-based, flexible, voluntary, and stakeholder-driven approach. This approach must be highlighted in bilateral and multilateral forums in which the U.S. participates. We also encourage showcasing the CSF in discussions with European counterparts to harmonize approaches and align cybersecurity risk management efforts. NIST should consider workshops with foreign counterparts in coordination with the private sector to raise awareness about the CSF as well as conduct practitioner-oriented workshops. The CSF can be the basis for cybersecurity capacity building efforts as well. Finally, we also encourage NIST to expand translation of the CSF into additional language to support broader use.

**Provide guidance on C-SCRM and incorporate core concepts into future version of the CSF.** We recommend that NIST integrate CSF and Cybersecurity SCRM. This will avoid the burden of developing another framework and reduce confusion about use of existing resources. Given the increased importance of cybersecurity issues in the supply chain, we believe it should be an element in the CSF. In our work on cybersecurity supply chain risk management, we find the CSF helpful for categorizing our activities.

In addition, the NIICS could help to address a lack of awareness and understanding of just what to focus on within the supply chain and what threats and vulnerabilities need to be prioritized. Given that supply chains are traditionally focused on optimization and efficiency, the NIICS has an opportunity to convey value and a business case for C-SCRM to supply chain professionals, rather than just speak of cybersecurity risks and practices in general. NIST can bring supply chain subject matter experts into the cybersecurity conversation and vice versa through a deliberate effort in the CSF and the NIICS to align these communities.

With respect to the software security work stemming from EO 14028, we recommend the concept of secure software development be extended to secure service development that uses practices commonly known as DevSecOps or secure DevOps. We acknowledge that the SSDF

identifies its application to DevSecOps as work to be undertaken in the future, and AWS believes this is critical and welcomes the opportunity to collaborate on this effort.

## Additional Suggestions

**Highlight interaction between five functions:** In addition, further clarification of how the five functions interact and support each other should be included in the next version of the CSF. The way it is currently written, the five functions are described as very distinct categories. However, they are interdependent and rely on each other for optimal functioning. For example, in the supply chain context, an organization may want to block a server rack from being used if it arrives with parts from unauthorized suppliers, which is a combination of Protect (blocking the use of unauthorized components) and Detect (how do we know there are unauthorized components present) functions.

**Measure effectiveness:** The CSF would also benefit from inclusion of metrics to support measuring effectiveness and how well it is being implemented. Further, measures that incentivize uptake of the framework could aid in overcoming barriers to adoption.

**Provide additional implementation resources:** NIST could improve the CSF by including resources to assist with implementation. For example, this could include road maps, best practices, metrics, key performance indicators.

## Conclusion

As noted, we appreciate NIST's outreach to stakeholders for substantive feedback as it embarks on a review of the CSF and Cybersecurity Supply Chain Risk Management efforts. 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 collaborating with NIST as it considers how to build on the success of the CSF and proceed in the future.