SECURITIES AND EXCHANGE COMMISSION

[Release No. 34-103204; File Nos. SR-DTC-2024-801; SR-FICC-2024-803; SR-NSCC-2024-801]

Self-Regulatory Organizations; The Depository Trust Company; Fixed Income Clearing Corporation; National Securities Clearing Corporation; Notice of No Objection to Advance Notices to Host Certain Core Clearance and Settlement Systems in a Public Cloud

June 6, 2025.

I. INTRODUCTION

On August 14, 2024, The Depository Trust Company ("DTC"), Fixed Income Clearing Corporation ("FICC"), and National Securities Clearing Corporation ("NSCC," each a "Clearing Agency," and collectively, "Clearing Agencies") filed with the Securities and Exchange Commission ("Commission"), respectively, advance notices SR-DTC-2024-801, SR-FICC-2024-803, and SR-NSCC-2024-801 (collectively, the "Advance Notices") pursuant to Section 806(e)(1) of Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act, entitled Payment, Clearing and Settlement Supervision Act of 2010 ("Clearing Supervision Act"),[1] and Rule 19b-4(n)(1)(i)[2] under the Securities Exchange Act of 1934 ("Exchange Act"),[3] seeking no objection to host a specified set of core clearance, settlement, and risk applications, including SCI systems and critical SCI systems under Regulation Systems Compliance and Integrity ("Reg.

---

1 12 U.S.C. 5465(e)(1).

2 17 CFR 240.19b-4(n)(1)(i).

3 15 U.S.C. 78a *et seq*.

SCI")[4] (together, "Core C&S Systems"), on an on-demand network of configurable information technology resources running on a public cloud infrastructure ("Cloud" or "Cloud Infrastructure") hosted by a single, third-party service provider ("the Cloud Service Provider" or "the CSP") (altogether, the "Cloud Proposal").[5] On September 4, 2024, the Commission published notice of the Advance Notices in the *Federal Register* to solicit public comment and to extend the review period for the Advance Notices.[6] The Commission has received no comments regarding the Advance Notices.

On December 5, 2024, the Commission requested that the Clearing Agencies provide it with additional information regarding the Advance Notices, pursuant to Section 806(e)(1)(D) of the Clearing Supervision Act,[7] which tolled the Commission's period of review of the Advance Notices until 120 days[8] from the date the requested information was received by the Commission.[9] The Commission received the Clearing Agencies'

---

4 17 CFR 242.1000 *et seq*.

5 Based on information confidentially filed by the Clearing Agencies, all the Clearing Agencies propose to use the same, single third-party service provider. The Clearing Agencies are each a subsidiary of the Depository Trust & Clearing Corporation ("DTCC"). DTCC operates on a shared service model with respect to the Clearing Agencies. Most corporate functions are established and managed on an enterprise-wide basis pursuant to intercompany agreements under which it is generally DTCC that provides relevant services to the Clearing Agencies. *See* Securities Exchange Act Release No. 100853 (Aug. 28, 2024), 89 FR 71964, 71965, n.7 (Sept. 4, 2024) (File No. SR-DTC-2024-801); Securities Exchange Act Release No. 100852 (Aug. 28, 2024), 89 FR 72128, 72129, n.7 (Sept. 4, 2024) (File No. SR-FICC-2024-803); Securities Exchange Act Release No. 100851 (Aug. 28, 2024), 89 FR 71991, 71992, n.7 (Sept. 4, 2024) (File No. SR-NSCC-2024-801) ("Notices of Filing").

6 Notices of Filing, *supra* n. 5. Given the substantial similarity between the Notices of Filing, citations to a Notice of Filing refer to Securities Exchange Act Release No. 100853 (Aug. 28, 2024), 89 FR 71964 (Sept. 4, 2024) (File No. SR-DTC-2024-801) unless otherwise stated below.

7 12 U.S.C. 5465(e)(1)(D).

8 The Commission had already extended the review period for an additional 60 days (to 120 days total prior to the request for information) for the proposed changes because they raise novel and complex issues pursuant to 12 U.S.C. 5465(e)(1)(H). *See* Notice of Filing, 89 FR at 71982.

9 *See* 12 U.S.C. 5465(e)(1)(E)(ii) and (G)(ii); Memorandum from Office of Clearance and Settlement, Division of Trading and Markets, titled "Commission's Request for Additional Information" (Dec. 5, 2024), *available at https://www.sec.gov/comments/sr-dtc-2024-801/srdtc2024801-545495-1562502.pdf*.

response to the Commission's request for additional information on February 6, 2025.[10] This publication serves as notice of no objection to the Advance Notices.

II. BACKGROUND

The Clearing Agencies are the only entities providing central counterparty ("CCP") or central securities depository ("CSD") services in the U.S. equity and government security markets. DTC is the CSD for substantially all corporate and municipal debt and equity securities available for trading in the United States. NSCC provides clearing, settlement, risk management, CCP services, and a guarantee of completion for virtually all broker-to-broker trades involving equity securities, corporate and municipal debt securities, and unit investment trust transactions in the U.S. markets. FICC is a CCP and provider of clearance and settlement services for the U.S. treasury and mortgage-backed securities markets. The Clearing Agencies' role as covered clearing agencies for these markets is operationally complex and makes the Clearing Agencies an integral part of the national system for clearance and settlement.

The Clearing Agencies currently operate their Core C&S Systems within private, on-premises data centers, with a primary data center in one region, and a second recovery data center in a second region, with corresponding data bunkers for data protection and restoration.[11] The Clearing Agencies now propose to host a specified set of Core C&S

---

10 *See* Memorandum from Office of Clearance and Settlement, Division of Trading and Markets, titled "Response to the Commission's Request for Additional Information" (Feb. 6, 2025), *available at https://www.sec.gov/comments/sr-ficc-2024-803/srficc2024803-568115-1628302.pdf*.

11 As described in the Notice of Filing, the Clearing Agencies' current on-premises hosting capabilities, both mainframe and private cloud, are operating in one primary data center in one region, with a second, recovery data center in a second region. *See* Notice of Filing, 89 FR at 71965 and 71972 (referring to these data centers as primary and backup). The Clearing Agencies state that these data bunkers do not have Compute (as defined below) capabilities and cannot run applications. Their purpose is specifically to be used for data protection and restoration. *See* Notice of Filing, 89 FR at 71965.

Systems on an on-demand network of configurable information technology resources running on the Cloud hosted by a single, third-party CSP. The Clearing Agencies state that the proposed transition aligns with their broader corporate strategy to modernize their technology, maximize platform value for stakeholders, and invest in risk management capabilities.[12]

The Clearing Agencies state that they have assessed the capabilities of the single CSP in adherence with their Clearing Agency Risk Management Framework, which requires the respective board of directors to approve policies governing relationships with service providers, such as the CSP, thus helping to ensure alignment with the Clearing Agencies' risk management principles.[13] The Clearing Agencies also state that the CSP is a well-known, reputable, industry-leading and capable CSP.[14] The Clearing Agencies further state that they and the CSP have spent several years discussing the Clearing Agencies' needs, including operational, legal, and regulatory obligations, what-if scenarios, and commercial implications, and that these discussions have led to a number of benefits, including the CSP introducing new products and the adoption of a contractual agreement that addresses the Clearing Agencies' needs for hosting Core C&S Systems in the Cloud.[15]

---

12 *See* Notice of Filing, 89 FR at 71965.

13 *See* Notice of Filing, 89 FR at 71968. The Clearing Agencies provided the Clearing Agency Risk Management Framework in a confidential exhibit 3 to the Advance Notices. See *id.*, n.25.

14 *See* Notice of Filing, 89 FR at 71968.

15 *See* Notice of Filing, 89 FR at 71968. As confidential exhibits to File Nos. SR-DTC-2024-801, SR-FICC-2024-803, and SR-NSCC-2024-801, the Clearing Agencies provided two examples of CSP white papers as well as the contractual agreement that addresses the Clearing Agencies' needs for hosting Core C&S Systems (the "Cloud Agreement").

The Clearing Agencies do not propose to transition all Core C&S Systems entirely out of their regional data centers to the Cloud at this time. To mitigate risks associated with the proposed migration to the Cloud, the Clearing Agencies have identified a specified set of Core C&S Systems to migrate to the Cloud, incrementally, over the period of several years.[16] The result would be that the Clearing Agencies would host some Core C&S Systems on-premises and others in the Cloud, with no on-premises backup capabilities to address short-term disruptions.[17]

For over the past 11 years, the Clearing Agencies have operated several non-Core C&S Systems in the Cloud, including systems that support risk analysis, reporting engines, and shared infrastructure capabilities, which the Clearing Agencies state has provided the opportunity to refine their technical, risk, legal, and compliance capabilities.[18] Given the Cloud's maturation and growing industry adoption, the Clearing Agencies stated that they believe that hosting Core C&S Systems in the Cloud, via a single CSP, is now appropriate and essential.[19] By leveraging the services of a single CSP, the Clearing Agencies state they seek to enhance efficiency, reduce costs, mitigate risks, and maintain a cohesive operational environment.[20] The proposed migration of a

---

16 The Clearing Agencies provided a list of Core C&S Systems and corresponding timeframe for migration to the Cloud in a confidential exhibit to File Nos. SR-DTC-2024-801, SR-FICC-2024-803, and SR-NSCC-2024-801.

17 The Clearing Agencies would provide notice of any deviation from the proposed transition schedule to Commission staff, the reason for the deviation, and how the proposed implementation schedule would be updated. *See* Notice of Filing, 89 FR 71969. Further, any deviation from the specified set of Core C&S Systems identified to be migrated to the Cloud, or any deviation from the transition schedule for such hosting would necessitate a separate analysis to determine whether such deviation could materially affect the nature or level of risk posed by each of the Clearing Agencies, and if so, would require a separate Advance Notice filing.

18 *See* Notice of Filing, 89 FR at 71965, n.11.

19 *See* Notice of Filing, 89 FR at 71966.

20 *See* Notice of Filing, 89 FR at 71966.

specified set of Core C&S Systems to a single CSP would be based on the Clearing Agencies' provisioning of scalable resources that would: (i) handle various computationally intensive applications with load-balancing and resource management ("Compute"); (ii) provide configurable storage ("Storage"); and (iii) provide network resources and services ("Network").[21] These resources would be logically segregated from other CSP customers, and the Clearing Agencies would utilize the CSP's platform and service offerings for building and operating those Core C&S Systems.[22]

The proposed migration of a specified set of Core C&S Systems would impact various aspects of the Clearing Agencies' operations, including (i) resiliency,[23] (ii) security, and (iii) scalability. The move to a single CSP also would introduce additional risks associated with a migration to the Cloud, which the Clearing Agencies have identified and addressed through various controls, mitigation efforts, and policies and procedures. A summary of each of these aspects of the Clearing Agencies' operations as they would be affected by the proposal is provided below.

A. *Resiliency*

The Clearing Agencies currently operate Core C&S Systems in two on-premises data centers, with one serving as the primary data center and the other serving as the secondary, each located in a separate region.[24] As described in the Advance Notices, the

---

21 *See* Notice of Filing, 89 FR at 71966.

22 *See* Notice of Filing, 89 FR at 71966.

23 In this context, "resiliency" is the "ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that include cyber resources." *Systems Security Engineering: Cyber Resiliency Considerations for Engineering of Trustworthy Secure Systems*, Spec. Publ. NIST SP No. 800-160, vol. 2 (2018). *See* Notice of Filing, 89 FR at 71966.

24 *See supra* note 11.

Clearing Agencies propose to provision, within a single CSP, redundant Compute, Storage, and Network resources in two geographically separate and segregated Cloud regions, each consisting of three availability zones, for a total of six availability zones. Each availability zone would be composed of multiple physical data centers with independent infrastructure,[25] enabling failover between availability zones within a region without service disruptions.[26] The proposed Cloud Infrastructure would operate in a "hot/warm" configuration, with the primary "hot" region actively processing transactions while the secondary "warm" region remains on standby, receiving duplicated data and maintaining capacity for failover.

The Clearing Agencies state that this design enhances resiliency by reducing operational complexity, providing automation tools to reduce human error, ensuring adequate capacity in the event of an outage, and enabling application rotation between regions.[27] The Clearing Agencies state that moving a specified set of Core C&S Systems to the Cloud will materially improve resiliency and reduce risk, as failover to a secondary Cloud region would be less likely than an unplanned out-of-region failover under the current on-premises model because of the additional levels of redundancy built into the proposed Cloud Infrastructure.[28] For example, if the "hot" data center in the primary region were to fail under the current on-premises model, the Clearing Agencies would

---

25 In this context, each physical data center would have its own support staff, dedicated connections to utility power, standalone backup power sources, independent mechanical services, and independent network connectivity. *See* Notice of Filing, 89 FR at 71967.

26 *See* Notice of Filing, 89 FR at 71967.

27 *See* Notice of Filing, 89 FR at 71966-67.

28 *See* Notice of Filing, 89 FR at 71967. The Clearing Agencies state that they plan to continue to own or lease private data center space to host private cloud and mainframe capabilities to facilitate a long-term exit plan from the Cloud, if needed. These on-premises backups would not be available to address short-term incidents at the CSP. *See* Notice of Filing, 89 FR at 71972.

need to failover to the "warm" data center in the secondary region. However, if the "hot" data center in the primary region were to fail under the proposed Cloud Infrastructure, there would still be two additional availability zones in the "hot" region prior to needing to failover to the secondary "warm" region.[29]

The Clearing Agencies also describe their processes for responding to potential outages. The Clearing Agencies state that, in the very unlikely event of an unexpected single- or multi-region outage in which the Clearing Agencies operate, or a complete and unexpected outage of the CSP, the Clearing Agencies would initiate their Major Incident Management process, which is an existing process that involves evaluating the technical impact of the event, and if the event is deemed to have a material impact to the business, the Business Incident Management System would be activated.[30] Depending on the severity of the event, the DTCC Global Business Continuity and Resilience ("BCR") Policy[31] would provide a predictable structure to be utilized during crises and could be leveraged to address, respond to, and manage an outage. In addition to internal risk management practices, the Clearing Agencies have plans to help address various outage scenarios and the potential effects of an outage.[32]

---

29 *See* Notice of Filing, 89 FR at 71967.

30 *See* Notice of Filing, 89 FR at 71972.

31 The Clearing Agency provided the BCR Policy and Standards in a confidential exhibit to File Nos. SR-DTC-2024-801, SR-FICC-2024-803, and SR-NSCC-2024-801. *See* Notice of Filing, 89 FR at 71971, n. 43.

32 *See* Notice of Filing, 89 FR at 71972. The Clearing Agencies have established a list of situations that are covered under the BCR Policy and Standards, any of which could escalate to a disaster and trigger use of the Standards. The technology events include (i) infrastructure outage, (ii) external hosting provider service outage, and (iii) loss of logical access to a Clearing Agency facility. *See* Notice of Filing, 89 FR at 71973, n.65.

Additionally, the Clearing Agencies stated that the migration of a specified set of Core C&S Systems to the Cloud provides a more effective strategy for maintaining system performance and avoiding system degradation because the CSP performs regular system upgrades and maintenance better and faster than on-premises solutions.[33]

Further, the Clearing Agencies state that the underlying legal agreement with the CSP is a strong tool in helping to effectively mitigate the commercial and regulatory risks borne from the concentration risk.[34] Under such agreement, subject to certain exceptions, the CSP must provide an extensive notice if it wishes to terminate the Cloud Agreement for convenience or if it wishes to terminate an individual CSP service offering or lower an existing service level agreement ("SLA") on which the Clearing Agencies rely.[35] The agreement also provides for termination by the CSP with a shorter notice period in the event of a critical breach or an uncured material breach, but requires an extension of this notice period by the CSP if the Clearing Agencies demonstrate a good faith effort to cure the alleged breach.[36] In all cases of an alleged breach, the CSP must notify the Clearing Agencies in writing and provide time for them to cure the alleged breach.[37] If the breach remains uncured after that period, the CSP can only terminate the rights or accounts associated with the breach, not the entire agreement.[38] The Clearing Agencies state that they would have ample notice to shift operations to avoid a disruption to Core C&S

---

33 *See* Notice of Filing, 89 FR at 71967.

34 *See* Notice of Filing, 89 FR at 71970.

35 *See* Notice of Filing, 89 FR at 71970.

36 *See* Notice of Filing, 89 FR at 71970.

37 *See* Notice of Filing, 89 FR at 71970.

38 *See* Notice of Filing, 89 FR at 71970.

Systems, if needed.[39] The agreement provides for the parties to work together and for the CSP to provide professional services to assist with such a shift.[40]

B. *Security*

The Clearing Agencies have developed a Cloud security program to allow the Clearing Agencies to manage the security of the core applications that would run in the Cloud. The Clearing Agencies' Cloud security program also would provide the Clearing Agencies with tools to assess and monitor the CSP's management of the Cloud's security.[41] The Clearing Agencies are also proposing to implement cloud-specific tools provided by the CSP and selected third parties that are not currently available for use in the Clearing Agencies' on-premises data centers.[42] As described below, the proposed Cloud security program focuses on four elements: (i) access controls; (ii) data governance; (iii) configuration management; and (iv) testing.

1. Access Controls

The Clearing Agencies propose to enforce a strict separation of duties and least-privileged access[43] for infrastructure, applications, and data to protect confidentiality,

---

39 *See* Notice of Filing, 89 FR at 71971.

40 *See* Notice of Filing, 89 FR at 71970.

41 The Clearing Agencies state that hosting Core C&S Systems in the Cloud would not change the physical and cybersecurity standards they follow, which are currently designed to align with the National Institute of Standards and Technology ("NIST"), Cyber Security Framework, and Center for Internet Security benchmarks. *See* Notice of Filing, 89 FR at 71967. Further, the Clearing Agencies state that adhering to NIST standards is considered a best practice for financial services use of Cloud. *See* Notice of Filing, 89 FR at 71967.

42 *See* Notice of Filing, 89 FR at 71967. For example, the Clearing Agencies have stated that by hosting in Cloud through the CSP, they would be able to implement automation, monitoring, security incident response capabilities, default separation between Reg. SCI and non-Reg SCI operating domains, and ubiquitous encryption. The proposed Cloud Infrastructure would also enable micro-segmentation of applications and infrastructure services provided by the CSP. *Id*. at 71968.

43 "Least-privileged access" means users will have only the permissions needed to perform their work, and no more. *See* Notice of Filing, 89 FR at 71975.

availability, and integrity of the data in the Cloud.[44] Using third-party tools, the Clearing Agencies would automate role-based access to Core C&S Systems in the Cloud.

To enhance security, the Clearing Agencies have established Identity and Access Management ("IAM")[45] requirements that build on the least-privileged model. Access to Cloud systems would follow a standardized, auditable approval process, with identifications and permissions managed throughout their lifecycle from a centralized IAM system. The Clearing Agencies state that role-, attributable-, and context-based access controls would align with internal standards[46] and industry best practices to uphold least-privileged access and separation of duties.[47] Additionally, the Clearing Agencies would utilize third-party tools for single sign-on and access management, separate from those provided by the CSP. Since the Clearing Agencies would continue to provide cryptographic services and key management, neither the CSP nor other network providers could decrypt Clearing Agency data at rest or in transit.[48]

---

44 *See* Notice of Filing, 89 FR at 71975.

45 "IAM" controls refers to a set of processes and procedures that determine who has access to systems, the granting of access to applications, and controlling what information those persons can access. *See* Notice of Filing, 89 FR 71975.

46 *See* Notice of Filing, 89 FR at 71975. The Clearing Agencies provided the DTCC Information Security – Monitoring and Incident Management Policy and Control Standards in a confidential exhibit to File Nos. SR-DTC-2024-801, SR-FICC-2024-803, and SR-NSCC-2024-801. This document governs the Clearing Agencies' information security monitoring and incident management and specifies requirements for (i) detecting unauthorized information processing activities, (ii) ensuring information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken, and (iii) ensuring a consistent and effective approach is applied to the management of information security incidents. *See* Notice of Filing, 89 FR at 71975, n.85.

47 *See* International Organization for Standardization/International Electrotechnical Commission ("ISO/IEC") 27002:2013 – Information technology – Security techniques – Code of practice for information security controls; *see also* NIST Cybersecurity Framework (CSF) Version 1.1; *see also* NIST Special Publication 800-53 Revision 4 – Security and Privacy Controls for Federal Information Systems and Organizations. *See* Notice of Filing, 89 FR at 71975.

48 *See* Notice of Filing, 89 FR at 71975.

2. Data Governance

The Clearing Agencies' data governance framework that would apply to the proposed Cloud Infrastructure is identified within the Clearing Agencies' Information Security Policies and Control Standards.[49] These policies regulate data movement within the Cloud and across networks. Specifically, they require a system or Software as a Service to store data and information, including all copies of data and information in the system, in the U.S., throughout its lifecycle; be able to retrieve and access the data and information throughout its lifecycle; for data in the system hosted in the Cloud, encrypt such data with key pairs kept and owned by the Clearing Agencies; comply with U.S. federal and applicable state data regulations regarding data location; and enable secure disposition of non-records in accordance with internal policies and procedures.[50] Additionally, the Clearing Agencies' policies establish an overall data governance framework applied to the management, use, and governance of Clearing Agency information accessed, stored, or transmitted through the Cloud Infrastructure.[51] These security measures include ubiquitous authentication, automated public key infrastructure,

---

49 The Information Security Policies and Control Standards are a series of documents that the Clearing Agencies provided as confidential exhibits to File Nos. SR-DTC-2024-801, SR-FICC-2024-803, and SR-NSCC-2024-801. The Clearing Agencies also provided the DTCC Data Risk Management Policy, which establishes requirements for the Clearing Agencies' sound management of data risk across the data lifecycle, in a confidential exhibit to File Nos. SR-DTC-2024-801, SR-FICC-2024-803, and SR-NSCC-2024-801.

50 *See* Notice of Filing, 89 FR at 71976.

51 The Clearing Agencies provided the Operational & Technology Risk Technology Risk Management Procedure—Application Penetration Test, which describes the application penetration test procedures for the Clearing Agencies' web applications and supports compliance with the Information Systems Acquisition Policy, Development and Maintenance Policy Security Control Standards, and Ethical Application Penetration Testing ("EAPT") Control Standards, in confidential exhibits 3 to File Nos. SR-DTC-2024-801, SR-FICC-2024-803, and SR-NSCC-2024-801. *See* Notice of Filing, 89 FR at 71971 n.46.

and key management strategies for both data in transit and at rest.[52] External connectivity to Cloud-hosted systems would remain secured through dedicated private circuits or encrypted tunnels, with additional controls restricting network access.[53]

3. Configuration Management

The Clearing Agencies propose to use automated delivery of business and security capabilities and continuous integration/continuous deployment pipeline methods. The Clearing Agencies state this approach would ensure security controls are consistently and transparently deployed on demand.[54] Further, the Clearing Agencies would implement continuous configuration monitoring, periodic vulnerability scanning, and regular system reviews and testing reports provided by the CSP.[55] For example, the CSP agreement provides for quarterly compliance briefings between the Clearing Agencies and the CSP, during which the Clearing Agencies would be provided information and review service level performance, material system changes, capacity management, SLA updates, and important security notices.[56] The Cloud agreement permits the Clearing Agencies to perform an annual review of the CSP's documentation and services to gain

---

52 *See* Notice of Filing, 89 FR at 71976.

53 *See* Notice of Filing, 89 FR at 71976.

54 *See* Notice of Filing, 89 FR at 71977.

55 *See supra* note 15. For example, the Reg. SCI Addendum, provided by the Clearing Agencies in a confidential exhibit to File Nos. SR-DTC-2024-801, SR-FICC-2024-803, and SR-NSCC-2024-801, states that the Clearing Agencies review the CSP's Systems Organization Controls 2 ("SOC–2") report on an annual basis. *See* Notice of Filing, 89 FR at 71979, n.134. Further, the CSP must make its SOC-2 report available to the Clearing Agency on demand. *See* Notice of Filing, 89 FR at 71979. The CSP also conducts periodic audit meetings specifically designed to discuss security concerns with its customers, and the Clearing Agencies have certain audit rights under the SCI Addendum to review information about the nature and scope of the CSP's vulnerability management program. *See* Notice of Filing, 89 FR at 71974 n. 70. The Reg. SCI Addendum also obligates the CSP to provide the Clearing Agencies with immediate notification where a systems intrusion by an unauthorized party or a systems disruption is suspected. *See* Notice of Filing, 89 FR at 71971.

56 *See* Notice of Filing, 89 FR at 71971.

comfort that the CSP is meeting its contractual obligations and that the notification procedures are in place to allow the Clearing Agencies to meet their regulatory requirements, particularly Reg. SCI.[57] The agreement also provides for the Clearing Agencies' regulator to receive information about the Clearing Agencies' usage of the CSP services and it allows the regulator to perform its own on-site review, if requested.[58]

The Clearing Agencies also propose to use tools offered by the CSP, developed by the Clearing Agencies, and third- parties to track metrics, monitor log files, set alarms, and have the ability to act on changes to the Core C&S Systems and the environment in which they operate.[59] For example, while the CSP would provide a dashboard indicating general system health,[60] the Clearing Agencies' centralized logging system would provide a single frame of reference for log aggregation, access, and workflow management by ingesting the CSP's logs from native detective tools and the Clearing Agencies' monitoring vulnerability management controls.[61] This instrumentation would give the Clearing Agencies a real-time view into Cloud service availability as well as the ability to track historical data.[62]

4. Testing

The Clearing Agencies propose the use of various security testing techniques for the Cloud Infrastructure. Through a risk-based analysis, a Clearing Agency team determines whether and what type of security testing is required. Such techniques include

---

57 *See* Notice of Filing, 89 FR at 71971.

58 *See* Notice of Filing, 89 FR at 71971.

59 *See* Notice of Filing, 89 FR at 71977.

60 *See* Notice of Filing, 89 FR at 71977.

61 *See* Notice of Filing, 89 FR at 71977.

62 *See* Notice of Filing, 89 FR at 71977.

automated security testing,[63] manual penetration testing,[64] and Blue Team testing.[65] The Clearing Agencies would employ processes for managing and remediating the results of its security testing.

In addition, the Clearing Agencies stated that the CSP asserts that it maintains an automated test system, with executive oversight, and conducts full-scope assessments of its hardware, infrastructure, internal threats, and application software as well as a program for conducting internal adversarial assessments designed not only to evaluate system security but also the processes used to monitor and defend its infrastructure.[66] The CSP provides customers, such as the Clearing Agencies, industry standard reports prepared by an independent third-party auditor to provide relevant contextual information and also conducts periodic audit meetings specifically designed to discuss security concerns.[67] Additionally, the CSP agreement includes provisions related to the Clearing Agencies' testing of the CSP's systems and intrusion reporting to facilitate the flow of security information to the Clearing Agencies.[68]

---

63 Automated security testing uses industry standard security testing tools and/or other security engineering techniques specifically configured for each test. *See* Notice of Filing, 89 FR at 71977.

64 Manual penetration testing uses information gathered from automated testing or other sources to identify vulnerabilities and deliver payloads with the intent to break, change, or gain access to the unauthorized area within a system. *See* Notice of Filing, 89 FR at 71977.

65 Blue Team testing identifies security threats and risks in the operating environment and analyzes the network, system, and Software-as-a-Service environments and their current state of security readiness to ensure that they are as secure as possible before deploying to a production environment. *See* Notice of Filing, 89 FR at 71977. Software-as-a-Service is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted.

66 *See* Notice of Filing, 89 FR at 71974.

67 *See* Notice of Filing, 89 FR at 71974, n.70.

68 *See* Notice of Filing, 89 FR at 71971 and 71972 n. 57. Further, the Clearing Agencies have certain audit rights to review information about the nature and scope of the CSP's vulnerability management program under the CSP agreement. *See* Notice of Filing, 89 FR at 71974, n.70.

C. *Scalability*

The Clearing Agencies state that the transition from their current on-premises data centers to the Cloud will increase scalability and agility in managing Compute, Storage, and Network resources that support Core C&S Systems.[69] The Clearing Agencies state that, to ensure operational readiness, the Cloud would enable them to pre-provision Compute and Storage resources while maintaining the ability to scale dynamically.[70] The Clearing Agencies would not, however, rely on capacity on demand, but rather on pre-provisioned capacity to run applications and services, which the Clearing Agencies state would reduce the risk of running out of capacity.[71] The Clearing Agencies state that they would use tools offered by the CSP as well as those developed by the Clearing Agencies and third parties, to monitor Core C&S Systems running in the Cloud, which would enable them to integrate the availability and capacity management of Cloud into their existing processes.[72] This approach would allow Compute capacity to be increased in one or both regions through manual or automated processes.[73] Further, the Clearing Agencies state that the Cloud would enable rapid provisioning or de-provisioning of resources to meet demands, allowing them to accommodate elevated trade volumes and provide more flexibility to create development and test environments. For example, the CSP could support elastic workloads and scale dynamically without the need for the Clearing Agencies to procure, test, and install additional servers, storage, or other hardware.[74] The

---

69 *See* Notice of Filing, 89 FR at 71968.

70 *See* Notice of Filing, 89 FR at 71968.

71 *See* Notice of Filing, 89 FR at 71972.

72 *See* Notice of Filing, 89 FR at 71977.

73 *See* Notice of Filing, 89 FR at 71968.

74 *See* Notice of Filing, 89 FR at 71968.

Clearing Agencies state the ability to quickly scale workloads materially improves their ability to respond to unexpected market events and external scenarios, such as a global pandemic.[75] Additionally, the Clearing Agencies state that the ability to quickly scale workloads enables the Clearing Agencies to run risk calculations more frequently, at greater speeds, and with more compute-intensive models than is economically feasible with their on-premises infrastructure.[76]

The Clearing Agencies would combine their pre-provisioned primary capacity with regular capacity stress testing to verify that the underlying Compute resources can sustain required business volumes. Stress testing results would be used to determine the base-level provisioning capacity.[77]

Overall, the Clearing Agencies state that the transition to the Cloud would materially enhance the Clearing Agencies' ability to quickly scale workloads, perform risk calculations with greater speed and complexity, and innovate faster to meet evolving business requirements, while also ensuring optimal performance during peak trading periods and efficient resource allocations during lower-demand periods.[78]

III. DISCUSSION AND NOTICE OF NO OBJECTION

Although the Clearing Supervision Act does not specify a standard of review for an advance notice, the stated purpose of the Clearing Supervision Act is instructive: to mitigate systemic risk in the financial system and promote financial stability by, among

---

75 *See* Notice of Filing, 89 FR at 71968.

76 *See* Notice of Filing, 89 FR at 71968.

77 *See* Notice of Filing, 89 FR at 71968.

78 *See* Notice of Filing, 89 FR at 71968.

other things, promoting uniform risk management standards for systemically important financial market utilities ("SIFMUs") and strengthening the liquidity of SIFMUs.[79]

Section 805(a)(2) of the Clearing Supervision Act authorizes the Commission to prescribe regulations containing risk management standards for the payment, clearing, and settlement activities of designated clearing entities engaged in designated activities for which the Commission is the supervisory agency.[80] Section 805(b) of the Clearing Supervision Act provides the following objectives and principles for the Commission's risk management standards prescribed under section 805(a):[81]

- To promote robust risk management;
- To promote safety and soundness;
- To reduce systemic risks; and
- To support the stability of the broader financial system.

Section 805(c) provides, in addition, that the Commission's risk management standards may address such areas as risk management and default policies and procedures, among other areas.[82]

The Commission has adopted risk management standards under section 805(a)(2) of the Clearing Supervision Act and section 17A of the Exchange Act (the "Clearing Agency Rules").[83] The Clearing Agency Rules require, among other things, each covered

---

79 *See* 12 U.S.C. 5461(b).

80 12 U.S.C. 5464(a)(2).

81 12 U.S.C. 5464(b).

82 12 U.S.C. 5464(c).

83 17 CFR 240.17ad-22. *See* Securities Exchange Act Release No. 68080 (Oct. 22, 2012), 77 FR 66220 (Nov. 2, 2012) (S7-08-11). *See also* Securities Exchange Act Release No. 78961 (Sept. 28, 2016), 81 FR 70786, 70806 (Oct. 13, 2016) (S7–03–14) ("Covered Clearing Agency Standards"). DTC, FICC, and NSCC are each a "covered clearing agency" as defined in Rule 17ad-22(a).

clearing agency to establish, implement, maintain, and enforce written policies and procedures that are reasonably designed to meet certain minimum requirements for its operations and risk management practices on an ongoing basis.[84] As such, it is appropriate for the Commission to review advance notices against the Clearing Agency Rules and the objectives and principles of these risk management standards as described in Section 805(b) of the Clearing Supervision Act. As discussed below, the proposals in the Advance Notices are consistent with the objectives and principles described in Section 805(b) of the Clearing Supervision Act,[85] and in the Clearing Agency Rules, in particular Rule 17ad-22(e)(17)(ii).[86]

A. *Consistency with Section 805(b) of the Clearing Supervision Act*

The proposed changes contained in the Advance Notices are consistent with the stated objectives and principles of section 805(b) of the Clearing Supervision Act. Specifically, as discussed below, the changes proposed in the Advance Notices are consistent with promoting robust risk management, promoting safety and soundness, reducing systemic risks, and supporting the stability of the broader financial system.[87]

The Clearing Agencies' proposal is consistent with robust risk management, specifically operational risk management, and the promotion of safety and soundness. Specifically, the proposal to host a specified set of Core C&S Systems in the Cloud, when supported by the appropriate legal agreements, such as the agreements discussed in part II above, and system configurations, should provide opportunities for improvements

84 17 CFR 240.17ad-22.

85 12 U.S.C. 5464(b).

86 17 CFR 240.17ad-22(e)(17)(ii).

87 12 U.S.C. 5464(b).

in resiliency, security, and scalability compared to existing infrastructures in traditional, on-premises data centers. Based on a review of the complete record, including the confidential information provided by the Clearing Agencies, the proposal to host a specified set of Core C&S Systems in two geographically separate and segregated Cloud regions, each consisting of three availability zones, for a total of six availability zones, would provide a level of security and resiliency to the Clearing Agencies' C&S Systems beyond that provided by their current on-premises-only infrastructure.

As described above, the legal agreements underlying the relationship between the Clearing Agencies and the CSP are designed to support the Clearing Agencies' ability to comply with its regulatory obligations related to the management of operational risk. For example, the CSP agreement includes provisions related to the Clearing Agencies' testing of the CSP's systems and intrusion reporting to facilitate the flow of security information to the Clearing Agencies and provide the Clearing Agencies with the right to review information about the nature and scope of the CSP's vulnerability management program. The agreement further obligates the CSP to provide the Clearing Agencies with immediate notification where a systems intrusion by an unauthorized party or a systems disruption is suspected.

Moving to a third-party hosted Cloud Infrastructure presents the risk that the Clearing Agencies could be overly reliant on the CSP to provide test results reliably and consistently. As described above, however, the CSP provides customers industry standard reports prepared by an independent third-party auditor and discusses security concerns in periodic audit meetings specifically designed to discuss security concerns.[88] Further, the

[88] *See* Notice of Filing, 89 FR at 71974, n.70.

CSP agreement provides for the Clearing Agencies' testing of the CSP's systems and intrusion reporting to facilitate the flow of security information to the Clearing Agencies[89] as well as the Clearing Agencies' rights to review information about the nature and scope of the CSP's vulnerability management program under the CSP agreement.[90]

Further, the proposal's reliance on the CSP is not objectionable because the CSP and the Clearing Agencies have negotiated and entered into a legal agreement governing their relationship which addresses salient parts of the relationship between the Clearing Agencies and the CSP in various relevant areas. For example, in this agreement, the Clearing Agencies have certain audit rights to review information about the nature and scope of the CSP's vulnerability management program.[91] In this agreement, the CSP makes certain representations and ongoing commitments about the systems and services that it will provide related to, among other things, information security;[92] the use of industry standards;[93] capacity planning;[94] vulnerability assessments;[95] penetration testing;[96] briefing meetings;[97] the Clearing Agencies' testing of the CSP's systems;[98]

---

89 *See* Notice of Filing, 89 FR at 71971 and 71972 n. 57.

90 *See* Notice of Filing, 89 FR at 71974, n.70.

91 *See* Notice of Filing, 89 FR at 71974, n.70.

92 *See* Notice of Filing, 89 FR at 71979.

93 *See* Notice of Filing, 89 FR at 71979. The CSP is required to make available its SOC-2 report, as well as other certifications from accreditation bodies and information regarding its alignment with various frameworks, including NIST-CSF and ISO. *Id.*

94 *See* Notice of Filing, 89 FR at 71974.

95 *See* Notice of Filing, 89 FR at 71974.

96 *See* Notice of Filing, 89 FR at 71971.

97 *See* Notice of Filing, 89 FR at 71978.

98 *See* Notice of Filing, 89 FR at 71972.

performance monitoring and information;[99] record keeping;[100] systems intrusion and disruption issues;[101] and regulatory supervision.[102] Specifically, the agreement provides for quarterly compliance briefings between the Clearing Agencies and the CSP, wherein the Clearing Agencies would receive information;[103] detailed quarterly briefing meetings during which the Clearing Agencies could review service level performance, material system changes, capacity management, SLA updates, and important security notices;[104] permits the Clearing Agencies to perform an annual review of the CSP's documentation and services to ensure the CSP is meeting its contractual and regulatory requirements such as Reg. SCI;[105] and provides for the Clearing Agencies' regulator to receive information about the Clearing Agencies' usage of the CSP services and for the regulator to perform on-site reviews, if it requests.[106] The underlying agreements and other materials provided confidentially support the ability for the Clearing Agencies to meet their regulatory requirements.[107]

Moreover, to the extent the proposed changes are consistent with promoting the Clearing Agencies' robust risk management as well as safety and soundness, they are also consistent with supporting the stability of the broader financial system. The Clearing

---

99 *See* Notice of Filing, 89 FR at 71971.

100 *See* Notice of Filing, 89 FR at 71979.

101 *See* Notice of Filing, 89 FR at 71971.

102 *See* Notice of Filing, 89 FR at 71979-80.

103 *See* Notice of Filing, 89 FR at 71979.

104 *See* Notice of Filing, 89 FR at 71971.

105 *See* Notice of Filing, 89 FR at 71971.

106 *See* Notice of Filing, 89 FR at 71971; *see also supra* note 44.

107 Based on its general supervisory knowledge, the Commission understands that the CSP engaged by the Clearing Agencies has a demonstrated track record of providing such services, which also supports the Clearing Agencies' ability to meet their regulatory obligations in reliance upon such a provider.

Agencies have been designated as SIFMUs, in part, because failure or disruption to any Clearing Agency could increase the risk of significant liquidity or credit problems spreading among financial institutions or markets.[108] The proposed changes should support the Clearing Agencies' ability to continue providing services to the U.S. securities markets.

As described above, the proposal would provide for pre-provisioned resources in the Cloud to match the Clearing Agencies' current capacity while also allowing the Clearing Agencies to quickly provision additional capacity as necessary without the Clearing Agencies being required to purchase and install additional hardware in their on-premises data centers. The Clearing Agencies' continued operations would, in turn, help support the stability of the financial system by reducing the risk of significant operational problems spreading among market participants that rely on the Clearing Agencies' central role in the U.S. securities market.

As part of its review, the Commission considered each Clearing Agency's reliance on the CSP from an operational resilience perspective to support its ability to provide core clearance and settlement services.[109] The Commission has also considered the mitigating factor whereby the Clearing Agencies propose to implement their applications across two regions each with three availability zones comprising multiple data centers. Establishing multiple backup systems across the proposed Cloud Infrastructure supports the Clearing Agencies' ability to continue providing services to

---

108 *See* Financial Stability Oversight Council ("FSOC") 2012 Annual Report, Appendix A, *https://home.treasury.gov/system/files/261/here.pdf*.

109 This is similar to the Clearing Agencies' current use of two data centers, which similarly depend on single vendors for certain services across both centers.

the U.S. securities markets. As described above, the proposed structure is more operationally robust than the Clearing Agencies' current on-premises footprint. The likelihood of a complete outage of the proposed Cloud Infrastructure should be lower than the likelihood of a complete outage of the current, on-premises environment, which would increase the likelihood that the Clearing Agencies would be able to continue providing services.

Separate from the operational resilience provided by the proposed transition, the Commission has also considered the reliance of the Clearing Agencies upon a single CSP from a commercial perspective. Although the CSP could choose, consistent with the terms of the applicable agreements described in II.A, to terminate its relationship with the Clearing Agencies, the legal agreements underlying the proposal provide assurance that the Clearing Agencies should be able to continue providing services to the U.S. securities markets. As described above, the terms of the agreements should provide sufficient notice to the Clearing Agencies prior to termination to allow the Clearing Agencies to shift their business away from the CSP.[110] As described above, the agreement requires that the CSP provide extensive notice if it wishes to terminate the Cloud Agreement for convenience or if it wishes to terminate an individual CSP service offering or lower an existing SLA.[111] Even in the case of a termination for cause, the CSP must provide notice and an opportunity to cure,[112] all of which provides the Clearing Agencies with time to shift operations to avoid a disruption to Core C&S Systems.

---

110 The Clearing Agencies state that they plan to continue to own or lease private data center space to host private cloud and mainframe capabilities to facilitate a long-term exit plan from the Cloud, if needed. *See* Notice of Filing, 89 FR at 71972.

111 *See* Notice of Filing, 89 FR at 71970.

112 *See* Notice of Filing, 89 FR at 71970.

Accordingly, and for the reasons stated above, the changes proposed in the Advance Notices are consistent with section 805(b) of the Clearing Supervision Act.[113]

B. *Consistency with Rule 17ad-22(e)(17)(ii) under the Exchange Act*

Rule 17ad-22(e)(17)(ii) under the Exchange Act requires that a covered clearing agency establish, implement, maintain, and enforce written policies and procedures reasonably designed to, as applicable, manage the covered clearing agency's operational risks by ensuring that systems have a high degree of security, resiliency, operational reliability, and adequate, scalable capacity.[114]

As described in Section II.A. above, the Clearing Agencies propose to increase the resiliency of a specified set of Core C&S Systems by migrating from two on-premises data centers in separate regions, with one serving as the primary data center and the other serving as the secondary backup data center, to two geographically separate and segregated Cloud regions. As described in Section II.B. above, while the Clearing Agencies would not change their physical and cybersecurity standards, migrating specified Core C&S Systems would enable them to expand their existing physical and cyber security capabilities with a focus on: (i) access controls; (ii) data governance; (iii) configuration management; and (iv) testing, as well as the availability of additional tools that cannot be used in the Clearing Agencies' on-premises data centers.[115] As described in Section II.C. above, operating in a Cloud Infrastructure would allow the Clearing Agencies to quickly scale resources and increase capacity to meet elevated trade volumes more quickly than is currently possible. This dynamic scalability offered by migrating a

---

113 12 U.S.C. 5464(b).

114 17 CFR 240.17ad-22(e)(17)(ii).

115 *See supra* note 32; *see also* Notice of Filing, 89 FR at 71967-68.

specified set of Core C&S Systems to the Cloud should allow the Clearing Agencies to continue operating during periods of unexpected market events that create volatility in the U.S. securities markets when the Clearing Agencies may need additional capacity, but would not have the time to purchase and install additional hardware in their on-premises datacenters.

Accordingly, the changes proposed in the Advance Notices are consistent with Rule 17ad-22(e)(17)(ii) under the Exchange Act.[116]

IV. CONCLUSION

IT IS THEREFORE NOTICED, pursuant to Section 806(e)(1)(I) of the Clearing Supervision Act, that the Commission DOES NOT OBJECT to the Advance Notices (SR-DTC-2024-801; SR-FICC-2024-803; and SR-NSCC-2024-801) and that the Clearing Agencies are AUTHORIZED to implement the proposed changes as of the date of this notice.

By the Commission.

Vanessa A. Countryman,

Secretary.

[116] 17 CFR 240.17ad-22(e)(17)(ii).