Amazon Web Services

Commentary to the Advance Notice of Proposed Rulemaking (ANPR) on Enhanced Cyber Risk Management Standards

This document is provided for informational and discussion purposes, to assist in the development of the ANPR for Cyber Risk Management document. This document is solely for use of parties who receive it directly from Amazon Web Services. It may not be distributed or forwarded to other parties without the express consent of Amazon Web Services.

February 17, 2017

Robert deV. Frierson
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

Legislative and Regulatory Activities Division
Office of the Comptroller of the Currency
400 7th Street SW
Suite 3E-218, mail stop 9W-11
Washington, DC 20219

Robert E. Feldman
Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

Via e-mail to: regs.comments@federalreserve.gov (Board of the Federal Reserve (Board))
regs.comments@occ.treas.gov (Office of the Comptroller of Currency (OCC))
Comments@fdic.gov (Federal Deposit Insurance Corporation (FDIC))

RE: Docket No. R-1550 and RIN 7100-AE-61 (Board)
Docket ID OCC-2016-0016 (OCC)
RIN 3064-AE45 (FDIC)

Amazon comments in response to Banking Agencies' Advanced Notice of Proposed Rulemaking regarding *Enhanced Cyber Risk Management Standards*

Dear Mr. Frierson, Mr. Feldman, et al.:

Amazon Web Services (AWS) welcomes this opportunity to share our comments with the Federal Financial Institutions Examination Council (FFIEC) on the Advance Notice of Proposed Rulemaking (ANPR) on Enhanced Cyber Risk Management Standards (Framework) released for comment in October 2016.

This document summarizes our comments from the perspective of an Infrastructure-as-a-service (IaaS) Cloud Service Provider (CSP). It reflects our experiences providing commercial cloud services to a global customer base and adhering to the highest international security standards, to include compliance within the existing financial services certifications and accreditations. The term customer within includes financial services institutions or financial third-party service providers directly consuming AWS services. We are also providing responses to three specific sections that we deem applicable to commercial cloud providers, such as AWS -- Sector-Critical Systems; Internal and External Dependency; and Incident Response, Cyber Resilience, and Situational Awareness.

While the FFIEC's goal of strengthening the resilience of the financial sector is laudable, imposing additional cybersecurity requirements on CSPs could unnecessarily lead to redundancy and increases in compliance costs, while potentially leaving systemically important financial institutions less secure. Given these concerns, as the FFIEC weighs the scope of applicability for future rulemaking on enhanced cybersecurity standards, the agencies should consider these two critical factors: 1) CSPs already comply with stringent cyber security requirements; and 2) AWS customers, including entities regulated by the FFIEC already, have the freedom necessary under the AWS services to control and maintain their own cybersecurity posture in the cloud.

AWS is already subject to robust security requirements in the form of sector-specific, national, and international security certifications and accreditations[1], many of which align to the NIST Cybersecurity Framework. These existing standards address the risk factors described in the ANPR, including access management, threat modeling, threat intelligence gathering and analytics, vulnerability management, continuous monitoring, and incident reporting, among others. The FFIEC's ANPR on Enhanced Cybersecurity Standards discusses imposing additional sector-specific cybersecurity requirements on regulated entities including third-party service providers. To do this for CSPs would create a redundant and unnecessary layer of requirements.

Additionally, placing new requirements that do not provide additional security benefits above existing standards could result in higher operating costs for CSPs, higher costs for financial services customers, and compromise security outcomes. While there are real and concrete burdens that would result from creating new cybersecurity regulation for CSPs, the benefits are unclear.

Turning to the second factor that the FFIEC should consider in evaluating the scope of applicability for future rulemaking, AWS operates a self-service cloud as an IaaS CSP with certain responsibilities (including security and compliance responsibilities) shared between AWS and the customer. This means that 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 native 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 an incredibly secure cyber 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:

1. **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 the annual financial audit. For this purpose, AWS publishes a wide range of specific IT controls in our Service Organization Controls 1 (SOC 1) Type II report.
2. **General control standard compliance.** If an AWS customer requires a broad set of control objectives to be met, they may review AWS's industry certifications to ensure the controls audited align with their internal requirements. With the AWS ISO 27001 certification, AWS complies with a broad, comprehensive security standard and follows best practices in

[1] This includes FedRAMP (NIST 800-53), ISO 27001, PCI, and SOC to account for the cybersecurity risk management practices of CSPs

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. 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.

Many of the controls identified in the Framework are in the NIST Cybersecurity Framework. For AWS, these controls are already part of our audit program specifically as it relates to our SOC 1 Type II audit program and ISO certification. This approach allows AWS to provide consistent and appropriate information about our risk and compliance program to enable customers to incorporate AWS controls into their governance framework. This information can assist customers in documenting a complete control and governance framework with AWS included as an important part of that framework.

Overall, we recommend the FFIEC carefully consider the universe of comprehensive regulations, controls, attestations, and requirements governing cloud computing technologies and their related security components. When crafting regulations, the FFIEC should also consider a CSPs role in working with covered data, and assign the appropriate responsibilities for compliance. The advantages of such a recommendation is that organizations that leverage these services can benefit from the security rigor of independently verified certifications without having to expend valuable resources on determine a vendor's compliance through audits and other expensive and time consuming processes. It also gives greater transparency and evidence to the regulatory agencies in addition to oversight of all "service providers," whether financial institutions or third-party service providers. A similar approach was taken by the Monetary Authority of Singapore, in their *Outsourced Service Providers Audit Report*, https://abs.org.sg/industry-guidelines/outsourcing, whereby a service provider furnishes a copy of its audit report (OSPAR) to its customers.

Sector-Critical Systems
Response 1 – (Addresses Questions 7, 8, and 11)

AWS does not know what data customers are storing in the cloud, nor can we distinguish personal data from any other type of data stored by a customer as part of that customer's content. For IaaS providers, data classification requirements are scoped to provide the customer with the capability to classify their own data and architect their solution to ensure compliance with data classification or other security requirements.

ISO, NIST and other reputable standards place the responsibility of data and systems classification on customers (i.e. data owners), as they are the best positioned to determine the value, use, sensitivity and criticality of their data. Risk management obligations vary depending on the role of the parties that handle the data. Data owners (i.e. those who generate and control content, such as FS institutions) and data processors (i.e. custodians who handle data in order to provision services) should be subject to requirements appropriate for the roles they play. In the context of data classification, FS institutions are solely responsible for classifying their systems and data.

Recommendation:

It is important to note that a blanket application of all systems as "critical" (despite its actual risk posture) does not reflect a risk-based, outcome-focused approach to security. Protecting data and systems classified at higher levels requires a higher standard of care, which translates into the customer spending increased

resources on securing, monitoring, measuring, remediating, and reporting risks. It would be impractical to commit the significant resources required to securely manage higher impact data and systems that do not meet that threshold. A risk-based approach means applying the security measures commensurate with the potential exposure and consequence of the loss of confidentiality, integrity or availability of the data.

The FFIEC should leverage a risk-based, outcome-focused approach to classifying systems as critical. This type of classification should depend on 1) purpose for which it is used, 2) impact to the FS institution or sector from a prolonged disruption, failure and/or compromise, and 3) risk posture of the system or function. When considering these three factors, cloud services do not rise to the threshold established for sector-critical systems. Cloud computing provides a commercial, scalable, elastic pool of shareable computing resources that are most often used by organizations to power their own business processes and services. System criticality should be applied to a discrete set of functions, technical solutions, assets or processes rather than underlying IT infrastructure, such as IaaS.

Internal and External Dependency

Response 2 - (Addresses Question 21):

AWS, as a third-party service provider, is subject to, and complies with, strict security standards. Extending additional security requirements to an external entity is an example of overreach that will add redundancy to non-critical systems. This could be a barrier for entry and drive valuable security service providers away from the financial services industry and thus, have the unintended consequence of reducing the security resources available to the financial services industry. The ability for a service provider to collectively demonstrate its compliance with international and industry standards is critical to cost management of its oversight program. Certifications and attestations allow customers to benefit from a lower cost of auditability and more transparency from independent third-parties.

Recommendation: Any final rule should leverage existing industry and where appropriate governmental standards that establish best practices for cyber security governance. Any additional or custom requirements may result in reduced access to the most innovative and security technology, such as commercial cloud computing; create less competition and availability to cutting edge technology to the extent third-party service providers would be willing to agree to additional audits; and ultimately drive up costs for customers.

Incident Response, Cyber Resilience, and Situational Awareness

Response 3 - (Questions 24 and 28)

As it relates to the following language from the ANPR "the agencies are considering a requirement that covered entities establish plans and mechanisms to transfer business, where feasible, to another entity or service provider with minimal disruption and within prescribed time frames if the original covered entity or service provider is unable to perform", we submit the following for consideration.

The ANPR should provide more clarity on the impact of requiring service providers to transfer workloads should an event leave the service provider unable to provide business services by clearly defining "prescribed time frames" and "minimal disruption." The impact of a time requirement decoupled from an appropriate risk assessment may result in customers forced to reduce their use of services to the lowest common denominator that can degrade security options.

Additionally, requirements of this nature speak to a business process outsourcing service, where a vendor is providing all of the necessary resources, applications, and personnel, and the firm provides only the data. In their use of AWS, financial services customers maintain a large amount of control over their environment and establishing systems and process that meet regulatory requirements are under their control. Customers can choose how to design in order to ensure their architecture can be migrated, over time, to another platform, where on-premise or to another provider. Additionally, commercial service providers, such as AWS, operate at a scale that allows customers to store their data in multiple regions to support customer continuity in the wake of a disaster.

***Recommendation*:** A requirement should allow for a risk assessment of the chances of a disruption to the service and a time frame commensurate with the risk. This would allow firms to manage to their own internal risk management policies and the FFIEC member regulators can evaluate those standards as appropriate. This would allow customers to use services that are innovative and contribute to their competitive advantage, while allowing them to remain secure.

Conclusion

To optimize for trustworthiness, consistency and repeatability, any certification should integrate international standards to the maximum extent possible, keeping the goal of harmonization in mind wherever possible. Doing so will reduce the cost of implementation and increase the likelihood that more entities will voluntarily adopt it. Consistently evolving, existing global certifications and attestations provide a reasonable set of security domain coverage for cloud services. Additionally, new certifications need to add value to the extent that they provide additional insight into existing practices beyond what most CSPs already achieve with existing audit regimes. It is also important to consider that new certifications could cause marketplace confusion if they do not remove the need for existing certifications or do not address substantial net-new domains.

We recommend that the proposed standards leverage widely-accepted, industry-reputed, third-party security certifications and attestations. By recognizing and accepting other security certifications, organizations that leverage these services can benefit from the security rigor of the independently verified assessments, streamline their own risk management efforts, and avoid duplication.