From: **Hyun, Min**
Date: Fri, Apr 7, 2017 at 2:42 PM
Subject: NIST Cybersecurity Framework Version 1.1- AWS comments
To: "cyberframework@nist.gov" <cyberframework@nist.gov>
Cc: Gile, Chris

On behalf of Chris Gile, Senior Manager, Amazon Web Services (AWS), please find attached our comments to the NIST Cybersecurity Framework Version 1.1. update. AWS appreciates NIST's collaborative and open public comment process. We look forward to our continued partnership to evolve the NIST CSF so that it increases in relevance, effectiveness, and adoption by organizations from industries, sectors, and geographies worldwide.

Please feel free to reach out to me directly if you would like to further discuss our comments.

Thank you,
Min

Min Hyun | Cloud Security Policy and Strategy

[Attachment Copied Below]

April 10, 2017

Submitted via e-mail to cyberframework@nist.gov

Amazon Web Services Comments on the "*NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1"*

Amazon Web Services (AWS) appreciates the opportunity to comment on the *NIST Framework for Improving Critical Infrastructure Cybersecurity v 1.1 (herein "CSF")*. As a global, hyperscale cloud service provider (CSP), AWS takes a rigorous, risk-based approach to the security of our services and the safeguarding of customer data. We enforce our own internal security assurance process on all of our cloud services to evaluate the effectiveness of the managerial, technical, and operational controls necessary for protecting against current and emerging security threats impacting our security and resiliency. This mandatory security assurance process results in real security benefits and attests to our commitment to embed security throughout all phases of the development and operational processes of our services lifecycle.

Due to our global footprint and worldwide customer base, we have extensive experience in satisfying security compliance assessments, which include ISO 27001 and FedRAMP, among other international, national, and sectoral certifications and attestations. We want to reiterate our support for how the NIST CSF leverages some of the most widely reputed and accepted certifications, which allows adopting organizations and their reviewers (e.g. third party auditors, regulators, oversight entities, etc.) to streamline and re-use, instead of over-engineer and redo.

Our comments below address the following themes, which we believe will increase the security effectiveness and adoption of the CSF: (1) Explicitly recognize integration of other third party-validated certifications and attestations that achieve equivalent security outcomes, (2) Clarify use of *Implementation Tiers* as an internal gauge without mandating external reporting, and (3) "Measuring and Demonstrating Cybersecurity" requires additional consideration. We also provide below our response to the specific questions listed in the CSF v1.1 public comment solicitation.

1. **Explicitly recognize integration of other third party-validated certifications and attestations that achieve equivalent security outcomes.**

The CSF reinforces the important practice of leveraging the audit work performed under existing certifications through its use of *Informative References*. The value of the *Informative References* is that it streamlines efforts through the reciprocity of other trustworthy third party certifications that attest to the implementation and effectiveness of equivalent risk management practices. By recognizing and accepting other security certifications, organizations that leverage these services can benefit from the security rigor of the independently verified assessments and avoid duplication. It delivers on the "do once, use many" approach so that all

parties can focus constrained resources on real risk management instead of paper-based compliance.

NIST can promote broader adoption of the CSF by more explicitly encouraging organizations to integrate other third party-validated certifications and attestations that achieve equivalent security outcomes yet are not specified in the *Informative References*. Often times, CSF consumers view the *Information References* as an exclusive, authoritative list of acceptable certifications without realizing that it was not intended to be comprehensive, but rather illustrative and suggestive.

Recommendation: By clarifying that CSF adopters have the discretion to leverage other industry accepted certifications, attestations, and models as *Informative References*, NIST can increase the value proposition, scale, and use of the CSF.

2. **Clarify use of *Implementation Tiers* as an internal gauge without mandating external reporting.**

The use of *Implementation Tiers* in the context of cybersecurity risk management warrants careful evaluation as it can add substantial complexity and subjectivity without clear benefits. As stated in the CSF v 1.1, “implementation tiers are a *qualitative* metric of overall cybersecurity risk management practices.” Since the tiers are *qualitative*, it would be the most meaningful and impactful to use them relative to a specific organizational context- not external to or across organizations.

When individual organizations apply *Implementation Tiers,* it helps them gauge organizational risk management behavior and preparedness. The tiers function as internal designations that factor in the organization’s specific operating environment and risk tolerance level, rather than at the broader infrastructure level. Organizations may determine that certain *Implementation Tiers* are acceptable for a certain set of practices based on risk prioritization and specific application. The Chief Information Officer or organization head should be held accountable for these organization-specific decisions as they have the context for and authority to approve them. Imposing external reporting of *Implementation Tiers* can result in oversight that is not appropriately contextualized and can lead to stack ranking across organizations, which is not the intended purpose. For instance, small and medium-sized contractors will generally face more challenges with investing in and maturing security capabilities compared to large commercial practices. Applying *Implementation Tiers* in this situation can yield misinterpretation and the unintended consequence of calibrating and benefitting certain entities over others, resulting in a more destructive than constructive approach.

Additionally, *Implementation Tiers* are not intended to cascade down to individual services, systems, or contractors that support an organization. Rather, they were designed to gauge *organizational* risk management aptitude; i.e., the practices in place at the enterprise/application level. Contractor systems and services are tools that support an organization and can assist an organization in conforming to the

CSF. For instance, AWS's CloudWatch[1] solution can empower an organization with advanced monitoring capabilities (e.g., log if someone changes a policy, stops a cloud instance, etc.) to support the "Asset Management" category (specifically, sub-categories ID.AM-1, ID.AM-2). The technical, operational, and managerial controls of this particular service are already accounted for through AWS's FedRAMP and ISO certifications.

Recommendation: We advise including use case scenarios to describe the intended implementation and outcome of the *Implementation Tiers* at the organizational and sectoral levels to clarify proper application. This will help flesh out requirements that are applicable to a particular use case or intended outcome scenario and help to avoid situations where conceptual constructs may be valueadd in theory, but where actual practice may not yield the intended outcome in implementation (e.g. FISMA certification and accreditation process for information systems and FISMA scorecard, which have either evolved or have been deprecated).

---

[1] Amazon CloudWatch is a monitoring service for cloud resources and the applications customers run on AWS. CloudWatch collects and tracks metrics, collects and monitors log files, sets alarms, and automatically reacts to changes in a customer's AWS resources. https://aws.amazon.com/cloudwatch/

---

3. "Measuring and Demonstrating Cybersecurity" requires additional consideration.

Measuring cybersecurity return on investment and calculating risk have been a longstanding challenge for all types of organizations regardless of their maturity. It is difficult to measure the litany of risks that are averted 24x7x365 due to effective cybersecurity risk management. Compounding the complexity is that organizations want to measure a wide variety of issues based on organizational mission, business objectives, role, and risk tolerance, among other factors. Moreover, in addition to identifying the performance measurements themselves, organizations need the right structure in place so that measures are effectively used by decision makers to render risk informed decisions and investments.

There are leading practices and principles for developing measures and metrics developed by cybersecurity research and consulting institutions. In fact, NIST Special Publication 800-55 Revision 1, "Performance Measurement Guide for Information Security"[2] and GAO's report on "Information Security: Concerted Effort Needed to Improve Federal Performance Measures"[3] collectively set forth important information security performance measurement types and attributes that are worth evaluating, updating, and considering for integration into the CSF. Further, with the recent alignment of agency FISMA reporting requirements to the CSF, there may be key lessons learned from how agency Chief Information Officers, agency Inspectors General, and the Office of Management and Budget leverage the CSF to gauge the cybersecurity risk posture of federal agencies and the .gov enterprise.

Recommendation: We recommend that NIST evaluate and consider for integration existing leading practices defined by NIST, GAO, professional security services, and cybersecurity research institutions. We also recommend that NIST work with the stakeholder community to define a foundational set of organization- and sectoragnostic security performance indicators that address common, high impact risks.
Until these prerequisite steps have been taken, we advise that NIST defer the inclusion of the section “Measuring and Demonstrating Cybersecurity.”

---

[2] http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf
[3] http://www.gao.gov/assets/300/295160.pdf

AWS Response to CSF Version 1.1 Questions

1. Are there any topics not addressed in the draft Framework Version 1.1. that could be addressed in the final?

Refer to our comments above for suggested revisions to enhance Version 1.1. We also recommend a multi-stakeholder discussion on the new section "Measuring and Demonstrating Cybersecurity" at the forthcoming NIST workshop.

2. How do the changes made in the draft Version 1.1. impact the cybersecurity ecosystem?

Refer to our comments above.

3. For those using Version 1.0, would the proposed changes impact your current use of the Framework? If so, how?

As an Infrastructure-as-a-Service provider, AWS operates a self-service cloud with certain responsibilities (including security and compliance responsibilities) shared between AWS and the customer. In other words, AWS customers have total control over their own cyber risk management. Customers independently determine their cyber posture using a combination of controls managed by AWS and controls implemented and managed by them, either using AWS (or AWS partner) provided security services or through their own tools. AWS cybersecurity management tools allow customers to leverage best-in-class cybersecurity products regardless of their size or industry. This means that all AWS customers can maintain a secure cybersecurity risk posture, giving companies across industries the same high bar security capabilities.

For the AWS controls, we provide IT control information to customers through an external third-party audit program. The two most common ways that customers leverage our third-party audit program are:

a) Specific control definition. AWS customers are able to identify the controls managed by AWS through an external attestation of the operating effectiveness in order to comply with compliance requirements—such as FedRAMP and our Service Organization Controls 1 (SOC 1) Type II report.

b) General control standard compliance. If an AWS customer requires a broad set of control objectives to be met, they can review AWS's industry certifications to ensure the controls audited align with their internal requirements. For example, with the AWS ISO 27001 certification, AWS complies with a broad, comprehensive security standard and follows best practices in maintaining a secure environment. With the PCI Data Security Standard (PCI DSS), AWS complies with a set of controls important to

companies that handle credit card information. With FedRAMP, federal agencies that have data classified at low, moderate, and high impact levels can securely operate and store their public sector data in AWS's government or commercial cloud. Compliance with these general standards provides customers with in-depth information on the comprehensive nature of the controls and security processes in place and can be considered when managing compliance.

4. For those not currently using Version 1.0, does the draft Version 1.1 affect your decision to use the Framework? If so, how?

Not applicable. Refer to response #3 above.

5. Does this proposed update adequately reflect advances made in the Roadmap areas?

We recommend that NIST create a tool to track progress on issues identified in the Roadmap. Doing so will help stakeholders have visibility into the plans underway to address each priority and progress to date. Lacking this context, AWS is not positioned to provide fully informed comments or recommendations.

6. Is there a better label than "version 1.1." for this update?

We support NIST's suggested label for this update.

7. Based on this update, activities in the Roadmap areas, and activities in the cybersecurity ecosystem, are there additional areas that should be added to the Roadmap? Are there any areas that should be removed from the Roadmap?

We recognize the complexity and range of important topics identified in the Roadmap. In light of increasing systems dependencies and interconnections within and among organizations, it is important to address IoT security and risk prioritization.

We appreciate NIST's collaborative and open public comment process. We look forward to our continued partnership to evolve the NIST CSF so that it increases in relevance, effectiveness, and adoption by organizations from industries, sectors, and geographies worldwide.

Sincerely,

Chris Gile, Senior Manager, Security Assurance
Amazon Web Services