November 30, 2020

Vanessa Countryman
Secretary
Securities and Exchange Commission
100 F Street NE., Washington, DC 20549

Sent via email to: rule-comments@sec.gov

Re: *File No. S7-10-20; Proposed Amendments to the National Market System Plan Governing the Consolidated Audit Trail to Enhance Data Security*

Dear Ms. Countryman:

Amazon Web Services ("AWS") appreciates this opportunity to offer comments on the 'Proposed Amendments to the National Market System Plan Governing the Consolidated Audit Trail (CAT) to Enhance Data Security'. According to the proposal, the amendments are designed to enhance the security of the CAT. AWS supports efforts by the SEC to enhance the security and privacy of the information in the CAT. These important policy objectives can be achieved in a variety of ways, by leveraging the capabilities of modern cloud service providers, coupled with effective governance and oversight, as we detail below.

This letter summarizes our comments from the perspective of a Cloud Service Provider ("CSP") that provides services to the CAT Plan Processor, Participants, and Industry Members (IM's) that will access and/or report data into the CAT. It reflects our experiences providing commercial cloud services to a global customer base and adhering to the highest U.S. and international security standards, to include compliance within the existing financial services certifications and accreditations. We offer our perspectives as a cloud service provider with deep knowledge on how cloud infrastructure works, and capabilities for customers to achieve security, privacy protection, resiliency, and capacity objectives while also fostering innovation.

Amazon.com, Inc., incorporated in 1994, launched AWS in 2006 to offer IT infrastructure services to businesses. Today, Amazon Web Services provides highly reliable, scalable, low-cost cloud infrastructure that powers hundreds of thousands of businesses in 190 countries around the world. Amazon Web Services is an independent business segment of Amazon.com, Inc. led by AWS CEO, Andy Jassy. AWS financial services customers vary in size from fintech startups to globally systemically important banks, and operate in every industry segment including asset management, banking, capital markets, and insurance. Additionally, the AWS cloud enables organizations to innovate faster and more cost effectively while improving their security posture and operational resilience. Our infrastructure technologies include compute, storage, databases, and emerging technologies like machine learning.

Our comments focus on four areas of the proposal: Secure Analytical Workspace (SAW), U.S. citizen requirements, network connectivity, and dedicated cloud hosts. In summary, our comments capture the following key points:

- There are multiple options for securely architecting the SAW. Legal account ownership is not required to ensure SAW security. The shared responsibility model allows for security to be managed equally effectively in either a centralized or decentralized approach.
- A U.S. Citizen requirement should not be required as CSPs employees will not have access to CAT production systems or encrypted CAT data. AWS controls on access to customer data are demonstrated by compliance with FedRAMP and SOC controls, among other compliance programs.
- Private connectivity is not necessary to provide a secure connectivity into CAT. Internet access that is encrypted and strongly authenticated should remain an option for broker dealers to report data to CAT through the CAT Reporter Portal.
- Dedicated hosts would offer no practical security benefit, but would significantly increase operational risks and costs related to processing times, service level agreements (SLAs), scalability, and resiliency / disaster recovery. AWS offers dedicated hosts to customers to address software licensing requirements, not to improve security controls. Therefore, because of the operational risks associated with dedicated hosts, this solution is not viable for CAT.

Secure Analytical Workspace (SAW)

The proposed amendment poses questions regarding how SAWs should be set up, how access should be managed, and related operational issues. In questions 9, 11 and 13, the SEC asks about the optimal architecture and security controls of the SAW. These questions focus on the most appropriate SAW approach – a decentralized model in which participants would provide and manage SAW Accounts, or a centralized model in which the Plan Processor would provide and manage SAW Accounts. Our comments focus on the technical capabilities of these SAW options, not organizational or resourcing implications. In our view, the shared responsibility model[1] allows for security to be effectively managed in either a centralized or decentralized approach. The only difference is which organization applies which security controls. This is because accounts are logical entities, so the same security controls apply regardless of which legal entity owns the account. In either model, we suggest a controls matrix that defines which organization is responsible for which controls.

In question 21, the SEC asks whether secure file sharing should be the only method of extracting data from CAT, or whether other methods of extraction should be permitted. There are other cloud-native data transfer solutions besides secure file sharing, which can be secured, controlled, monitored, and audited. For example, data transfer could be done using Amazon Kinesis Data Streams (real-time data streaming service), AWS DataSync (provides data transfer between storage services), and Amazon EMR (moves data from Amazon Simple Storage Service to other S3 locations or Hadoop Distributed File System (HDFS) storage). Each of these options supports

[1] Security and compliance is a shared responsibility between AWS and the customer. This shared model can help relieve the customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall.

proactive controls, such as AWS Identity and Access Management (IAM) controls, and reactive controls, such as AWS CloudTrail and Amazon CloudWatch for monitoring, logging, and auditing. We would suggest these as equally effective alternatives to secure file sharing, which should be evaluated against CAT's data transfer requirements.

U.S. Citizenship Requirement

Question 157 asks whether additional restrictions should be required to enhance security, such as imposing U.S. citizenship requirements on all administrators or other staff with access to the CAT System and/or the Central Repository. AWS does not believe that a U.S. citizenship requirement is appropriate for CSPs that support the implementation of the CAT system and/or the Central Repository for several reasons. First, AWS employees will not have access to CAT production systems or encrypted CAT data. Second, restricting access to only U.S. citizens could impact CAT service levels, performance, and scalability, access to important AWS hosted services, and access to global talent for continuous support. Third, controls on access to customer data are demonstrated by AWS' compliance with FedRAMP and SOC controls, among other compliance programs. A more effective control is the application of the principle of least privilege, which is the security best practice noted below of limiting user, application, and service permissions to only those necessary to perform a function or task.

Network Connectivity

The proposed amendments include Questions 158-9 about whether the SEC should require certain changes to how the CAT is architected, including the use of private lines and virtual private networks (VPNs). These questions imply that there would be security issues with the use of certain aspects of cloud services, including architecture and networking. Today, Industry Members (IMs) have the option to connect to the CAT Reporter Portal via the internet. In our view, the following measures contribute to the security of the CAT internet connectivity:

- uses an authenticated, encrypted connection (SSL VPN) through the CAT Secure Reporting Gateway (SRG)
- requires strong Multi-Factor Authentication (MFA) to establish a secure, encrypted session
- includes network isolation limiting access to only authorized endpoints
- supports encryption of data in transit
- ensures that the client's computer never talks directly with the CAT application
- uses TLS standards and applies security best practices identified above (e.g., least privilege access, network segmentation)

Dedicated Cloud Hosts

The SEC seeks input on whether the CAT System should use dedicated cloud hosts that are physically isolated from a hardware perspective and whether all development/production be done on a separate dedicated host, or should only Customer Identifying Systems development and/or production be done in a dedicated host (questions 164-5). Simply put, using cloud dedicated hosts is not viable for the CAT for several reasons. There is no practical security benefit to using

dedicated hosts over shared tenancy. The multi-tenant cloud model supports a variety of security controls and design principles, which can be incorporated into the Comprehensive Information Security Program (CISP) or other guidelines as appropriate. These design principles are detailed below. Furthermore, dedicated hosts impose technical constraints on the CAT architecture, that would put the other CAT requirements at risk, including: capacity, scalability, resiliency/disaster recovery, and ability to meet processing SLAs.

No Practical Security Benefit to Using Dedicated Hosts

Dedicated hosts are primarily intended to support workloads with software licensing that requires a core or virtual machine-based licensing model. Dedicated hosts are not intended as a solution to improve security. The vast majority of cloud services are API-based services running in a multi-tenant model, and do not support the concept of dedicated hosts. Excluding these services from the CAT architecture would severely limit CAT's capability, scalability, and resiliency. Dedicated hosts share the same security controls and guiding principles of AWS' multi-tenant architecture, as detailed through: i) the AWS Well Architected Framework, ii) AWS security best practices, and iii) AWS compliance programs.

The AWS Well Architected Framework's Security pillar outlines AWS design principles for a secure environment. These principles apply equally in multi-tenant or dedicated host environments because they:

- Implement the principle of least privilege and enforce separation of duties with appropriate authorization for each interaction with your AWS resources.
- Enable traceability: Monitor, alert, and audit actions and changes to your environment in real time. Integrate log and metric collection with systems to automatically investigate and take action.
- Apply security at all layers: Apply a defense in depth approach with multiple security controls. Apply to all layers (for example, edge of network, VPC, load balancing, every instance and compute service, operating system application, and code).
- Automate security best practices: Automated software-based security mechanisms improve your ability to securely scale more rapidly and cost-effectively. Create secure architectures, including the implementation of controls that are defined and managed as code in version-controlled templates.
- Protect data in transit and at rest: Classify your data into sensitivity levels and use mechanisms, such as encryption, tokenization, and access control where appropriate.
- Keep people away from data: Use mechanisms and tools to reduce or eliminate the need for direct access or manual processing of data. This reduces the risk of mishandling or modification and human error when handling sensitive data.
- Prepare for security events: Prepare for an incident by having incident management and investigation policy and processes that align to your organizational requirements. Run incident response simulations and use tools with automation to increase your speed for detection, investigation, and recovery.

AWS' security capabilities are based on industry-standard virtualization security approaches. These capabilities are detailed in AWS security best practice documents and white papers.

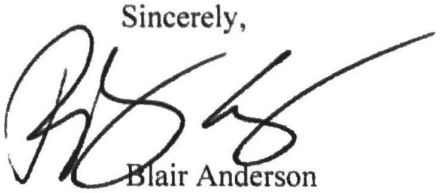
Finally, AWS supports various security standards and compliance certifications, such as FedRAMP, SOC, HIPAA, PCI, ISO 27001/17/18/9001, and CJIS. AWS' multi-tenant architecture and security controls framework supports sensitive data across many regulated industries, including financial services, healthcare, government, and criminal justice.

Dedicated Hosts Impose Technical Constraints that Increase CAT Risk and Cost

The primary constraint that dedicated hosts impose is the inability to use multi-tenant AWS hosted services, including Amazon Simple Storage Service, Amazon Athena, AWS Lambda, Amazon Simple Queue Service, Amazon Simple Notification Service, Amazon EMR, Amazon Redshift, and many others. Prohibiting the use of these multi-tenant, cloud-native services precludes CAT's ability to effectively scale to meet fluctuating workload demands, and optimize processing speed and efficiency. CAT would need to shift to third party or custom built services, increasing the integration complexity and operational burden imposed on the Plan Processor. The inability to use highly elastic and scalable serverless and event-driven architectures would put the CAT processing SLAs at risk. The durability of CAT data would be at risk, as AWS' highly durable storage services are not available on dedicated hosts, including Amazon Simple Storage Service which offers 99.999999999% durability. Amazon Simple Storage Service Glacier would not be available as an option for archiving data for records management purposes. CAT's ability to meet RegSCI requirements would be at risk, as compliance is based on multi-region capabilities and SLAs delivered by AWS services such as Amazon Simple Storage Service and AWS Key Management Service (KMS). Dedicated instances are less scalable to respond to any surge in capacity that may be required during a surge in market volume, and cost savings options such as Amazon Elastic Compute Cloud Spot instances capacity are not available. Finally moving to dedicated hosts would significantly increase CAT development and operating costs, by moving away from cloud-native (server-less, event-driven) architectures, to an approach that is more appropriate for an on-premises data centers. In conclusion, dedicated hosts would add no practical security value, but would significantly increase CAT's operational risk, complexity, and cost structure.

Thank you again for the opportunity to provide our perspective and inputs on the 'Proposed Amendments to the National Market System Plan Governing the Consolidated Audit Trail to Enhance Data Security'. We remain at your disposal in case you have any further questions.

Sincerely,



Blair Anderson
Director, AWS Public Policy