Required fields are shown with yellow backgrounds and asterisks.

Page 1 of * 128

SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549
Form 19b-4

File No. * SR 2024 - * 801
Amendment No. (req. for Amendments *)

Filing by The Depository Trust Company

Pursuant to Rule 19b-4 under the Securities Exchange Act of 1934

Initial * ☑ Amendment * ☐ Withdrawal ☐

Section 19(b)(2) * ☐ Section 19(b)(3)(A) * ☐ Section 19(b)(3)(B) * ☐

Pilot ☐

Extension of Time Period for Commission Action * ☐

Date Expires *

Rule

☐ 19b-4(f)(1) ☐ 19b-4(f)(4)
☐ 19b-4(f)(2) ☐ 19b-4(f)(5)
☐ 19b-4(f)(3) ☐ 19b-4(f)(6)

Notice of proposed change pursuant to the Payment, Clearing, and Settlement Act of 2010

Section 806(e)(1) * ☑ Section 806(e)(2) * ☐

Security-Based Swap Submission pursuant to the Securities Exchange Act of 1934
Section 3C(b)(2) * ☐

Exhibit 2 Sent As Paper Document ☐

Exhibit 3 Sent As Paper Document ☐

Description

Provide a brief description of the action (limit 250 characters, required when Initial is checked *).

Host Certain Core Clearance and Settlement Systems in a Public Cloud

Contact Information

Provide the name, telephone number, and e-mail address of the person on the staff of the self-regulatory organization prepared to respond to questions and comments on the action.

First Name * [redacted] Last Name * [redacted]

Title * [redacted]

E-mail * RuleFilingAdmin@dtcc.com

Telephone * [redacted] Fax

Signature

Pursuant to the requirements of the Securities Exchange of 1934, The Depository Trust Company has duly caused this filing to be signed on its behalf by the undersigned thereunto duly authorized.

Date 08/14/2024

By [redacted]
(Name *)

(Title *) [redacted]

NOTE: Clicking the signature block at right will initiate digitally signing the form. A digital signature is as legally binding as a physical signature, and once signed, this form cannot be changed.

Date: 2024.08.14 11:39:46 -04'00'

Required fields are shown with yellow backgrounds and astericks.

SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

For complete Form 19b-4 instructions please refer to the EFFS website.

Form 19b-4 Information *

Add | Remove | View

Narrative (DTC) - Public Cloud - 2024-

The self-regulatory organization must provide all required information, presented in a clear and comprehensible manner, to enable the public to provide meaningful comment on the proposal and for the Commission to determine whether the proposal is consistent with the Act and applicable rules and regulations under the Act.

Exhibit 1 - Notice of Proposed Rule Change *

Add | Remove | View

The Notice section of this Form 19b-4 must comply with the guidelines for publication in the Federal Register as well as any requirements for electronic filing as published by the Commission (if applicable). The Office of the Federal Register (OFR) offers guidance on Federal Register publication requirements in the Federal Register Document Drafting Handbook, October 1998 Revision. For example, all references to the federal securities laws must include the corresponding cite to the United States Code in a footnote. All references to SEC rules must include the corresponding cite to the Code of Federal Regulations in a footnote. All references to Securities Exchange Act Releases must include the release number, release date, Federal Register cite, Federal Register date, and corresponding file number (e.g., SR-[SRO]-xx-xx). A material failure to comply with these guidelines will result in the proposed rule change being deemed not properly filed. See also Rule 0-3 under the Act (17 CFR 240.0-3)

Exhibit 1A - Notice of Proposed Rule Change, Security-Based Swap Submission, or Advanced Notice by Clearing Agencies *

Add | Remove | View

Exh 1A (DTC) - Public Cloud - 2024-0

The Notice section of this Form 19b-4 must comply with the guidelines for publication in the Federal Register as well as any requirements for electronic filing as published by the Commission (if applicable). The Office of the Federal Register (OFR) offers guidance on Federal Register publication requirements in the Federal Register Document Drafting Handbook, October 1998 Revision. For example, all references to the federal securities laws must include the corresponding cite to the United States Code in a footnote. All references to SEC rules must include the corresponding cite to the Code of Federal Regulations in a footnote. All references to Securities Exchange Act Releases must include the release number, release date, Federal Register cite, Federal Register date, and corresponding file number (e.g., SR-[SRO]-xx-xx). A material failure to comply with these guidelines will result in the proposed rule change being deemed not properly filed. See also Rule 0-3 under the Act (17 CFR 240.0-3)

Exhibit 2- Notices, Written Comments, Transcripts, Other Communications

Add | Remove | View

Copies of notices, written comments, transcripts, other communications. If such documents cannot be filed electronically in accordance with Instruction F, they shall be filed in accordance with Instruction G.

☐ Exhibit Sent As Paper Document

Exhibit 3 - Form, Report, or Questionnaire

Add | Remove | View

Exh 3 (Redacted) - Public Cloud - 202

Copies of any form, report, or questionnaire that the self-regulatory organization proposes to use to help implement or operate the proposed rule change, or that is referred to by the proposed rule change.

☐ Exhibit Sent As Paper Document

Exhibit 4 - Marked Copies

Add | Remove | View

The full text shall be marked, in any convenient manner, to indicate additions to and deletions from the immediately preceding filing. The purpose of Exhibit 4 is to permit the staff to identify immediately the changes made from the text of the rule with which it has been working.

Exhibit 5 - Proposed Rule Text

Add | Remove | View

The self-regulatory organization may choose to attach as Exhibit 5 proposed changes to rule text in place of providing it in Item I and which may otherwise be more easily readable if provided separately from Form 19b-4. Exhibit 5 shall be considered part of the proposed rule change

Partial Amendment

Add | Remove | View

If the self-regulatory organization is amending only part of the text of a lengthy proposed rule change, it may, with the Commission's permission, file only those portions of the text of the proposed rule change in which changes are being made if the filing (i.e. partial amendment) is clearly understandable on its face. Such partial amendment shall be clearly identified and marked to show deletions and additions.

1. Text of the Advance Notice

(a) There is no rule text change proposed with this advance notice. The change proposed in this advance notice by The Depository Trust Company ("DTC") is described in detail in Item 10 below.

(b) Not applicable.

(c) Not applicable.

2. Procedures of the Clearing Agency

The proposed change was approved by Businesses, Technology and Operations committee of the Board of Directors of DTC at a meeting held on October 24, 2023.

3. Clearing Agency's Statement of the Purpose of, and Statutory Basis for, the Advance Notice

Not applicable.

4. Clearing Agency's Statement on Burden on Competition

Not applicable.

5. Clearing Agency's Statement on Comments on the Advance Notice Received from Members, Participants, or Others

DTC has not received or solicited any written comments relating to this proposal. If any written comments are received, DTC will amend this filing to publicly file such comments as an Exhibit 2 to this filing, as required by Form 19b-4 and the General Instructions thereto.

Persons submitting written comments are cautioned that, according to Section IV (Solicitation of Comments) of the Exhibit 1A in the General Instructions to Form 19b-4, the Securities and Exchange Commission ("Commission") does not edit personal identifying information from comment submissions. Commenters should submit only information that they wish to make available publicly, including their name, email address, and any other identifying information.

All prospective commenters should follow the Commission's instructions on How to Submit Comments, available at www.sec.gov/regulatory-actions/how-to-submitcomments. General questions regarding the rule filing process or logistical questions regarding this filing should be directed to the Main Office of the Commission's Division of Trading and Markets at tradingandmarkets@sec.gov or 202-551-5777.

DTC reserves the right to not respond to any comments received.

6. Extension of Time Period for Commission Action

Not applicable.

7. Basis for Summary Effectiveness Pursuant to Section 19(b)(3) or for Accelerated Effectiveness Pursuant to Section 19(b)(2) or Section 19(b)(7)(D)

(a) Not applicable.

(b) Not applicable.

(c) Not applicable.

(d) Not applicable.

8. Proposed Rule Change Based on Rules of Another Self-Regulatory Organization or of the Commission

Not applicable.

9. Security-Based Swap Submissions Filed Pursuant to Section 3C of the Exchange Act

Not applicable.

10. Advance Notices Filed Pursuant to Section 806(e) of the Payment, Clearing and Settlement Supervision Act

I. <u>Description of the Proposal</u>

Pursuant to Section 806(e)(1) of Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act, entitled the 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] DTC files this advance notice seeking no objection to host a specified set of core clearance, settlement, and risk applications, including any Regulation Systems Compliance and Integrity ("Reg. SCI") systems and Critical SCI systems,[4] ("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 ("Cloud Service Provider" or "CSP") (altogether, the "Cloud Proposal"), as described herein.

The specified set of Core C&S Systems that the Clearing Agencies intend to host in the Cloud, and the transition schedule for such hosting, are listed in Exhibit 3 to this advance notice

---

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.

4 17 CFR 242.1000 et seq.

filing.[5] However, the Clearing Agencies recognize that it may become necessary to deviate from the proposed transition schedule as risks change over time and the proposed implementation would occur over several years. The Clearing Agencies' process for monitoring, assessing, and escalating such risks, which may result in a deviation, is described in Section I.D, below. If the Clearing Agencies would need to deviate from that schedule, they would provide Commission staff notice of such deviation, the reason for the deviation, and how the implementation schedule would be updated to account for the deviation. Further, the Clearing Agencies recognize that deviating from the proposed transition schedule 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.

DTC's two affiliate clearing agencies, Fixed Income Clearing Corporation ("FICC") and National Securities Clearing Corporation ("NSCC" and together with DTC and FICC, the "Clearing Agencies")[6] have each filed with the Commission advance notices to adopt the same Cloud Proposal. Accordingly, each respective advance notice filing is written from the perspective of the Clearing Agencies, collectively, instead of DTC, FICC, and NSCC individually.[7]

A. The Current System and Summary of Proposed Change

Today, the Clearing Agencies' Core C&S Systems are hosted using Compute,[8] Storage and Networking, as defined below, running in private data centers (i.e., on-premises). The current data-center footprint consists of a single data center in each of two regions. Each regional data center has a corresponding data bunker used for synchronous data protection and restoration.[9]

---

5 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the proposed transition schedule (i.e., the Core C&S Systems to Move to Cloud). The Clearing Agencies have provided this schedule in confidential Exhibit 3 to this advance notice filing.

6 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.

7 Capitalized terms not otherwise defined herein have the meaning as set forth in respective rules of the Clearing Agencies, available at https://www.dtcc.com/legal/rules-and-procedures.

8 The existing Compute platform consists of both on-premises mainframe and private cloud platforms.

9 Note: The data bunkers cannot run applications, as they are only for data protection and restoration.

The Clearing Agencies view the proposed transition to using a Cloud Infrastructure to host the specified set of Core C&S Systems as a natural progression of the Clearing Agencies' information technology strategy that aligns with their overall corporate strategy – to deliver on modernization and maximize the value of their platforms for stakeholders and continue to invest in risk management excellence.

For over 11 years, the Clearing Agencies have honed their expertise in operating non-Core C&S Systems within the Cloud.[10] Throughout that time, the Clearing Agencies have continually refined their capabilities across technical, risk, legal, and compliance dimensions, in tandem with the Cloud's own evolution and the industry's increasing adoption of it. Given this extensive maturity and development over the past decade, the Clearing Agencies believe that hosting Core C&S Systems in the Cloud, via a single CSP, is now appropriate and essential. By consolidating resources under a single CSP, the Clearing Agencies can optimize efficiency, reduce costs, mitigate risks, and maintain a cohesive environment for seamless collaboration and operation.

As described in greater detail in this advance notice, the Clearing Agencies propose to provision, within a single CSP, logically segregated sections of the Cloud Infrastructure that would provide the Clearing Agencies with the virtual equivalent of physical data center resources, including scalable resources that can (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"). These resources would be logically segregated from other customers of the CSP. The Clearing Agencies would leverage the CSP's IaaS (i.e., infrastructure as a service) and PaaS (i.e., platform as a service) services for building and running Core C&S Systems.

The Clearing Agencies do not propose to transition all Core C&S Systems entirely out of their regional data centers at this time, but rather, to host a specified set of Core C&S Systems in a Cloud Infrastructure while maintaining the remaining applications in the Clearing Agencies' regional data centers for the near term. The proposed transition would be achieved incrementally

---

10 Some of the non-Core C&S Systems already operating in Cloud include systems that support risk analysis, various reporting engines, and shared infrastructure capabilities. More specifically, for risk analysis, there are applications for certain risk testing and calculations used to assess industry risk postures for various Clearing Agency clients, as well as warehousing large sets of risk data for quantitative analytics. For the various report engines, there are applications that provide publicly disseminatable data sets and documentation, certificate imaging, as well as certain archival storage capabilities. For shared infrastructure capabilities, there are applications that support the Clearing Agencies' engineering and development departments for dev-op capabilities such as code scanning, code repositories, and infrastructure-as-code deployment pipelines.

over a course of several years and would result in the Clearing Agencies hosting some Core C&S Systems on-premises and others in a Cloud Infrastructure.[11]

This phased approach to transitioning to Cloud is to reduce risk. The Clearing Agencies believe that a "big-bang" approach of moving all applications at once introduces significant execution risk, primarily driven by the sheer scale and scope of such an effort. Moreover, many clearance and settlement applications on the Clearing Agencies' mainframe are still tightly coupled together. Even after such applications are modernized, many could experience latency dependencies with other applications that have not yet been modernized, hence the need to keep some applications in the Clearing Agencies' existing data centers for the near term. However, applications with little to no coupling, particularly those applications that have already been modernized, are ripe for Cloud transition and the subject of this Cloud Proposal. As for the remaining clearance and settlement applications that are not part of this proposal and would continue to be hosted on-premises, the Clearing Agencies have not thoroughly assessed when those applications would transition to Cloud, which may take several years, or whether such transition would be the subject of a later, separate advance notice proposal.

Integration between on-premises and Cloud-based Core C&S Systems would, as it is for non-Core C&S Systems that are already hosted in private and public cloud, leverage existing patterns and processes. The primary methods of application integration are application program interfaces (a/k/a APIs), messaging queues (a/k/a MQ messaging), and file transfer. All three are used to integrate internal and client applications, and all three methods provide interoperability between applications running on mainframe, private cloud, and public cloud.

For these reasons, the Clearing Agencies strongly believe that the phased approach enables the Clearing Agencies to best approach the transition to Cloud, safely and confidently.

B. Why Use Cloud

The Clearing Agencies believe there are very strong and compelling reasons to use Cloud as part of their diverse, platform strategy, including, as discussed below, the waning of the on-premises industry, improved resilience, expanded security capabilities, and increased scalability.

1. Waning On-premises Industry

Although on-premises mainframes have been a stalwart for hosting critical applications for many years, it is the Clearing Agencies' experience that industry investment and development in on-premises platforms is waning, and the ability to source skilled and experienced staff to operate such platforms is increasingly challenging. Meanwhile, vendor consolidations are beginning to negatively affect investment and innovation in the private cloud space.[12] As investment dollars are increasingly allocated to Cloud, vendor choice, innovation,

---

11 A result of the Cloud Proposal would be that the Clearing Agencies would operate Reg. SCI and Critical SCI systems both on-premises and on a Cloud Infrastructure.

12 For example, the VBlock platform, which has been the core, private cloud distributed hosting platform of the Clearing Agencies for over a decade, is no longer available for

and support will continue to diminish for on-premises platforms. This poses a growing risk to the Clearing Agencies, who today continue to rely primarily upon on-premises mainframes and private cloud solutions from a resiliency perspective.[13] The Clearing Agencies believe the best way to manage against this risk at this time is to leverage a diverse platform strategy that will increase the use of and reliance upon Cloud. The use of Cloud, as part of a broader platform strategy, serves as an important tool in enabling the Clearing Agencies to anticipate and manage these and other risks more effectively.

2. Improved Resilience

The Clearing Agencies must ensure that any Core C&S Systems in the Cloud have resiliency and recovery capabilities commensurate with the Clearing Agencies' importance to the functioning of the U.S. financial markets. As explained in detail below, the Clearing Agencies believe that Cloud will enhance the resiliency of their Core C&S Systems by virtue of the Clearing Agencies' architectural design decisions, and the Cloud's redundancy, availability, and the Clearing Agencies' disciplined approach to deployment of Core C&S Systems to Cloud. In particular, the Clearing Agencies believe that Cloud will enhance their ability to withstand and recover from adverse conditions by provisioning redundant Compute, Storage, and Network resources in three availability zones, in each of two autonomous and geographically diverse regions, for a total of six availability zones that are comprised of many data centers.

The primary/hot region would be operational and accepting traffic, while the secondary/warm region would receive replicated data from the hot region with applications on stand-by. This solution significantly reduces operational complexity, mitigates the risk of human error by providing tools for automating routine tasks and orchestrating complex workflows, thereby reducing the need for manual intervention,[14] and provides resiliency and assured capacity (although, the Clearing Agencies would continue to periodically review the CSP's capacity planning process through quarterly reviews).[15]

---

purchase. Another example is the continued consolidation in the private cloud software space, which has concentrated the industry and reduce aggregate investment in innovation.

13 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).

14 The CSP's built-in security features in its Cloud Infrastructure also can reduce the risk of security breaches caused by human error, such as misconfigurations or improper access controls.

15 The Clearing Agencies would continue to perform periodic business continuity and disaster recovery tests to verify business continuity plans and disaster recovery infrastructure will support a two-hour recovery time objective for critical systems.

The Clearing Agencies are assured of adequate capacity with the proposed hot/warm architecture because the Compute resources of the warm, "recovery" region would be already running with needed capacity. Additionally, the Clearing Agencies have reviewed the effect of a large, regional outage with the CSP, which indicated that a vast majority of the CSP's customers are not configured to use the secondary region as a failover region; thus, they would not be using capacity in that region. Moreover, a review of data from two large outages in the primary region did not show a change in capacity availability in the secondary region.

The Clearing Agencies also believe that Cloud reduces capacity-management risks when compared with on-premises platforms in three important ways: (1) capacity in Cloud can be added almost instantly; (2) such capacity can be added at magnitudes greater than what is possible with traditional, on-premises platforms; and (3) the risk of a supply chain effect on capacity realization (i.e., the risks associated with receiving and deploying servers necessary to create more capacity) is greatly reduced.

The proposed hot/warm configuration also enables application rotation between regions. The Clearing Agencies would have the ability to operationally rotate either a single application, groups of applications, or all applications to the warm region for both planned and unplanned events. Collectively, the proposed design of the Cloud Infrastructure helps ensure that the Clearing Agencies can meet any applicable two-hour recovery time objective.

Each availability zone, in each of the two regions, would be comprised of multiple physical data centers. Each data center would have its own distinct physical infrastructure with separate staff and dedicated connections to utility power, standalone backup power sources, independent mechanical services, and independent network connectivity.

Although not dependent on each other, availability zones of a region are connected to each other with private, fiber-optic networking, enabling Core C&S Systems to automatically failover between a region's availability zones without interruption. Since each availability zone can operate independently, but failover capability is nearly instantaneous, a loss of one availability zone would not affect operation in another; therefore, no Core C&S System would be reliant on the functioning of a single availability zone.[16]

Altogether, the proposed Cloud Infrastructure would afford the Clearing Agencies six levels of redundancy (i.e., three availability zones, made up of many data centers, in each of the two regions), with primary/secondary regions running in a hot/warm configuration, respectively, in geographically separate and segregated locations, and with each region containing multiple copies of the data. Thus, even if an availability zone is lost in the primary region, the Cloud can

---

[16] To further ensure the resiliency of the Compute, Storage, and Network capabilities, the CSP's services are divided into "data plane" and "control plane" services. The Clearing Agencies' applications would run using data plane services, while control plane services are used to configure the environment. Resources and requests are further partitioned into cells, or multiple instantiations of a service that are segregated from each other and invisible to the CSP's customers, on each plane, again minimizing the effect of a potential incident to the smallest footprint possible.

continue to seamlessly operate Core C&S Systems in the primary region, thereby significantly reducing availability risk and any attendant consequences for the Clearing Agencies' participants and customers. As a result, the Cloud Infrastructure offers the Clearing Agencies multiple redundancies within which to run Core C&S Systems, limits the effect of an incident at the CSP to the smallest footprint possible, and mitigates the possibility of the Clearing Agencies suffering an intra-, inter-, or multi-region outage.

By comparison, the Clearing Agencies' current on-premises hosting capabilities, both mainframe and private cloud, are operating on one primary data center in one region, with a second, recovery data center in a second region (excluding data bunkers, which do not have Compute capabilities). In other words, it is many times less likely that an unplanned, out of region failover would be needed for Core C&S Systems hosted in Cloud than currently hosted on-premises. (Even in the unlikely event that the Clearing Agencies needed to fail over to the secondary Cloud region, the decision and process of doing so would continue to be in the sole discretion of the Clearing Agencies.) This increased redundancy represents a material improvement in resiliency for the Clearing Agencies and a material reduction in risk for the industry.

Additionally, transitioning to Cloud offers the Clearing Agencies a more effective strategy for avoiding technical debt and system degradation because the CSP, in its role as such, would be performing regular system upgrades and maintenance, helping to ensure the Cloud's resiliency. Unlike on-premises solutions that may struggle to keep pace with evolving technology, due in part to the waning demand for on-premises infrastructure, CSPs take on the responsibility of regularly updating and maintaining their cloud infrastructure, which they do in a competitive environment. This approach helps ensure that the CSP's cloud infrastructure remains up to date, secure, and performs at its best, minimizing the likelihood of accumulating technical debt and preventing the decline of system capabilities and resiliency over time. This is not to say that on-premises infrastructures are not updated or maintained today but, instead, that the CSP does it better and faster. CSPs excel in ensuring that systems remain up to date, secure, and perform at their best by leveraging automation, scalability, built-in security measures, service level agreements ("SLAs"), economies of scale, and continuous monitoring and improvement processes. These advantages collectively enable CSPs to provide more reliable, resilient, and high-performance services compared to traditional on-premises environments.

3. Expanded Security Capabilities

Hosting Core C&S Systems in Cloud would not change the physical and cybersecurity standards to which the Clearing Agencies currently align – the National Institute of Standards and Technology ("NIST")[17] and Center for Internet Security ("CIS").[18] Application of NIST is

---

17 National Institute of Standards and Technology (2023) The NIST Cybersecurity Framework 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (NIST CSWP) 29 ipd, Released August 8, 2023. https://doi.org/10.6028/NIST.CSWP.29.ipd.

18 Center for Internet Security Benchmarks, cisecurity.org/cis-benchmarks.

considered a best practice for financial services use of cloud.[19] Moreover, as discussed further below, the Clearing Agencies would continue to apply existing security processes and standards to include network and identity and access management ("IAM") controls, security governance and controls for sensitive data, security configuration, provisioning, logging and monitoring, and security testing and validations.

By hosting in Cloud through the CSP that the Clearing Agencies have engaged, the Clearing Agencies would be able to add cloud-specific security capabilities and measures provided by the CSP, as well as third-party tools. For example, such capabilities and measures would include automation, monitoring, and security incident response capabilities, as well as default separation between Reg. SCI and non-Reg. SCI operating domains, and ubiquitous encryption, all of which are not available in the current on-premises data centers. Similarly, micro-segmentation of applications and infrastructure provided by the CSP, which also is not available in the Clearing Agencies data centers, limits the effect of a security incident and reduces the time to detection and recovery.[20]

4. Increased Scalability

Cloud implementation would allow for greater scalability of Compute, Storage, and Network resources that support Core C&S Systems.[21] With a Cloud Infrastructure, the Clearing Agencies could quickly provision or de-provision Compute, Storage, or Network resources to meet demands, including elevated trade volumes, and provide more flexibility to create development and test environments, as well as other system development needs.[22] For example,

---

19 U.S. Department of the Treasury, *The Financial Services Sector's Adoption of Cloud Services* (February 8, 2024), available at https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf

20 For example, the CSP provides infrastructure capable of withstanding Distributed Denial of Service ("DDoS") attacks at far greater magnitudes than the Clearing Agencies' current capabilities, as the CSP has exponentially more internet bandwidth, given their business function, than the Clearing Agencies. (DDoS is a cyberattack in which the attacker floods a server with illegitimate traffic/requests to prevent legitimate users from accessing online services, websites, or computers connected to the attacked server.)

21 The Clearing Agencies would continue to follow existing policies and procedures regarding capacity planning and change management. The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the Change Management Policy and the Technology Capacity and Demand Assessment Policy. The Clearing Agencies have provided these documents in confidential Exhibit 3 to this advance notice filing.

22 The Clearing Agencies periodically perform capacity and availability planning analyses that result in capacity baselines and forecasts, as an input to technology delivery and strategic planning to ensure cost-justifiable support of operational business needs. These analyses are based on the collection of performance data, trending, scenarios, and periodic high-volume capacity stress tests and include storage capacity for log and record

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.

The Clearing Agencies would pre-provision Compute and Storage resources proactively, in addition to scaling resources on-demand. This means that the Clearing Agencies would be able to increase Compute capacity in one or both regions via manual or automated processes for Core C&S Systems. The rapid deployment of Compute capacity would allow the Clearing Agencies to obtain access to resources far more quickly than with on-premises data centers. The Clearing Agencies would combine the pre-provisioning of primary capacity with regular capacity stress testing to verify that the underlying Compute can sustain required business volumes. The stress testing data would be used to determine the base levels of pre-provisioned capacity.

The ability to quickly scale workloads materially improves the Clearing Agencies ability to respond to unexpected market events and external scenarios, such as a global pandemic.[23] This capability also enables the Clearing Agencies to run risk calculations more frequently, at greater speeds, and with more compute-intensive models than is economically feasible compared to the Clearing Agencies' on-premises infrastructure.

In sum, transitioning to Cloud not only enhances scalability but also significantly improves agility beyond the Clearing Agencies' on-premises capabilities. The on-demand resources provided by the CSP enable dynamic scalability, helping to ensure optimal performance during peak times, efficient resource allocation during periods of lower demand, and the ability to innovate faster to meet evolving business requirements.

C. Why a Single CSP is Appropriate

The Clearing Agencies strongly believe that hosting Core C&S Systems with a single CSP is appropriate. The Clearing Agencies have assessed the capabilities of the CSP in

---

retention. Results are reported to senior technology management as inputs to performance management and investment planning. In addition, each quarter, the Clearing Agencies review the CSP's capacity planning accuracy for the prior quarter and review the upcoming quarter's forecast, along with providing input to the CSP for anticipated major changes in the Clearing Agencies' proposed use of resources. The Clearing Agencies' IT Governance Committee is the designated escalation point for handling capacity management issues.

23 Supply chain challenges during the Covid-19 pandemic highlighted a lack of resiliency and scalability in traditional IT vendors' abilities to deliver resources when needed. Lead times of up to 18 months were experienced and delayed many efforts to expand capacity. This was not the case with CSPs, which did not experience capacity constraints or an ability to meet demand. This further demonstrates how the option to host Core C&S Systems in Cloud is a critical risk mitigation tool for managing against the long-term risk of a waning on-premises industry.

adherence with the Clearing Agency Risk Management Framework,[24] which requires the respective Board of Directors of the Clearing Agencies to approve policies governing relationships with service providers, such as the CSP, thus helping to ensure alignment with the Clearing Agencies' risk management principles.

Beyond simply being a well-known, reputable, industry-leading, and capable CSP, the Clearing Agencies and the CSP have spent several years discussing the Clearing Agencies' needs, including operational, legal, and regulatory obligations; what-if scenarios; and commercial implications. That extensive effort led to a number of benefits, including the CSP introducing new products[25] and the establishment of an exhaustive contractual agreement between the Clearing Agencies and the CSP that addresses the Clearing Agencies' needs for hosting Core C&S Systems in Cloud ("Cloud Agreement").[26] [27]

Meanwhile, it is generally understood that in the present environment adding a secondary CSP or an on-premises backup introduces significant complexity, costs, and risks that outweigh expected benefits.[28] An on-premises or secondary CSP backup would require the Clearing Agencies to engineer their primary Cloud Infrastructure to the lowest common denominator, so that the systems operating on the primary infrastructure also could run on a completely separate

---

24 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the Clearing Agency Risk Management Framework. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

25 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding two examples of CSP Whitepapers. The Clearing Agencies have provided these documents in confidential Exhibit 3 to this advance notice filing.

26 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the Cloud Agreement. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

27 Among other things, the Cloud Agreement sets forth the CSP's responsibility to maintain the hardware, software, networking, and facilities that run Cloud services. See also the separately submitted Table of Reg. SCI Provisions provided in confidential Exhibit 3 to this advance notice filing that provides a summary of the terms and conditions of the Cloud Agreement that the Clearing Agencies believe help enable their compliance with Reg. SCI.

28 As noted in the U.S. Department of Treasury's report, *The Financial Services Sector's Adoption of Cloud Services*, "No financial institution reported the capability to [run applications across multiple CSPs] for more complex use cases, such as running core operations on multiple public clouds. Running an application across multiple CSPs at the same time may also be less desirable, given the costs, staffing, and complexity involved in doing so, particularly given the complexity associated with identifying and managing risk across multiple cloud environments." Available at https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf at 6.

and distinct secondary, backup infrastructure. This approach would severely reduce the value that Cloud provides, introduce significant cost with little benefit, and greatly increase operational complexity, all of which would result in negative consequences for the efficiency and resiliency of the Clearing Agencies, their participants, and the industry.

Notwithstanding the extensive benefits from moving to Cloud, the Clearing Agencies fully appreciate and are committed to managing the risks presented in relying on a single CSP, as identified and discussed in Section II.A, further below.

D. Transition Timeframe

The Clearing Agencies believe that transitioning certain Core C&S Systems to the Cloud is critical to managing the risks that are inherent in technology and vendor selection. However, as stated above in Section I.A, the intent of the Cloud Proposal is not to move all Core C&S Systems to Cloud at one time. The Clearing Agencies believe that a "big-bang" transition would introduce unnecessary execution risk, primarily driven by the sheer scale and scope of such an effort. Moreover, many applications on the mainframe are still tightly coupled together and not ready to be moved to public cloud. Rather, at this time, the Clearing Agencies are proposing to move only a subset of the Core C&S Systems to the Cloud and to do so on an incremental basis, in consideration of the specifics of each application and the needs of the Clearing Agencies.[29] This approach helps enable the hosting of Core C&S Systems on the most appropriate platform, at the most appropriate time, in an efficient and secure manner.

The subset of Core C&S Systems selected for this proposal have been initially identified based on several preliminary criteria, including, but not limited to, whether:

- the application would benefit from the presence of data sets already present in Cloud;
- the application would benefit from elasticity enabled by Cloud (e.g., user interfaces); and
- the application already meets certain architectural patterns for Cloud (e.g., the application has already been modernized and currently hosted in private cloud and/or is a siloed application – little to no coupling with other applications).

Assuming the Clearing Agencies would receive no regulatory objection to this advance notice, each application of the proposed subset of Core C&S Systems then would undergo an in-depth, architectural review that would follow the Clearing Agencies' governance process,

---

[29] The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Global Business Continuity and Resilience Policy and Standards, which defines the governance structure, high-level roles and responsibilities, and the framework for business continuity and resilience processes at the Clearing Agencies. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

governed by the System Delivery Process.[30] The governance process includes, where applicable, a detailed review and approval by the Information Technology Architecture Review Board ("ARB"),[31] the New Initiatives process,[32] to include the Business Case Council and the Risk Assessment Council that vet the financials and risks of the proposed move, and the Investment Management Committee.[33] Further escalations would be made to the Executive Committee and applicable Board of Directors of the Clearing Agencies, as needed. Re-platforming efforts also would be communicated to regulators in accordance with the change reporting requirements of Section 1003(a)(1) of Reg. SCI, as applicable.[34]

The above-described governance process does not include a specific set of criteria or thresholds for the ultimate determination on whether an application should or should not be moved to Cloud – it is not a formulaic decision. Rather, the Clearing Agencies employ a more qualitative evaluation process that involves various reviews and considers high-level architectural principles that may be applicable to more than one application. However, at this time, none of the Core C&S Systems that have been initially identified as part of the Cloud Proposal, based on the preliminary criteria listed above, have completed that more detailed governance review process. Given the extensiveness of the process, it would not begin until after the Clearing Agencies would receive no regulatory objection to this advance notice.

Although the Clearing Agencies do not anticipate needing to deviate from the proposed transition schedule for the selected Core C&S Systems, the Clearing Agencies recognize that deviation may be necessary, given that the more in-depth governance review process has not completed and because risks could change over the proposed, multiyear implementation period. For example, a deviation may be necessary to address a business need or a change in industry or

---

30 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC System Delivery Policy. The System Delivery Policy defines requirements that support adherence to the System Delivery Process for application development projects. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

31 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the IT Architecture Policy ("ITA Policy"). The ITA Policy provides a set of controls that must be followed to adequately address applicable risks. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

32 The Clearing Agencies also have separately submitted a request for confidential treatment to the Commission regarding the New Initiatives Policy. The New Initiatives Policy provides the governance and oversight structure for the Clearing Agencies to bring initiatives to market timely and efficiently while minimizing risk. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

33 Such reviews and decisions are based on high-level architectural principles that may be applicable to more than one application.

34 17 CFR 242.1003, et seq.

regulatory requirements or standards. Regardless, any deviation would follow the same detailed governance process, and the Clearing Agencies would provide notice of such deviation to Commission staff, the reason for the deviation, and how the proposed implementation schedule would be updated to account for the deviation. Further, the Clearing Agencies recognize that deviating from the proposed transition schedule 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.

Even though certain on-premises infrastructure components would be decommissioned after applications are moved to Cloud, the Clearing Agencies' private cloud, mainframe services, and data-center facilities would remain available for no less than five more years to help facilitate exit plans from Cloud that rely on an on-premises option. However, to be clear, the on-premises option would not be available to address short-term disruptions, where the Cloud is temporarily unavailable. Management of such disruptions is discussed in Section II.B, further below.

II. Expected Effects on Risks to the Clearing Agencies, their Participants, or the Market

Although the Clearing Agencies are not proposing to transition all Core C&S Systems to Cloud for the reasons described in Sections I.A and D, above, transitioning the proposed subset of Core C&S Systems from an on-premises infrastructure supported by a consolidating industry, as described in Section I.B.1, above, to a new Cloud Infrastructure maintained by an industry-leading CSP provides numerous advantages, as described in Sections I.B.2-4 and C, above. However, such transition is not without risk, as discussed below.

A. Risks Presented by the Cloud Proposal

1. Concentration Risk

The Clearing Agencies appreciate that reliance on a single CSP for hosting the subset of Core C&S Systems that are the subject of this proposal creates concentration risk, particularly in the event of the CSP choosing to terminate its services (i.e., commercial risk) or is unexpectedly unavailable (i.e., operational risk). The Clearing Agencies also appreciate that they would have some reliance on the CSP to help meet certain regulatory obligations of the Clearing Agencies (i.e., regulatory risk), thus introducing the familiar concept of concentration risk in a relatively new context. However, concentration risk exists today as the Clearing Agencies are dependent on a single mainframe provider, a single database provider for the mainframe, and a single virtualization provider for private cloud. Moreover, the Clearing Agencies believe that they have adequately addressed these risks, as discussed throughout Sections II.B.1-4., below.

2. Cloud Management Risk

Managing the applicable subset of Core C&S Systems hosted on a Cloud Infrastructure presents different risks and challenges than managing such systems hosted on-premises because many activities and services previously provided by the Clearing Agencies would now be provided by the CSP. For example, the Clearing Agencies would be dependent upon the CSP for fulfilling all of its contractual obligations, including security of the Cloud, proper capacity

planning, and protection of Cloud services from prolonged operational outages. As such, overseeing the CSP becomes a critical activity to ensure the CSP is delivering services that meet or exceed the Clearing Agencies' requirements for operating those select Core C&S Systems. As discussed in Sections II.B.1-4, below, the Clearing Agencies believe that they have adequately addressed this risk.

B. Management and Mitigation of Identified Risks

1. Cloud Agreement

The Clearing Agencies believe that the Cloud Agreement, including all its amendments and addendums, is a strong tool in helping to effectively mitigate the commercial and regulatory risks borne from the concentration risk, as described in Section II.A.1, above, as well as risks in managing the CSP that would host the subset of selected Core C&S Systems in the Cloud, as described in Section II.A.2, above. Following is a summary of some of the key terms and conditions covered in the agreement and how they help mitigate these risks.

i. Adequate Notice

Under the Cloud Agreement, the CSP may not unilaterally terminate the relationship with the Clearing Agencies absent good cause or without sufficient notice to allow the Clearing Agencies to transition their applications elsewhere. Specifically, 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 SLA on which the Clearing Agencies rely.[35]

---

[35] The Cloud Agreement permits an exception to this sufficient notice provision in the event the CSP must terminate the individual service offering if necessary to comply with the law or requests of a government entity or to respond to claims, litigation, or loss of license rights related to third-party intellectual property rights. In this event, the CSP must provide reasonable notice to the Clearing Agencies of the termination of the individual service offering. See Reg. SCI Addendum, Section 10 *Termination*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

The CSP is permitted to terminate the Cloud Agreement with shorter notice periods in the event of a critical breach[36] or an uncured material breach[37] [38] of the Cloud Agreement. In the highly unlikely event that a critical breach or uncured material breach occurs, the Clearing Agencies would have sufficient notice to shift their operations away from the CSP. Contract provisions that allow a party to terminate for uncured material breaches are designed to limit the types of actions that could lead to contract termination and to establish a period of time to resolve an aggrieved party's claim (often 30 days) followed by an additional extended period in which to remediate the claim. This gives the parties time and incentive to address the problem without having to resort to termination. In other words, even if the CSP notifies the Clearing Agencies of an alleged breach (material or critical), termination of services is not immediate. Additionally, regardless of the need to shift operations elsewhere – convenience or breach – the Cloud Agreement provides for the parties to work together and for the CSP to provide professional services to assist with such a shift.[39]

The Clearing Agencies believe the risk of termination under the above-discussed shorter notice period is minimal. 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 ("Notice Period").[40] With respect to an alleged material breach, which requires the CSP to extend the Notice Period if the Clearing Agencies demonstrate a good faith effort to cure the alleged material breach, the Clearing Agencies would use the Notice Period to attempt to cure the alleged material breach while also preparing to transition elsewhere. As a result, it is highly unlikely that a critical breach or a material breach would remain uncured beyond the Notice Period. If one does remain uncured, however, the CSP can only terminate the rights or accounts associated with the breach,

---

36 Critical breaches are material breaches (i) for which the Clearing Agencies knew their behavior would cause a material breach (such as a willful violation of Cloud Agreement terms); (ii) that cause ongoing material harm to the CSP, its services, or its customers (e.g., criminal misuse of the services); or (iii) for undisputed non-payment under the Cloud Agreement. See Reg. SCI Addendum, Section 10 *Termination*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

37 Typically, a breach is considered material only if it goes to the root of the agreement between the parties or is so substantial that it defeats the object of the parties in making the contract. See Reg. SCI Addendum, Section 10 *Termination*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

38 See Reg. SCI Addendum, Section 10 *Termination*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

39 See Reg. SCI Addendum, Section 11 *Post-Termination Services*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

40 See Reg. SCI Addendum, Section 10 *Termination*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

not the entire Cloud Agreement;[41] meanwhile, and the Clearing Agencies would have ample notice to shift operations to avoid a disruption to Core C&S Systems, if needed.

As explained above, adequate notice under the Cloud Agreement plays an important role in managing concentration risk by providing the Clearing Agencies with advance warning of potential disruptions or changes in the agreement or services thereunder, which would allow the Clearing Agencies to take proactive measures in mitigating the potential impact of commercial and regulatory risk, thereby reducing concentration risk.

ii. Regulatory Compliance and CSP Oversight

The Clearing Agencies' transition to Cloud does not alter their responsibility to maintain compliance with applicable regulations. Consistent with FFIEC Guidance (as defined and discussed further below), the Clearing Agencies' will continue to fully comply with all applicable regulatory obligations, particularly Reg. SCI.[42]

The Clearing Agencies believe the combination of the following would provide them with reasonable assurance that the proposed transition to Cloud would enable them to continue to fully satisfy their regulatory obligations, including Reg. SCI, thus helping to mitigate the regulatory risk highlighted in Section II.A.1, above: (i) the Cloud Agreement; (ii) the CSP's compliance programs as described in its whitepapers[43] and publicly available policies (e.g., its

---

41 See Amendment 1, Section 8 *Temporary Suspension*, of the Cloud Agreement. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

42 Reg. SCI imposes certain information security and incident reporting standards on the Clearing Agencies and requires them to adopt an information technology governance framework reasonably designed to ensure that "SCI systems," and for purpose of security, "indirect SCI systems," have adequate levels of capacity, integrity, resiliency, availability, and security. 17 CFR 242.1000 et seq.

43 Supra note 25.

Penetration Testing Policy),[44] [45] [46] [47] and user guides; (iii) the CSP's SLAs;[48] [49] [50](iv) the CSP's Systems Organization Controls reports (e.g., SOC 1, SOC 2, SOC 3)[51] and International

---

44 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the Operational & Technology Risk Technology Risk Management ("OTR CS&TRM") 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. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

45 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the EAPT Control Standards. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

46 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Information Security – Systems Acquisition Development and Maintenance Policy and Control Standards, which governs the security aspects of information systems acquisition, development, and maintenance for DTCC and its subsidiaries. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

47 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Information Security – Communications and Operations Policy and Control Standards, which helps ensure the correct and secure operation of information processing facilities. The Clearing Agencies have provided this document in confidential Exhibit 3 The Clearing Agencies have provided this document in confidential Exhibit 3to this advance notice filing.

48 The Clearing Agencies have provided the CSP's SLAs in confidential Exhibit 3 to this advance notice filing.

49 Amendment 2, Section 2.2 *To the Service Level Agreements* of the Cloud Agreement provides that the CSP may change its SLAs from time to time but must provide prior notice to the Clearing Agencies before material reducing the benefits offered under the SLAs. The Clearing Agencies have provided Cloud Agreement in confidential Exhibit 3 to this advance notice filing.

50 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Legal Review of Third Party Vendor Contracts Policy, which (1) defines the scope of Vendor Contracts, (2) clarifies what agreements fall outside the scope and are excluded from the definition of Vendor Contracts, (3) details the process the Clearing Agencies follow when receiving requests to review Vendor Contracts and related materials from CPS Contracts, and (4) establishes the requirements around the creation, maintenance, update, review, and use of contract

Organization for Standardization ("ISO") certifications (e.g., ISO 27001);[52] (v) the CSP's size, scale, and ability to deploy extensive resources to protect and secure its facilities and services; and (vi) the CSP's commercial incentive to perform.

Moreover, as noted in Section II.B.ii., above, oversight of the CSP relationship and services has become a standing practice of the Clearing Agencies to ensure that the CSP is meeting or exceeding its contractual obligations, including helping the Clearing Agencies demonstrate their regulatory compliance. Such oversight, which also helps mitigate the cloud management risk raised in Section II.A.2, above, would include a strong relationship between the CSP and the Clearing Agencies, including between their senior management. Within the Cloud Agreement itself, there are established obligations on the CSP to provide the Clearing Agencies' information necessary for the Clearing Agencies to satisfy certain compliance and regulatory requirements, particularly Reg. SCI. For example, the Cloud Agreement 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.[53] The agreement also provides for detailed quarterly briefing meetings between the Clearing Agencies and the CSP, during which the Clearing Agencies would be provided information on and could review service level performance, material systems changes, capacity management, SLA updates, and important security notices.[54]

The Cloud Agreement permits the Clearing Agencies to perform an annual review of the CSP's documentation and services to gain comfort that the CSP is meeting its contractual requirements and that the notification procedures are in place to allow the Clearing Agencies to meet their regulatory requirements, particularly Reg. SCI. The agreement also allows a regulator

---

templates and negotiation guidelines for third party relationships. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

51 The FFIEC Guidance provides that the Clearing Agencies may obtain SOC reports, other independent audits, or ISO certification reports to gain assurance that the CSP's controls are operating effectively. See FFIEC, Security in a Cloud Computing Environment at 7. The Clearing Agencies review the CSP's SOC-2 on an annual basis.

52 The CSP has certifications for the following frameworks: NIST, Cloud Security Alliance, Control Objectives for Information and Related Technology ("COBIT"), ISO, and the Federal Information Security Management Act ("FISMA").

53 See Reg. SCI Addendum, Sections 8.1 *Systems Intrusion Notification* and 4 *Briefing Meetings*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

54 Id.

of the Clearing Agencies 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.[55]

2. Cloud Architecture

To mitigate operational risk associated with the concentration risk from relying on a single CSP, the Clearing Agencies would architect the Cloud Infrastructure hosting their Core C&S Systems to be highly resilient, improving the availability of such systems and related Clearing Agency services during any degradation in CSP services:

- Use of multiple availability zones per region. The Clearing Agencies would use at least three availability zones, in each of the two CSP regions, with each availability zone made up of multiple data centers.

- Multi-regions. In the event of a primary region outage, the Clearing Agencies would recover in the secondary region. Out-of-region recovery would be tested annually by the Clearing Agencies, and a primary/secondary (i.e., hot/warm) model would be used to ensure continuous data replication and recovery is achieved.[56] Recovery exercises of non-Core C&S Systems currently hosted in cloud demonstrate the ability to recover applications within required recovery time objectives, including meeting a 2-hour recovery time objective for relevant applications in the event of an out-of-region recovery.

- Multi-node, high availability clusters across availability zones. Clusters (i.e., three or more servers or nodes) protect against local hardware and service failures providing uninterrupted operations. Each cluster would be distributed across three availability zones. Clusters synchronously replicate data across all nodes to protect against data loss and provide continuous availability.

- Static stability and static capacity models. Static capacity would be pre-provisioned for compute, storage, and memory for applications based on capacity stress testing results and capacity requirements. The Clearing Agencies would pre-provision capacity needed for applications and services and would not rely on capacity on-demand models, thus reducing the risk of running out of capacity.

- Exit plans. The Clearing Agencies' existing policies require that all applications hosted in Cloud have documented exit plans, with each plan updated annually.[57] The

---

55 See Reg. SCI Addendum, Sections 3 *Customer Right of Access and Audit* and 4 *Briefing Meetings*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

56 See Reg. SCI Addendum, Section 5 *Customer Testing of CSP Systems*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

57 Supra note 29.

Clearing Agencies' Cloud architecture also reduces "vendor lock-in" by using capabilities such as "containers"[58] that can exist in both the public and private cloud, where appropriate and applicable. For the foreseeable future, the Clearing Agencies plan to continue to own or lease private data center space to host private cloud and mainframe capabilities. The Clearing Agencies private, on-premises data centers help enable a long-term exit plan from Cloud, if needed. However, such data centers would not be a means to address a short-term incident at the CSP. Additionally, for the second CSP that the Clearing Agencies already have contracted and connected with for hosting non-Core C&S Systems, they are now working on the contractual and operational requirements that would be necessary to possibly host Core C&S Systems in its Cloud to further enable exit plans from the primary CSP.

- Regional Isolation Architecture. A cross-regional outage is highly unlikely at the CSP, as the CSP has designed and implemented a series of controls to ensure that defects cannot be introduced to more than a single region at a time.[59] Services are regionally isolated with a single exception – the IAM service. The IAM service is not regionally isolated and depends on a single region. If the primary region for the IAM service fails, the service will continue to operate but as read-only. To mitigate this risk, the Clearing Agencies would architect applications and infrastructure services in such a manner that they would not require updates (i.e., writes) to the IAM service in order to rotate out of region.

In summary, cloud architecture helps mitigate operational risk borne from concentration risk, as raised in Section II.A.1, above, by providing resilient infrastructure, scalable resources, robust security measures, and disaster recovery capabilities, all of which assist in minimizing the impact of disruptions.

3. Standing Risk Management Practices

The Clearing Agencies' standing risk management practices also help minimize operational risk by systemically identifying, assessing, mitigating, monitoring, and responding to risk. For example, the Clearing Agencies have considered the possibility of the CSP being completely and unexpectedly unavailable, whether due to technical issues or other reasons. The parallel risk exists today with respect to the Clearing Agencies' existing infrastructure. Just like with the CSP, it is possible that the Clearing Agencies' two existing data centers – one primary and one backup – become completely and unexpectedly unavailable. In fact, it is more likely that those two data centers become unavailable than the CSP's data centers because the CSP has so many more data centers for each availability zone, in both its primary and secondary regions, with each data center, not just the associated region or availability zone, having its own physical

---

58 A container is a standard unit of software that packages up code and all its dependencies, so the application runs reliably from one computing environment to another (e.g., public and private clouds).

59 The CSP owns the control and has provided documentation of the control to the Clearing Agencies.

infrastructure, staff, power, backup power, mechanical services, and network connectivity, as discussed in Section I.B.2, above. Even for the CSP's IAM service that runs cross regions, the applications in each region operate off read-only versions of the IAM roles and responsibilities, such that loss of the primary would not affect operation of those applications. Nevertheless, to help manage a crisis event, such as the Clearing Agencies' or the CSP's data centers becoming unavailable, the Clearing Agencies have standing risk management plans and practices already in place, as described below.[60]

In the very unlikely event of an unexpected single- or multi-region outage in which the Clearing Agencies operate, or a complete and unexpected CSP outage, the Clearing Agencies would initiate the existing Major Incident Management ("MIM") 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 ("BIMS")[61] would be activated. Depending on the severity of the event, the DTCC Global Business Continuity and Resilience ("BCR") Policy would provide a predictable structure to be utilized during crises and could be leveraged to address, respond to, and manage an outage.[62] 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.[63]

---

60 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the Operational Response Capabilities Matrix. The Clearing Agencies have provided these documents in confidential Exhibit 3 to this advance notice filing.

61 MIM is part of the IT organization that manages technology specific incidents at the Clearing Agencies that are typically resolved at the application or hardware level with support from the appropriate subject matter experts ("SMEs"). Incidents that have a business impact are escalated to BIMS and appropriate SMEs are added to manage the impact, which includes Business Continuity and Resilience. BIMS participants can request the Crisis Management Team be activated if the incident requires discussion or has escalated to a potential disaster that may require a declaration of disaster.

62 The Clearing Agencies are taking into consideration the forthcoming requirements of adopted and effective Rule 17ad–25(i) under the Exchange Act, 17 CFR 240.17ad–25(i), and anticipate that the Clearing Agencies' approach in managing the risk presented by a CSP outage for Core C&S Systems would be consistent with those requirements.

63 For example, there is an existing plan to manage a Fedwire protracted outage. A Fedwire protracted outage is an interruption or outage of Federal Reserve Bank hardware or software that prevents the bank from processing payment orders online and that is not expected to be resolved before the bank's next Fedwire Funds Service Funds Transfer Business Day. In the event of such an outage, the Clearing Agencies will assess the situation and employ, as needed and applicable, the steps outlined in the BCR Policy and Standards, the Federal Reserve Banks Operating Circulars (see, e.g., Operating Circular No. 6, available at

The BCR Policy and Standards is structured to employ existing DTCC and Clearing Agency teams and committees, which become the tactical leadership to react, respond, and manage a crisis situation.[64] The teams are comprised of the following:

- Crisis Management Team. Comprised of the Management Committee, site General Managers, Head of the Board Risk Committee,[65] and other SMEs, as needed.

- Crisis Response Teams.

    - *Business Continuity Coordinators and Plan Approvers* – These are individuals who manage business continuity at a plan level.

    - *Fair and Orderly Markets Groups* – These are crisis teams comprised of internal stakeholders and top executives from external firms deemed necessary to ensure a fair and orderly market. They would be activated (based on impact to the legal entity) to gather information during a large systemic event when operational coordination is required with clients and the sector.

    - *IT Management Team* – Comprised of Information Technology managing directors and SMEs.

    - *Management Risk Committee* – Comprised of senior members across the enterprise.

    - *Senior Site Management Team ("SSMT")* – Each DTCC office with a facility level resilience plan ("FLRP") has an SSMT, that is comprised of senior leadership from the site.

---

https://www.frbservices.org/binaries/content/assets/crsocms/resources/rules-regulations/070123-operating-circular-6.pdf), and any other regulatory guidance.

64 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. The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the BCR Policy and Standards which define the governance structure, high-level roles and responsibilities, and the framework for business continuity and resilience processes at the Clearing Agencies. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

65 The Board Risk Committee is a Board level committee established by the Boards of the Clearing Agencies to assist their respective Boards in fulfilling their responsibilities for oversight of risk management activities at the Clearing Agencies. This includes oversight of credit, market, liquidity, operational, and systemic risks.

- *Site Assessment Team ("SAT")* – Sites with an FLRP have a SAT that responds to site-specific events. This team is comprised of a primary/back-up site General Manager and representatives from BCR, IT, Workplace Design and Service, Global Security Management, and Human Resources. A Data Center Services representative also is added for sites that have a data center.

- *MIM and BIMS Teams* – Part of the IT organization that manages technology specific and are typically resolved at the application or hardware level with support from the appropriate SMEs.

- Crisis Communication Team. The Crisis Communication Team is comprised of officer-level members from Marketing and Communication, Human Resources, General Counsel's Office, and Regulatory Relations, as well as members of their staffs, as applicable.

The Clearing Agencies believe that these standing risk management practices are key to managing the operational risk borne from concentration risk outlined in Section II.A.1, above, by helping to promote proactive risk management culture, enhancing operational resilience, and enabling the Clearing Agencies to better navigate uncertainties and maintain business continuity.

4. Industry Standards for Cloud Management

i. Cloud Management: Federal Financial Institutions Examination Council Cloud Computing Guidance ("FFIEC")

On April 30, 2020, FFIEC[66] issued a joint statement to address the use of Cloud computing services and security risk management principles in the financial services sector ("FFIEC Guidance").[67] While the FFIEC Guidance does not contain regulatory obligations, it highlights risk management practices that financial institutions should adopt for the safe and sound use of Cloud computing services in five broad areas ("FFIEC Risk Management Categories"): Governance, Cloud Security Management, Change Management, Resilience and Recovery, and Audit and Control Assessment. As discussed below, the Clearing Agencies would implement practices consistent with the FFIEC Risk Management Categories for Core C&S Systems operated in Cloud to help address cloud management risk, as highlighted in Section II.A.2, above, by providing frameworks, guidelines, and best practices, that enhance transparency, reliability, and security.

---

66 FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Consumer Financial Protection Bureau, and to make recommendations to promote uniformity in the supervision of financial institutions.

67 Available at https://www.ffiec.gov/press/pr043020.htm.

(a) Governance

The Clearing Agencies and the CSP rely on a shared responsibility model that differentiates between security "of" the Cloud and security "in" the Cloud.[68] This model is not specific to the agreement between the Clearing Agencies and the CSP; rather, it is a more universally followed model for public cloud services. Under the model, the CSP maintains sole responsibility and control over the security and resiliency "of" the Cloud, and their customers are responsible for the security and resiliency "in" the Cloud (i.e., security and resiliency of hosted applications and data). This means that the Clearing Agencies must manage their own application architectures, data backups, change management controls, network configurations within applications, and response to application failures. In addition, the Clearing Agencies must manage their own data usage and data-at-rest encryption configuration, IAM access policies and roles, operating system upkeep, security group configurations, and network traffic encryption in transit configurations. The Clearing Agencies also manage how they place workloads onto the CSP's platform.

Meanwhile, the CSP must manage backend hardware services for Compute, Storage, Networking, database, and global architectures such as regions, availability zones, data centers, power, and HVAC, as well as backend security services that protect core infrastructures. The CSP manages the underlying infrastructure and upkeep, so that the Clearing Agencies (and other customers) can place workloads on the CSP platform with proper security and separation without having to manage these traditional data center tasks. The Clearing Agencies review the CSP's policies and procedures for these functions during the quarterly reviews and during annual risk assessments.

When looking more closely at hardware management, the Clearing Agencies believe there are benefits in how the CSP manages hardware for Cloud compared to how the Clearing Agencies manage hardware for their own data centers. For example, with on-premises data centers, the Clearing Agencies must oversee a multifaceted supply chain, involving many vendors to obtain and administer physical Compute, Storage, and Network capacity. Delivery times may fluctuate, and scarcities can affect project outcomes, as seen during the Covid-19 pandemic. In contrast, with the proposed Cloud Infrastructure, the CSP controls the hardware supply chain and even partakes in key areas of the manufacturing process to circumvent typical problems such as chip shortages. Moreover, the Clearing Agencies get to review the CSP's equipment forecast for each upcoming quarter, affording the Clearing Agencies the opportunity to address potential supply chain difficulties, if any, without jeopardizing their access to adequate capacity, by leveraging capabilities such as reserved capacity. Altogether, the Clearing Agencies believe the CSP's management of Cloud hardware will be a benefit to them.

The CSP would perform its own risk and vulnerability assessments of the CSP infrastructure on which the Clearing Agencies would run their Core C&S Systems. In published

---

68 "Shared responsibility" conveys the responsibility of the Clearing Agencies and the CSP vis-à-vis each other from a business operations perspective. It does not mean that the CSP has taken on or that the Clearing Agencies have relinquished any of their Reg. SCI compliance requirements.

documentation and in meetings conducted with the CSP, the CSP asserts that it maintains an industry-leading automated test system, with strong executive oversight, and conducts full-scope assessments of its hardware, infrastructure, internal threats, and application software. The CSP asserts that it has an aggressive program for conducting internal adversarial assessments ("Red Team") designed not only to evaluate system security but also the processes used to monitor and defend its infrastructure. The CSP also uses external, third-party assessments as a cross-check against its own results and to ensure that testing is conducted in an independent fashion. Pursuant to the CSP's documentation, results of these processes are reviewed weekly by the CSP's Chief Information Security Officer and the Chief Executive Officer with senior CSP leaders to discuss security and action plans.[69]

The Clearing Agencies have the responsibility to perform risk assessments and technical security testing, including control validation, penetration testing, and adversarial testing of their applications running on the Cloud Infrastructure. This includes testing of the application interface layer of some CSP provided services such as storage and key management.

As mentioned, the Clearing Agencies' testing includes assessing the configuration of the CSP provided services. The Clearing Agencies' Technology Risk Management staff would work with the Clearing Agencies' Information Technology staff to ensure that the CSP tools are configured to appropriately manage and mitigate potential sources of risk and will assess the effectiveness of those configurations.[70] The Technology Risk Management staff has developed an application, Cloud Governance Insights ("CGI"), to continuously monitor all Cloud Infrastructure for alignment to security baselines and configurations best practices.[71] The CGI dashboard allows Information Technology and Technology Risk Management staff to understand

---

69 The CSP does not provide assessment results to its customers, as doing so would constitute a breach of generally accepted security best practices. Instead, the CSP provides its customers with industry-standard reports – such as SOC2 Type II – prepared by an independent third-party auditor to provide relevant contextual information to its customers. The CSP also conducts periodic audit meetings specifically designed to discuss security concerns with its customers discussed later during the "CSP Audit Symposium." Additionally, the Clearing Agencies have certain audit rights (pursuant to Section 3 *Customer Rights of Access and Audit* of the Reg. SCI Addendum) to review information about the nature and scope of the CSP's vulnerability management program.

70 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the OTR TRM Core Process Procedure – Security Configuration Violation Rules, which is used to manage enterprise information security risk by ensuring a consistent configuration violation scoring process that provides timely identification of configuration violations and their severity ratings. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

71 CGI is the Clearing Agencies' internally developed solution to perform Cloud Security Posture Management and assess Cloud Infrastructure compliance against TRM Control Standards and Security Baselines in near real-time.

the environment risk posture and reporting of key risk indicators ("KRIs"). The Clearing Agencies' Red Team would operate freely "in the Cloud," attempting to subvert or circumvent controls.[72] The testing would include probing of the CSP provided services to look for weaknesses in the Clearing Agencies' deployment of those tools.

Technology Risk Management staff would routinely report test results to the Technology Risk Management Steering Committee and the Management Risk Committee, appropriate functional Operations and Information Technology management, senior management, and the Board of Directors of the Clearing Agencies.[73] [74] Automated vulnerability scanning reports, source code analysis, and results of specific assessments would be risk-rated and assigned a priority for remediation in accordance with Clearing Agency Information Security Program requirements.[75] [76]

Management and oversight of the Cloud implementation follows the Clearing Agencies' standard governing principles for large information technology projects.[77] To maintain accountability over the CSP's performance, regular reporting to the Boards of the Clearing Agencies by senior management is essential and required, pursuant to the DTCC Third Party

---

72 Supra note 47.

73 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Information Security – Information Security Management Policy and Control Standards, which defines the roles, responsibilities, and accountabilities for DTCC's security practices and organization structure suited to protect DTCC's critical systems and business assets. Information Security Management evaluates DTCC's information security program's overall effectiveness, and establishes, maintains, communicates, and periodically reassesses information security policies and a comprehensive information security program that are approved by management. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

74 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Information Security – Risk Management Policy and Control Standards, which provides (i) requirements for establishing, implementing, maintaining, and continually improving the information risk management program, (ii) a governance structure utilized for the escalation of information risks to an appropriate management level, and (iii) organizational roles and responsibilities for the delivery of comprehensive information security and technology risk management program. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

75 Supra note 46.

76 Supra note 47.

77 Supra note 32.

Risk Procedures.[78] Such reporting helps ensure that senior management takes appropriate actions to address significant performance deterioration, changing risks, or material issues identified through ongoing monitoring, thereby helping to ensure proactive risk management and continuous improvement.[79] The Clearing Agencies' Board of Directors has established a Technology and Cyber Committee to assist the Board of Directors in overseeing information technology and cybersecurity strategy and capabilities.

Information Technology and the Enterprise Program Management Office ("EPMO") are responsible for the identification, management, monitoring, and reporting on the risks associated with the modernization and migration of applications to Cloud. To that end, reports on the status and progress of these efforts are reported to applicable Clearing Agency committees based on escalation criteria in the EPMO Procedure.[80] These reports include overall risk and issue summaries and analysis of key risk indicators for the migration of applications to the public cloud.

Finally, the Clearing Agencies' Internal Audit Department ("IAD"), as the independent third line of defense, is responsible for assessing and challenging the firm's control environment and risk management and control frameworks, which include those related to the Cloud, including, but not limited to, security controls and configurations, and report the results of those assessments to management and the Audit Committee of the Board.[81]

Ultimately, there is no primary/secondary relationship, as the Clearing Agencies and the CSP each have their own set of responsibilities which, when combined, address the entire risk space.

---

78 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Third Party Risk Procedures, which establish the standards and practices to be used by certain business line departments and/or functional units to manage the potential risks associated with engaging with an external service provider. The Clearing Agencies have provided these documents in confidential Exhibit 3 to this advance notice filing.

79 Supra note 62.

80 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the Enterprise Program Management Office Procedure, which outlines the minimum standards and practices the Clearing Agencies use to manage, measure, and monitor the performance of key processes aligned to the Enterprise Program Management Office Policy. The Clearing Agencies have provided these documents in confidential Exhibit 3 to this advance notice filing.

81 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the Internal Audit Department Policies and Procedures, which contains the policies and guidance that direct the activities of the Clearing Agencies' IAD. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

(b) Cloud Security Management

The Clearing Agencies have established a robust Cloud security program to (i) manage the security of the Core C&S Systems that would be running on the Cloud Infrastructure hosted by the CSP, and (ii) assess and monitor the CSP management of security of the Cloud Infrastructure that it operates. The security program is built upon Clearing Agency Information Security Policies and Control Standards that establish requirements that apply to any technology system as well as any tool that provides technology services.[82] [83] [84] [85] Below describes elements of the Clearing Agencies' Cloud security management in the areas of (i) IAM controls (i.e., determining who is accessing the systems, granting access to the applications, and then controlling what information they can access); (ii) security governance and controls for sensitive data; (iii) security configuration, provisioning, logging, and monitoring; and (iv) security testing.

(1) Network and IAM Controls

The Clearing Agencies recognize that robust network security configuration and IAM would provide reasonable assurance that users – including Clearing Agency employees, market

---

82 Supra notes 46-47, 73-74.

83 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Information Security – Asset Security Policy and Control Standards, which governs management of security for the information assets of the Clearing Agencies. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

84 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Information Security – Monitoring and Incident Management Policy and Control Standards, which governs DTCC's 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. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

85 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Information Security – Asset Access Control Policy and Standards, which governs management of security for the information assets of the DTCC and its subsidiaries. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

participants, and service accounts for systems[86] – are granted least-privileged access[87] to the network, applications, and data in the Cloud. The Clearing Agencies would use third-party tools to automate appropriate role-based access to the Core C&S Systems running in the Cloud. By enforcing strict separation of duties and least-privileged access for infrastructure, applications, and data, the Clearing Agencies would protect the confidentiality, availability, and integrity of the data in the Cloud.

The Clearing Agencies have established IAM requirements that build upon the least-privileged model.[88] As part of the IAM program, all users must be assigned an appropriate enterprise identification. Additionally, the Clearing Agencies have established Highly Privileged Access Management capabilities and policies to further restrict highly privileged access to be used only in pre-determined scenarios that must be tied to a change, incident, request, or release records.[89]

Cloud users would be granted access to systems via a standardized and auditable approval process. The user identifications and granted access would be managed through their full lifecycle from a centralized IAM system maintained and administered by the Clearing Agencies. Role-, attribute-, and context-based access controls would be used as defined by internal standards[90] consistent with industry recommended practices to promote the principles of least-privileged access and separation of duties.[91]

The Clearing Agencies would use and manage third-party tools not otherwise provided by nor managed by the CSP for single sign-on and least-privileged access.[92] The network also would include hardware and software to limit and monitor ingress and egress traffic, encrypt data

---

86 Service accounts are non-interactive accounts that permit application access to support activities such as monitoring, logging, or backup. Service accounts are also used for machine-to-machine communications.

87 Least-privileged access means users only have the permission needed to perform their work, and no more.

88 Supra note 85.

89 Id.

90 Id.

91 (1) ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security controls; (2) NIST Cybersecurity Framework (CSF) Version 1.1; (3) NIST Special Publication 800-53 Revision 4 – Security and Privacy Controls for Federal Information Systems and Organizations.

92 For example, the Clearing Agencies currently use Bravura Security Privileged Access Management (a/k/a PAM) for highly privileged access management.

in transmission, and isolate traffic between the Clearing Agencies and the Cloud.[93] Since the Clearing Agencies would continue to provide cryptographic services, including key management, the CSP and other network service providers would not be able to decrypt Clearing Agency data either at rest or while in transit.

(2) Security Governance and Controls for Sensitive Data

The Clearing Agencies' data governance framework that would apply to Cloud implementation is identified within the Clearing Agency Information Security Policies and Control Standards.[94] The Clearing Agency Information Security Policies and Control Standards address data moving between systems within the Cloud as well as data transiting and traversing both trusted and untrusted networks. For example, the Clearing Agencies' Information Security Policies and Control Standards require a system or Software as a Service (i.e., SaaS) to (i) store data and information, including all copies of data and information in the system, in the U.S., throughout its lifecycle; (ii) be able to retrieve and access the data and information throughout its lifecycle; (iii) for data in the system hosted in the Cloud, encrypt such data with key pairs kept and owned by the Clearing Agencies; (iv) comply with U.S. federal and applicable state data regulations regarding data location; and (v) enable secure disposition of non-records in accordance with the Clearing Agencies' Information Governance Policy.[95]

Furthermore, the Clearing Agencies' policies establish the overall data governance framework applied to the management, use, and governance of Clearing Agency information to include digital instantiations, storage media, or whether the information is located, processed, stored, or transmitted on the Clearing Agencies' information systems and networks; public, private, or hybrid cloud infrastructures; third-party data centers and data repositories; or SaaS applications.[96] The Information Classification and Handling Policy[97] classifies the Clearing Agencies' information into categories. System owners of technology that enable classification and/or labeling of information are responsible for ensuring the correct classification level is designated in the system of record and the applicable controls are enforced. All information requiring disposal is required to be disposed of securely in accordance with all applicable

---

93 Supra notes 47, 84-85.

94 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Data Risk Management Policy, which establishes requirements for the sound management of data risk across the data lifecycle. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

95 Supra note 85.

96 Supra note 46.

97 Supra note 83.

procedures. Sensitive data must be handled in a manner consistent with requirements in the Information Classification and Handling Policy.

The Clearing Agencies would implement key security components, namely ubiquitous authentication, and encryption via use of an automated public key infrastructure, coupled with responsive, highly available authentication, authorization tools, and key management strategies to ensure appropriate industry standard security controls are in place for sensitive data both in transit to and at rest in Cloud.[98]

External connectivity to the Clearing Agencies' systems hosted by the CSP would be provided, as it is now, through dedicated private circuits or over encrypted tunnels through the Internet. These network links also would have additional security controls, including encryption during transmission and restrictions on network access to and from the Cloud. Additionally, the Clearing Agencies would use dedicated redundant private network connections between the Clearing Agencies data centers and the CSP infrastructure. The Clearing Agencies currently maintains two data centers and will do so in the near term to provide redundant, geographically diverse connectivity for market participants.

All network communications between the Clearing Agencies and the Cloud Infrastructure would rely on industry standard encryption for traffic while in transit. Data at rest would be safeguarded through pervasive encryption. The Clearing Agencies' Encryption Standards[99] describe requirements for implementation of the minimum required strengths, encryption at rest, and cryptographic algorithms approved for use in cryptographic technology deployments across the Clearing Agencies. All Clearing Agency identifying data is encrypted in transit using industry standard methods. The Key Management Service ("KMS") Strategy[100] dictates that all CSP endpoints support HTTPS for encrypting data in transit. The Clearing Agencies also secure connections to the endpoint service by using virtual private computer endpoints and ensures client applications are properly configured to ensure encapsulation between minimum and maximum Transport Layer Security versions pursuant to the Clearing Agencies' encryption standard.

The Clearing Agencies would have exclusive control over the encryption keys; only Clearing Agency authorized users and approved third parties would be able to access Clearing Agency data. The CSP systems and staff would not have access to the Clearing Agencies'

---

98 Supra note 47.

99 Supra note 91.

100 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Information Security – Public Key Infrastructure Policy and Control Standards, which governs the public key infrastructures implemented and used within DTCC and its subsidiaries. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

certificates or keys.[101] The Clearing Agencies would be responsible for the application architecture, software, configuration, and use of the CSP services, and for the maintenance of the environment, including ongoing monitoring of the application environment to achieve the appropriate security posture. To do this, the Clearing Agencies would follow (i) existing security design and controls; (ii) Cloud-specific information security controls defined in the Clearing Agencies' Information Security Policies and Control Standards;[102] and (iii) regulatory compliance requirements detailed in sources or information technology practices that are widely available and issued by an authoritative body that is a U.S. governmental entity or agency including NIST-CSF,[103] COBIT,[104] and the FFIEC Guidelines.[105]

The Clearing Agencies would use third-party and custom developed tools for CSP security compliance monitoring, security scanning, and reporting. Alerts and all API-level actions would be gathered using both CSP provided, Clearing Agency developed, and third-party monitoring tools. The CSP provided monitoring tool would be enabled by default at the organization level to monitor all CSP services activity. Centralized logging provides near real-time analysis of events and contains information about all aspects of user and role management, detection of unauthorized, security relevant configuration changes, and inbound and outbound communication.

As discussed just above, the Clearing Agencies would use a KMS Strategy to encrypt data in transit and at rest in the Cloud. KMS is designed so that no one, including CSP employees, can retrieve customer plaintext keys and use them. The Federal Information Processing Standards 140-2 validated Host Security Modules ("HSMs") in KMS protect the confidentiality and integrity of Clearing Agency customer keys.[106] Customer plaintext keys are not written to disk and are only used in protected, volatile memory of the HSMs for the time needed to perform the customer's requested cryptographic operation. KMS keys are not transmitted outside of Cloud regions in which they were created. Updates to the KMS HSM

---

101 Certificate management is the process of creating, monitoring, and handling digital keys (certificates) to encrypt communications.

102 Supra note 91.

103 NIST Cybersecurity Framework Version 1.1.

104 COBIT 2019 Framework: Governance and Management Objectives.

105 FFIEC Information Technology Examination Handbook – Information Security (September 2016).

106 The HSM is analogous to a safe to which only the Clearing Agencies have the combination and the ability to access the keys to locks stored within.

firmware will be controlled by quorum-based access control[107] that is audited and reviewed by an independent group within the CSP.

(3) Security Configuration, Provisioning, Logging, and Monitoring

Automated delivery of business and security capability via the use of "Infrastructure as Code" and continuous integration/continuous deployment pipeline methods would permit security controls to be consistently and transparently deployed on-demand. The Clearing Agencies would provision Cloud Infrastructure using pre-established system configurations that are deployed through Infrastructure as Code, then scanned for compliance to secure baseline configuration standards. The Clearing Agencies also would employ continuous configuration monitoring and periodic vulnerability scanning. The Clearing Agencies would perform regular reviews and testing of Clearing Agency systems running in Cloud while relying upon information provided by the CSP through the CSP's SOC2 and Audit Symposiums. Finally, configuration, security incident, and event monitoring would rely on a blend of CSP native and third-party solutions.

The Clearing Agencies also plan to use tools offered by the CSP, developed by the Clearing Agencies, and third parties to monitor the Core C&S Systems running in Cloud. The Clearing Agencies would track metrics, monitor log files, set alarms, and have the ability to act on changes to Core C&S Systems and the environment in which they operate. The CSP would provide a dashboard to reflect-general health (e.g., up/down status of a region and CSP provided services running in that region) but would not give additional insights into performance of services and applications which run on those services. The Clearing Agencies' centralized logging system would provide for a single frame of reference for log aggregation, access, and workflow management by ingesting the CSP's logs coming from native detective tools and the Clearing Agencies' instrumented controls for logging, monitoring, and vulnerability management. This instrumentation would give the Clearing Agencies a real-time view into the availability of Cloud services as well as the ability to track historical data. By using the enterprise monitoring tools that the Clearing Agencies have in place, the Clearing Agencies would be able to integrate the availability and capacity management of Cloud into the Clearing Agencies' existing processes, hosted in Cloud, to respond to issues in a timely manner.

The Clearing Agencies also would use specialized third-party tools, as discussed just above, to programmatically configure Cloud services and securely deploy infrastructure. This automation of configuration and deployment would help ensure that Cloud services are repeatably and consistently configured securely and validated. Change detection tools providing event logs into the incident management system also are vital for reacting to and investigating unexpected changes to the environment.

The Clearing Agencies would implement tools for the Core C&S Systems and back-office environments that would be hosted on the Cloud Infrastructure, notably, IAM, monitoring

---

[107] A quorum-based access mechanism requires multiple users to provide credentials over a fixed period in order to obtain access.

and Security Information and Event Management systems, the workflow system of record for incident handling, KMS, and enterprise Data Loss Prevention.

Finally, the CSP prioritizes assurance programs and certifications, underscoring its ability to comply with financial services regulations and standards and to provide the Clearing Agencies with a secure Cloud Infrastructure.[108]

(4) Security Testing and Verification

Security testing is integrated into business-as-usual processes as outlined in relevant policy and procedures.[109] These documents define how testing is initiated, executed, and tracked.

For new assets and application (or code) releases, Technology Risk Management determines whether and what type of security testing is required through a risk-based analysis.[110] If required, testing would be conducted prior to implementation. The different testing techniques are outlined below:

- Automated Security Testing. Using industry standard security testing tools and/or other security engineering techniques specifically configured for each test, the Clearing Agencies would test to identify vulnerabilities and deliver payloads with the intent to break, change, or gain access to unauthorized areas within an application, data, or system.

- Manual Penetration Testing. Using information gathered from automated testing and/or other information sources, the Clearing Agencies would manually test to identify vulnerabilities and deliver payloads with the intent to break, change, or gain access to the unauthorized area within an application or system.

- Blue Team Testing. The Blue Team identifies security threats and risks in the operating environment and analyzes the network, system, and SaaS environments and their current state of security readiness. Blue Team assessment results guide risk mitigation and remediation, validate the effectiveness of controls, and provide evidence to support authorization or approval decisions. Blue Team testing ensures that the Clearing Agencies' networks, systems, and SaaS solutions are as secure as possible before deploying to a production environment.

---

108 The CSP has certifications for the following frameworks: NIST, Cloud Security Alliance, COBIT, ISO, and FISMA.

109 Supra note 46.

110 Supra note 30.

The results of the Clearing Agencies' security controls testing are risk-rated and managed to remediation via two separate control standards.[111]

(c) Change Management: Software Development and Release Process

Consistent with FFIEC Guidance, the Clearing Agencies' use of Cloud would have sufficient change management controls in place to effectively transition systems and information assets to Cloud and would help ensure the security and reliability of applications in Cloud.[112] The Clearing Agencies' enterprise software development lifecycle processes[113] would help ensure the same control environment for all Clearing Agency resources. The Clearing Agencies would establish baselines for design inputs and control requirements and enforce workload isolation and segregation through Cloud using existing Cloud native technical controls and added new tools. The Clearing Agencies also would plan to use other specialized platform monitoring tools for logging, scanning of configuration, and systems process scanning. The Clearing Agencies also would have oversight as the code owner and would have final review and approval for related changes and code merges before deployment into production. Finally, the Clearing Agencies would periodically conduct static code scanning and perform vulnerability scanning for external dependencies prior to deployment in production, along with manual penetration testing of the provided application code. In addition, the Clearing Agencies would perform routine scans of Compute resources with the existing enterprise scanning tools. Any identified vulnerabilities would be reviewed for severity, prioritized, and logged for remediation tracking in upcoming development releases.

The Clearing Agencies would create a "user acceptance plan" prior to promoting code to Cloud production. This user acceptance plan would include tests of all major functions, processes, and interfacing systems, as well as security tests. Through acceptance tests, the Clearing Agencies' users would be able to simulate complete application functionality of the live environment. The change would move to the next stage of the Clearing Agencies' delivery model only after satisfying the criteria for this phase.[114]

The Clearing Agencies would have internal projects that would address change management of the various applications and services. In particular, the Clearing Agencies would run a suite of supporting services that enable building, running, scaling, and monitoring of the Clearing Agencies' business applications in Cloud, in an automated, resilient, and secure manner.[115] The application platform relies on various CSP and third-party tools for different

---

111 Supra notes 46-47.

112 Supra note 30.

113 Id.

114 The "user acceptance plan" represents only one aspect of the overall change management program at the Clearing Agencies.

115 Supra note 30.

components, including IaaS, Infrastructure as Code, CI/CD, Container as a Service, Continuous Delivery, and Platform Monitoring.

With respect to software development in Cloud, the Clearing Agencies would establish a closed, non-production Cloud environment that would enable the Clearing Agencies to develop, test, and integrate new capabilities, including those related to security capabilities. This non-production Cloud environment would focus on the foundational security, operations, and infrastructure requirements with the intent to take lessons learned to implement into future production. The Clearing Agencies would maintain a Cloud Reference Architecture that defines necessary capabilities and controls required to securely host Core C&S Systems. The minimum foundational security requirements would be based on the NIST-CSF and CIS benchmarks and include the design and implementation requirements of a secure Cloud account structure within a multi-region Cloud environment. The Clearing Agencies would maintain enterprise security requirements that provide structure for current and future development. As the Cloud environment is further developed and expanded, there would be a comprehensive process to identify any incremental risks and develop and implement controls to manage and mitigate those risks.

(d) Resilience and Recovery

As noted earlier, given the Clearing Agencies' roles as systemically important financial market utilities, it is vital that operations moved to the Cloud have appropriately robust resilience and recovery capabilities. As discussed in Section II.B.ii.2, above, the Cloud Infrastructure would be architected to include (i) two autonomous and geographically diverse regions; (ii) three availability zones per region, with each availability zone comprised of multiple data centers; (iii) multi-node, high availability clusters across each availability zone; (iv) static stability and static capacity models; and (v) regional isolation, all to help ensure the persistent availability of Compute, Storage, and Network capabilities in Cloud.

Additionally, the CSP's practice in deploying service updates to Cloud would help ensure that the consequences of any incidents would be limited to the fullest extent possible.[116] The CSP achieves this by (i) fully automating the build and deployment process and (ii) deploying services to production in a phased manner.

CSP service updates are first deployed to cells, which minimizes the chance that a disruption from a service update in one cell would disrupt other cells. Following a successful cell-based deployment, service updates are next deployed to a specific availability zone, which limits any potential disruption to that zone. Following a successful availability zone deployment, service updates are then deployed in a staged manner to other availability zones, starting with the same region and later within other regions until the process is complete.

---

116 The Clearing Agencies would continue to retain responsibility for patching, configuration, and monitoring of the operating systems and applications in Cloud.

The Clearing Agencies would meet regularly with the CSP, in addition to formal quarterly briefing meetings with the CSP, as described in the Reg. SCI Addendum.[117] The informal discussions and quarterly briefing meetings would permit the Clearing Agencies to gather information in advance of the quarterly systems change report. Most reportable systems changes would continue to occur based on changes to Compute, Storage, Network, or applications controlled by the Clearing Agencies.

(e) Audit Controls and Assessment

The Clearing Agencies would regularly test security controls and configurations, including by monitoring the CSP's technical, administrative, and physical security controls that support the Clearing Agencies' systems in the Cloud Infrastructure.

(1) Internal Risk Assessments

As part of their existing third-party vendor risk activities, the Clearing Agencies' Third-Party Risk department ("TPR") would assess the operational risks of the CSP as a critical vendor annually.[118] [119] [120] Additionally, as a critical vendor, the CSP is subject to heightened risk management requirements, as defined in the DTCC Third Party Risk CriticalPlus Program

---

117 See Reg. SCI Addendum, Section 4 *Briefing Meetings*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

118 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Third Party Risk Governance & Monitoring Procedures, which describes the minimum requirements for practices and standards to be used by business owners to monitor and manage third party relationships for DTCC and its subsidiaries. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

119 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Third Party Risk Policy and the DTCC Third Party Risk Procedures, which establish the standards and practices to be used by certain business line departments and/or functional units to manage the potential risks associated with engaging with an external service provider. The Clearing Agencies have provided these documents in confidential Exhibit 3 to this advance notice filing.

120 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the Third Party Risk – Technology and Resilience Procedure, which supplements the "DTCC Third Party Risk Policy", "DTCC Third Party Risk Procedures", and "DTCC Third Party Risk Governance and Monitoring Procedures" and covers the following: standard technology risk assessments (e.g., due diligence), fourth party reviews, NYDFS cyber security assessments, and onsite assessments. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

Procedures,[121] which include an executive sponsor that must be at the Managing Director level or higher, documented annual meetings, quarterly reporting, and monthly notifications. Issues rated moderate or above, negative news, performance concerns or remediations are directly escalated to the Management Risk Committee monthly.[122]

(2) Internal Audit Department

As mentioned in Section II.B.ii.4.(a), above, the Clearing Agencies' IAD, as the third line of defense, is independent from the Clearing Agencies' business lines, support areas, and controls functions, and promotes resiliency and security through the assessment of risk management and control frameworks to raise awareness of control risks and changes for improving controls and governance processes.

IAD assesses the risks of the Clearing Agencies, at least annually, as part of the development of the risk-based audit plan, which is reviewed and refreshed, as needed, on a quarterly basis.[123] The development of the audit plan includes the consideration of IADs risk assessment results, which informs cycle coverage requirements for Cloud. Additional considerations include, but are not limited to, regulatory requirements and expectations, initiatives, and institutional and industry risk trends, including risks associated with technology and cloud-based processes.

IAD's specific reviews of Cloud Infrastructure have not identified any material deficiencies and the scope of the reviews have included, but are not limited to, consideration of governance and oversight, contagion risk and logical separation, access management, security configuration and monitoring, concentration risk, exit strategy, business continuity and disaster recovery. IAD also has assessed the design of controls for a cloud platform scheduled for use in 2024 and is proposing a Cloud Security audit for 2024.[124]

---

121 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Third Party Risk CriticalPlus Program Procedures. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

122 Supra note 62.

123 Supra note 81.

124 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the Clearing Agencies' Cloud Platform Internal Audit Report. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

(3) Key Risk and Key Performance Indicators[125]

The Clearing Agencies have established processes to evaluate the Clearing Agencies' management of CSPs. Cloud vendors are rated through a quarterly TPR survey. If a survey results in a poor rating, then it is reported to the Management Risk Committee ("MRC").[126] TPR is responsible for the timely reporting and escalation of third-party risks. On a regular basis, TPR will review all active assessments to identify any high risks or potential issues that may require further discussion or escalation to senior management, Corporate Procurement Services ("CPS"), or internal stakeholders. The DTCC Third Party Risk Procedures provide a list of events that must be presented to the MRC.[127]

The Clearing Agencies have developed key performance indicators ("KPIs") for Cloud and socialized these KPIs internally. The KRIs already exist for Core C&S Systems and are aligned to overall systems availability, capacity, data integrity, and security.[128] The CSP KPIs would feed into existing KRIs and would be used to evaluate the CSP's performance after Cloud implementation. KPIs would be added to monitor the performance and risks of the CSP services for which the Clearing Agencies have contracted. These post-Cloud implementation KRIs and KPIs would allow the Clearing Agencies to assess their ongoing use of the CSP against their operational and security requirements and would help demonstrate the effectiveness of risk controls and the CSP's performance against commitments in the SLAs, and will be reported on a regular basis to the Clearing Agencies' Management Committee, Board of Directors, and Technology and Risk Committees of the Board of Directors.

(4) Auditing the CSP and Access Rights[129]

The CSP hosts an annual Audit Symposium. The Cloud Agreement gives the Clearing Agencies the right to attend the symposium so that the Clearing Agencies may inspect and verify evidence of the design and effectiveness of the CSP's control environment.[130] The CSP also hosts an annual Cloud security conference focused on security, governance, risk and compliance, which the Clearing Agencies would attend. Through preparation for and attendance at these

---

125 Supra note 62.

126 Supra note 119.

127 Supra note 78.

128 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the IT-Q4 2023 Risk Tolerance. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

129 Supra note 62.

130 See Reg. SCI Addendum, Section 3 *Customer Right of Access and Audit*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

events, the Clearing Agencies could provide feedback and make requests of the CSP for future modifications of its control environment.

The Clearing Agencies' Information Technology staff currently meets with CSP representatives weekly to focus on technical issues related to the Clearing Agencies' proposed Cloud environment. As required under the Cloud Agreement, the Clearing Agencies hold quarterly compliance briefings with the CSP, wherein the Clearing Agencies receive information, including any necessary documentation, from the CSP to help assure the Clearing Agencies that the CSP is meeting its obligations.[131] The information provided includes updates to services and SLAs, CSP performance, and details that help the Clearing Agencies meet their reporting obligations under Section 1003(a)(1) of Reg. SCI. The Clearing Agencies' management, including Security, Information Technology, TPR, and the Internal Audit Department, coordinate to ensure appropriate representation during such briefings. The CSP is required under Cloud Agreement to maintain records showing its compliance with the agreements for a period of five years.[132]

The CSP would be required to maintain an information security program, including controls and certifications, that is as protective as the program evidenced by the CSP's SOC-2 report. The CSP must make available on demand to the Clearing Agencies its SOC-2 report as well as the CSP's other certifications from accreditation bodies and information on its alignment with various frameworks, including NIST-CSF, and ISO.[133]

As part of the annual risk assessment of the CSP, TPR collects risk and control related assurance documents from the CSP and coordinates review with the Clearing Agencies' respective subject matters specialists. TPR, Security, and Business Continuity would determine the adequacy and reasonableness of the documentation received to complete the Third-Party Risk Assessment. Finally, the Cloud Agreement provides that the Clearing Agencies' and their

---

131 Supra note 117.

132 See Reg. SCI Addendum, Section 7.3 *CSP Records*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

133 The FFIEC Guidance provides that the Clearing Agencies may obtain SOC reports, other independent audits, or ISO certification reports to gain assurance that the CSP's controls are operating effectively. See FFIEC, Security in a Cloud Computing Environment, at 7. The Clearing Agencies review the CSP's SOC-2 on an annual basis. See Reg. SCI Addendum, Section 2 *CSP Information Security Program*. The SOC reports, along with other artifacts showing compliance with these sections, are available to the Clearing Agencies on demand. In addition, during each Briefing Meeting (See Reg. SCI Addendum Section 4 *Briefing Meetings*), updates are provided on any material changes to certification standards, policies, procedures, controls or security standards at the CSP. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

regulators may visit the facilities of the CSP under specified conditions. TPR would help coordinate bi-annual visits of the data centers.[134]

The Clearing Agencies plan to use the CSP's services combined with additional third-party tools to monitor systems deployed by ingesting logs into a security incident and event monitoring tool to provide a "single pane of glass" view into the Cloud Infrastructure. When incidents are detected, the Clearing Agencies would follow their existing incident response governance to identify, detect, contain, eradicate, and recover from incidents.

III. Consistency with the Clearing Supervision Act

The stated purpose of the Clearing Supervision Act is to mitigate systemic risk in the financial system and promote financial stability by, among other things, promoting uniform risk management standards for systemically important financial market utilities and strengthening the liquidity of systemically important financial market utilities.[135] Section 805(a)(2) of the Clearing Supervision Act[136] also authorizes the Commission to prescribe risk management standards for the payment, clearing and settlement activities of designated clearing entities, like the Clearing Agencies, for which the Commission is the supervisory agency. Section 805(b) of the Clearing Supervision Act[137] states that the objectives and principles for risk management standards prescribed under Section 805(a) shall be to:

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

The Commission adopted Rule 17ad-22 under Section 805(a)(2) of the Clearing Supervision Act and the Exchange Act in furtherance of these objectives and principles.[138] Rule 17ad-22 under the Exchange requires covered clearing agencies, like the Clearing Agencies, to

---

134 See Reg. SCI Addendum, Sections 3 *Customer Right of Access and Audit* and 9 *Regulatory Supervision*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

135 12 U.S.C. 5461(b).

136 12 U.S.C. 5464(a)(2).

137 12 U.S.C. 5464(b).

138 17 CFR 240.17ad-22. Exchange Act Release Nos. 68080 (October 22, 2012), 77 FR 66220 (November 2, 2012) (S7-08-11) (Clearing Agency Standards); 78961 (September 28, 2016), 81 FR 70786 (October 13, 2016) (S7-03-14) (Standards for Covered Clearing Agencies).

establish, implement, maintain, and enforce written policies and procedures that are reasonably designed to meet certain minimum requirements for their operations and risk management practices on an ongoing basis.[139]

The Clearing Agencies believe that the Cloud Proposal is consistent with Section 805(b)(1) of the Clearing Supervision Act[140] and the requirements of Rules 17ad-22(e)(17)(ii) under the Exchange Act.[141]

A. Consistency with Section 805(b)(1) of the Clearing Supervision Act

Promote Robust Risk Management. As described above, the Clearing Agencies believe that the Cloud Proposal promotes robust risk management, specifically operational risk management, by providing scalable and secure infrastructure for hosting Core C&S Systems. The Cloud Proposal would add additional security capabilities, allow for regular updates and maintenance of applications, and reduce the risk of data breaches while also ensuring compliance with industry standards. Additionally, transitioning to Cloud would offer flexibility in scaling resources, which can enable the Clearing Agencies to adapt quickly to changing security needs and allocate resources more efficiently.

Today, the Clearing Agencies' ability to risk manage extreme market events is directly tied to their ability to scale their on-premises resource during such events, which is directly tied to the Clearing Agencies having previously expended enough capital to build enough capacity based on earlier performance testing of their applications to withstand such extreme market events. Although the Clearing Agencies would continue to performance test their applications regardless of where the applications are hosted, by hosting the applications in Cloud, the number of scalable resources is already available, when needed, without the Clearing Agencies having to pre-purchase it or build it. This level of nearly unbounded, on-demand scalability provides a much-welcomed risk-management feature for extreme events, such as a global pandemic as noted above.

Overall, risk management is inherently strengthened by hosting in Cloud through advanced security features, real-time monitoring, on-demand scalability, and compliance standards implemented by the CSP. By leveraging these capabilities, the Clearing Agencies can better proactively identify and address risks, ensuring data integrity and regulatory compliance.

Promote Safety and Soundness. The Clearing Agencies also believe that the Cloud Proposal promotes safety and soundness. As discussed above, transitioning to Cloud provides centralized management and improved scalability. The CSP provides cloud-specific security capabilities, including encryption, access controls, and regular updates, reducing the risk of security breaches. Centralized monitoring allows for better visibility into potential threats, enabling quick response and mitigation. The agility afforded by Cloud would allow the Clearing

---

139 17 CFR 240.17ad-22.

140 12 U.S.C. 5464(b)(1).

141 17 CFR 240.17ad-22(e)(17)(ii).

Agencies to respond to performance challenges more efficiently and effectively. For instance, as noted above, in the face of unexpected surges in demand, Cloud scalability would allow the Clearing Agencies to seamlessly adjust resources, helping to prevent service disruptions and loss of operations. Such agility not only enhances the effectiveness of operations but also mitigates the risks associated with unexpected fluctuations in workload performance. These benefits improve the Clearing Agencies abilities to maintain operational continuity and resilience, which help promote safety and soundness.

Reduce Systemic Risk. The Clearing Agencies also believe that the Cloud Proposal would reduce systemic risk by improving overall resilience and security. As described above, hosting Core C&S Systems in Cloud would provide distributed infrastructure and data redundancy (i.e., multiple availability zones, supported by many data centers, across two regions), making the systems less susceptible to single points of failure. Moreover, disaster recovery would be streamlined, minimizing the effect of potential disruptions, while automatic backup systems, geographic redundancy, and faster data recovery mechanisms would all contribute to a more resilient infrastructure. In the event of a localized issue, the distributed nature of Cloud would help prevent widespread disruptions.

Production resiliency also is greatly improved in Cloud compared to the Clearing Agencies' on-premises capabilities, where a single location hosts an application, on a single copy of primary storage. Instead, Cloud would host an application across three primary availability zones, made of up of many data centers, each of which contain actively running instances and synchronous copies of the data. If the Clearing Agencies' primary, on-premises data center fails, an out of region recovery will be necessary and will likely result in approximately two hours of downtime. By comparison, in Cloud, even if an entire availability zone fails (meaning the failure of multiple data centers), Core C&S Systems would continue to operate within the region, thus avoiding an out of region recovery and any downtime.

The Clearing Agencies would employ meaningful security capabilities and measures provided by the CSP and third-party tools to further enhance the security of the Clearing Agencies' Core C&S Systems. This approach to security would help reduce systemic risks associated with operational outages and significantly reduce the risk associated with data loss or downtime. Additionally, the Cloud environment facilitates regular updates and patch management, ensuring that security measures stay current. This proactive maintenance helps mitigate vulnerabilities that could otherwise contribute to systemic risk. Overall, the adoption of Cloud enhances the stability and security of IT infrastructure, contributing to a reduction in systemic risks.

Altogether, the Clearing Agencies believe that the benefits afford from operating in a Cloud Infrastructure would help the Clearing Agencies reduce systemic risk.

Support the Stability of the Broader Financial System. The Clearing Agencies believe that the Cloud Proposal supports the stability of the broader financial system by enhancing efficiency, resilience, and security of the Clearing Agencies' Core C&S Systems. Cloud services would provide the Clearing Agencies with scalable and flexible infrastructure, allowing for more efficient resource allocation and cost management, which supports operational resiliency and

stability. With the ability to rapidly deploy new applications and services, the Clearing Agencies would become more agile in adapting to market trends and participant and customer needs.

In terms of resilience, the Cloud Infrastructure offers distributed data storage and failover solutions, reducing the impact of localized disruptions and improving recovery capabilities. This resilience is crucial for the Clearing Agencies' Core C&S Systems to continue functioning even in the face of unforeseen events. Moreover, the CSP's strengthened security capabilities help protect sensitive data, mitigating the risk of cyberattack or data breaches that could undermine the stability of the financial system. Overall, the transition to Cloud fosters improved operational efficiency, resilience, and robust security practices, contributing to the stability of the broader financial system.

Accordingly, the proposed changes provided in this Cloud Proposal are consistent with (i) promoting robust risk management; (ii) promoting safety and soundness; (iii) reducing systemic risks; and (iv) promoting the stability of the broader financial system, all in support of the objectives and principles of Section 805(b) of the Clearing Supervision Act.[142]

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

Rule 17ad-22(e)(17)(ii) requires the Clearing Agencies to establish, implement, maintain, and enforce written policies and procedures reasonably designed to manage the Clearing Agencies' operational risk by "ensuring that systems have a high degree of security, resiliency, operational reliability, and adequate, scalable capacity."[143]

Security. As described above and in policies and procedures confidentially filed, the Clearing Agencies have established a robust Cloud security program to manage the security of the Core C&S Systems that would be running in Cloud and to monitor the CSP's management of security of the Cloud Infrastructure that it operates. Processes are formally defined, automated to the fullest extent, repeatable with minimal variation, accessible, adhered to, and timely. The enterprise security program encompasses all of the Clearing Agencies' assets existing in the Clearing Agencies' offices, data centers, and within the Cloud Infrastructure, and IAM controls ensure least-privileged user access to applications in Cloud. The Clearing Agencies have appropriate controls in place to help ensure the security of confidential information in-transit between the Clearing Agencies' data centers and the Cloud Infrastructure, between systems within the Cloud Infrastructure, and at-rest. All network communications between the Clearing Agencies and Cloud would rely on industry standard encryption for traffic while in transit, and data at rest would be safeguarded through pervasive encryption. Finally, automated delivery of business and security capability via the use of the Infrastructure as Code, Cloud agnostic tools,

---

142 12 U.S.C. 5464(b).

143 17 CFR 240.17ad-22(e)(17)(ii). The Clearing Agencies maintain several policies specifically designed to manage the risks associated with maintaining adequate levels of system functionality, confidentiality, integrity, availability, capacity, and resiliency for systems that support core clearing, risk management, and data management services.

and continuous integration/continuous deployment pipeline methods help ensure security controls are consistently and transparently deployed.

Resiliency and Operational Reliability. As stated above, resiliency and operational reliability of the Cloud Infrastructure is built into the system with functionality for the Clearing Agencies' Core C&S Systems to run in multiple availability zones within multiple regions. Regions are segregated from one another and are designed to minimize the possibility of a multi-region outage. The Clearing Agencies have designed their Cloud Infrastructure to have primary (hot)/secondary (warm) regions, at all times, ensuring Compute, Storage, and Network resources would be available in a new redundant region in the event of a primary region failure. As a result, the Cloud Infrastructure offers the Clearing Agencies multiple redundancies within which to run Core C&S Systems, while simultaneously restricting the effect of an incident at the CSP to the smallest footprint possible.

Scalability. As described above, since additional computing power can be launched on demand, the scalability in a Cloud computing environment is considerable and instantaneous. The Clearing Agencies could provision or de-provision Compute, Storage, and Network resources to meet demand at any given point in time. In the current on-premises environment, immediate scalability is limited by the capacity of the on-premises hardware. Additional physical servers and network equipment would be needed to scale beyond the limits of the on-premises hardware, potentially affecting the ability to quickly adapt to evolving market conditions, including spikes in trading volume.

For these reasons, the Clearing Agencies believe that the Cloud Proposal would help ensure that the Clearing Agencies' systems have a high degree of security, resiliency, operational reliability, and adequate, scalable capacity, consistent with Rule 17ad-22(e)(17)(ii) under the Exchange Act.[144]

11. Exhibits

Exhibit 1 – Not applicable.

Exhibit 1A – Notice of advance notice for publication in the Federal Register.

Exhibit 2 – Not applicable.

Exhibit 3 – Confidential Supporting Information. ***Omitted and filed separately with the Commission. Confidential treatment of this Exhibit 3 being requested pursuant to 17 CFR 240.24b-2.***

Exhibit 4 – Not applicable.

Exhibit 5 – Not applicable.

---

144 17 CFR 240.17ad-22(e)(17)(ii).

EXHIBIT 1A

SECURITIES AND EXCHANGE COMMISSION
(Release No. 34-[_____]; File No. SR-DTC-2024-801)

[DATE]

Self-Regulatory Organizations; The Depository Trust Company; Notice of Filing of Advance Notice to Host Certain Core Clearance and Settlement Systems in a Public Cloud

Pursuant to Section 806(e)(1) of Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act entitled the Payment, Clearing, and Settlement Supervision Act of 2010 ("Clearing Supervision Act")[1] and Rule 19b-4(n)(1)(i) under the Securities Exchange Act of 1934 ("Act"),[2] notice is hereby given that on August __, 2024, The Depository Trust Company ("DTC") filed with the Securities and Exchange Commission ("Commission") the advance notice as described in Items I, II and III below, which Items have been prepared by the clearing agency. The Commission is publishing this notice to solicit comments on the advance notice from interested persons.

I. Clearing Agency's Statement of the Terms of Substance of the Advance Notice

DTC files this advance notice seeking no objection to host a specified set of core clearance, settlement, and risk applications, including any Regulation Systems Compliance and Integrity ("Reg. SCI") systems and Critical SCI systems,[3] ("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

---

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

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

3 17 CFR 242.1000 et seq.

single, third-party service provider ("Cloud Service Provider" or "CSP") (altogether, the "Cloud Proposal"), as described in greater detail below.

II. Clearing Agency's Statement of the Purpose of, and Statutory Basis for, the Advance Notice

In its filing with the Commission, the clearing agency included statements concerning the purpose of and basis for the advance notice and discussed any comments it received on the advance notice. The text of these statements may be examined at the places specified in Item IV below. The clearing agency has prepared summaries, set forth in sections A and B below, of the most significant aspects of such statements.

(A) Clearing Agency's Statement on Comments on the Advance Notice Received from Members, Participants, or Others

DTC has not received or solicited any written comments relating to this proposal. If any written comments are received, DTC will amend this filing to publicly file such comments as an Exhibit 2 to this filing, as required by Form 19b-4 and the General Instructions thereto.

Persons submitting written comments are cautioned that, according to Section IV (Solicitation of Comments) of the Exhibit 1A in the General Instructions to Form 19b-4, the Securities and Exchange Commission ("Commission") does not edit personal identifying information from comment submissions. Commenters should submit only information that they wish to make available publicly, including their name, email address, and any other identifying information.

All prospective commenters should follow the Commission's instructions on How to Submit Comments, available at www.sec.gov/regulatory-actions/how-to-submitcomments. General questions regarding the rule filing process or logistical

questions regarding this filing should be directed to the Main Office of the Commission's Division of Trading and Markets at tradingandmarkets@sec.gov or 202-551-5777.

DTC reserves the right to not respond to any comments received.

(B) Advance Notice Filed Pursuant to Section 806(e) of the Clearing Supervision Act

I. Description of the Proposal

Pursuant to the Clearing Supervision Act and Rule 19b-4(n)(1)(i) under the Exchange Act,[4] DTC files this advance notice seeking no objection to the Cloud Proposal, as described herein.

The specified set of Core C&S Systems that the Clearing Agencies intend to host in the Cloud, and the transition schedule for such hosting, are listed in Exhibit 3 to this advance notice filing.[5] However, the Clearing Agencies recognize that it may become necessary to deviate from the proposed transition schedule as risks change over time and the proposed implementation would occur over several years. The Clearing Agencies' process for monitoring, assessing, and escalating such risks, which may result in a deviation, is described in Section I.D, below. If the Clearing Agencies would need to deviate from that schedule, they would provide Commission staff notice of such deviation, the reason for the deviation, and how the implementation schedule would be updated to account for the deviation. Further, the Clearing Agencies recognize that deviating from the proposed transition schedule would necessitate a separate analysis to

---

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

5 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the proposed transition schedule (i.e., the Core C&S Systems to Move to Cloud). The Clearing Agencies have provided this schedule in confidential Exhibit 3 to this advance notice filing.

determine whether such deviation could materially affect the nature or level of risk posed by each of the Clearing Agencies.

DTC's two affiliate clearing agencies, Fixed Income Clearing Corporation ("FICC") and National Securities Clearing Corporation ("NSCC" and together with DTC and FICC, the "Clearing Agencies")[6] have each filed with the Commission advance notices to adopt the same Cloud Proposal. Accordingly, each respective advance notice filing is written from the perspective of the Clearing Agencies, collectively, instead of DTC, FICC, and NSCC individually.[7]

A. The Current System and Summary of Proposed Change

Today, the Clearing Agencies' Core C&S Systems are hosted using Compute,[8] Storage and Networking, as defined below, running in private data centers (i.e., on-premises). The current data-center footprint consists of a single data center in each of two regions. Each regional data center has a corresponding data bunker used for synchronous data protection and restoration.[9]

---

6 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.

7 Capitalized terms not otherwise defined herein have the meaning as set forth in respective rules of the Clearing Agencies, available at https://www.dtcc.com/legal/rules-and-procedures.

8 The existing Compute platform consists of both on-premises mainframe and private cloud platforms.

9 Note: The data bunkers cannot run applications, as they are only for data protection and restoration.

The Clearing Agencies view the proposed transition to using a Cloud Infrastructure to host the specified set of Core C&S Systems as a natural progression of the Clearing Agencies' information technology strategy that aligns with their overall corporate strategy – to deliver on modernization and maximize the value of their platforms for stakeholders and continue to invest in risk management excellence.

For over 11 years, the Clearing Agencies have honed their expertise in operating non-Core C&S Systems within the Cloud.[10] Throughout that time, the Clearing Agencies have continually refined their capabilities across technical, risk, legal, and compliance dimensions, in tandem with the Cloud's own evolution and the industry's increasing adoption of it. Given this extensive maturity and development over the past decade, the Clearing Agencies believe that hosting Core C&S Systems in the Cloud, via a single CSP, is now appropriate and essential. By consolidating resources under a single CSP, the Clearing Agencies can optimize efficiency, reduce costs, mitigate risks, and maintain a cohesive environment for seamless collaboration and operation.

As described in greater detail in this advance notice, the Clearing Agencies propose to provision, within a single CSP, logically segregated sections of the Cloud Infrastructure that would provide the Clearing Agencies with the virtual equivalent of

---

10 Some of the non-Core C&S Systems already operating in Cloud include systems that support risk analysis, various reporting engines, and shared infrastructure capabilities. More specifically, for risk analysis, there are applications for certain risk testing and calculations used to assess industry risk postures for various Clearing Agency clients, as well as warehousing large sets of risk data for quantitative analytics. For the various report engines, there are applications that provide publicly disseminatable data sets and documentation, certificate imaging, as well as certain archival storage capabilities. For shared infrastructure capabilities, there are applications that support the Clearing Agencies' engineering and development departments for dev-op capabilities such as code scanning, code repositories, and infrastructure-as-code deployment pipelines.

physical data center resources, including scalable resources that can (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"). These resources would be logically segregated from other customers of the CSP. The Clearing Agencies would leverage the CSP's IaaS (i.e., infrastructure as a service) and PaaS (i.e., platform as a service) services for building and running Core C&S Systems.

The Clearing Agencies do not propose to transition all Core C&S Systems entirely out of their regional data centers at this time, but rather, to host a specified set of Core C&S Systems in a Cloud Infrastructure while maintaining the remaining applications in the Clearing Agencies' regional data centers for the near term. The proposed transition would be achieved incrementally over a course of several years and would result in the Clearing Agencies hosting some Core C&S Systems on-premises and others in a Cloud Infrastructure.[11]

This phased approach to transitioning to Cloud is to reduce risk. The Clearing Agencies believe that a "big-bang" approach of moving all applications at once introduces significant execution risk, primarily driven by the sheer scale and scope of such an effort. Moreover, many clearance and settlement applications on the Clearing Agencies' mainframe are still tightly coupled together. Even after such applications are modernized, many could experience latency dependencies with other applications that have not yet been modernized, hence the need to keep some applications in the Clearing

---

[11] A result of the Cloud Proposal would be that the Clearing Agencies would operate Reg. SCI and Critical SCI systems both on-premises and on a Cloud Infrastructure.

Agencies' existing data centers for the near term. However, applications with little to no coupling, particularly those applications that have already been modernized, are ripe for Cloud transition and the subject of this Cloud Proposal. As for the remaining clearance and settlement applications that are not part of this proposal and would continue to be hosted on-premises, the Clearing Agencies have not thoroughly assessed when those applications would transition to Cloud, which may take several years, or whether such transition would be the subject of a later, separate advance notice proposal.

Integration between on-premises and Cloud-based Core C&S Systems would, as it is for non-Core C&S Systems that are already hosted in private and public cloud, leverage existing patterns and processes. The primary methods of application integration are application program interfaces (a/k/a APIs), messaging queues (a/k/a MQ messaging), and file transfer. All three are used to integrate internal and client applications, and all three methods provide interoperability between applications running on mainframe, private cloud, and public cloud.

For these reasons, the Clearing Agencies strongly believe that the phased approach enables the Clearing Agencies to best approach the transition to Cloud, safely and confidently.

B. Why Use Cloud

The Clearing Agencies believe there are very strong and compelling reasons to use Cloud as part of their diverse, platform strategy, including, as discussed below, the waning of the on-premises industry, improved resilience, expanded security capabilities, and increased scalability.

1. Waning On-premises Industry

Although on-premises mainframes have been a stalwart for hosting critical applications for many years, it is the Clearing Agencies' experience that industry investment and development in on-premises platforms is waning, and the ability to source skilled and experienced staff to operate such platforms is increasingly challenging. Meanwhile, vendor consolidations are beginning to negatively affect investment and innovation in the private cloud space.[12] As investment dollars are increasingly allocated to Cloud, vendor choice, innovation, and support will continue to diminish for on-premises platforms. This poses a growing risk to the Clearing Agencies, who today continue to rely primarily upon on-premises mainframes and private cloud solutions from a resiliency perspective.[13] The Clearing Agencies believe the best way to manage against this risk at this time is to leverage a diverse platform strategy that will increase the use of and reliance upon Cloud. The use of Cloud, as part of a broader platform strategy, serves as an important tool in enabling the Clearing Agencies to anticipate and manage these and other risks more effectively.

---

12 For example, the VBlock platform, which has been the core, private cloud distributed hosting platform of the Clearing Agencies for over a decade, is no longer available for purchase. Another example is the continued consolidation in the private cloud software space, which has concentrated the industry and reduce aggregate investment in innovation.

13 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).

2. Improved Resilience

The Clearing Agencies must ensure that any Core C&S Systems in the Cloud have resiliency and recovery capabilities commensurate with the Clearing Agencies' importance to the functioning of the U.S. financial markets. As explained in detail below, the Clearing Agencies believe that Cloud will enhance the resiliency of their Core C&S Systems by virtue of the Clearing Agencies' architectural design decisions, and the Cloud's redundancy, availability, and the Clearing Agencies' disciplined approach to deployment of Core C&S Systems to Cloud. In particular, the Clearing Agencies believe that Cloud will enhance their ability to withstand and recover from adverse conditions by provisioning redundant Compute, Storage, and Network resources in three availability zones, in each of two autonomous and geographically diverse regions, for a total of six availability zones that are comprised of many data centers.

The primary/hot region would be operational and accepting traffic, while the secondary/warm region would receive replicated data from the hot region with applications on stand-by. This solution significantly reduces operational complexity, mitigates the risk of human error by providing tools for automating routine tasks and orchestrating complex workflows, thereby reducing the need for manual intervention,[14] and provides resiliency and assured capacity (although, the Clearing Agencies would continue to periodically review the CSP's capacity planning process through quarterly reviews).[15]

---

14 The CSP's built-in security features in its Cloud Infrastructure also can reduce the risk of security breaches caused by human error, such as misconfigurations or improper access controls.

15 The Clearing Agencies would continue to perform periodic business continuity and disaster recovery tests to verify business continuity plans and disaster

The Clearing Agencies are assured of adequate capacity with the proposed hot/warm architecture because the Compute resources of the warm, "recovery" region would be already running with needed capacity. Additionally, the Clearing Agencies have reviewed the effect of a large, regional outage with the CSP, which indicated that a vast majority of the CSP's customers are not configured to use the secondary region as a failover region; thus, they would not be using capacity in that region. Moreover, a review of data from two large outages in the primary region did not show a change in capacity availability in the secondary region.

The Clearing Agencies also believe that Cloud reduces capacity-management risks when compared with on-premises platforms in three important ways: (1) capacity in Cloud can be added almost instantly; (2) such capacity can be added at magnitudes greater than what is possible with traditional, on-premises platforms; and (3) the risk of a supply chain effect on capacity realization (i.e., the risks associated with receiving and deploying servers necessary to create more capacity) is greatly reduced.

The proposed hot/warm configuration also enables application rotation between regions. The Clearing Agencies would have the ability to operationally rotate either a single application, groups of applications, or all applications to the warm region for both planned and unplanned events. Collectively, the proposed design of the Cloud Infrastructure helps ensure that the Clearing Agencies can meet any applicable two-hour recovery time objective.

---

recovery infrastructure will support a two-hour recovery time objective for critical systems.

Each availability zone, in each of the two regions, would be comprised of multiple physical data centers. Each data center would have its own distinct physical infrastructure with separate staff and dedicated connections to utility power, standalone backup power sources, independent mechanical services, and independent network connectivity.

Although not dependent on each other, availability zones of a region are connected to each other with private, fiber-optic networking, enabling Core C&S Systems to automatically failover between a region's availability zones without interruption. Since each availability zone can operate independently, but failover capability is nearly instantaneous, a loss of one availability zone would not affect operation in another; therefore, no Core C&S System would be reliant on the functioning of a single availability zone.[16]

Altogether, the proposed Cloud Infrastructure would afford the Clearing Agencies six levels of redundancy (i.e., three availability zones, made up of many data centers, in each of the two regions), with primary/secondary regions running in a hot/warm configuration, respectively, in geographically separate and segregated locations, and with each region containing multiple copies of the data. Thus, even if an availability zone is lost in the primary region, the Cloud can continue to seamlessly operate Core C&S

---

16 To further ensure the resiliency of the Compute, Storage, and Network capabilities, the CSP's services are divided into "data plane" and "control plane" services. The Clearing Agencies' applications would run using data plane services, while control plane services are used to configure the environment. Resources and requests are further partitioned into cells, or multiple instantiations of a service that are segregated from each other and invisible to the CSP's customers, on each plane, again minimizing the effect of a potential incident to the smallest footprint possible.

Systems in the primary region, thereby significantly reducing availability risk and any attendant consequences for the Clearing Agencies' participants and customers. As a result, the Cloud Infrastructure offers the Clearing Agencies multiple redundancies within which to run Core C&S Systems, limits the effect of an incident at the CSP to the smallest footprint possible, and mitigates the possibility of the Clearing Agencies suffering an intra-, inter-, or multi-region outage.

By comparison, the Clearing Agencies' current on-premises hosting capabilities, both mainframe and private cloud, are operating on one primary data center in one region, with a second, recovery data center in a second region (excluding data bunkers, which do not have Compute capabilities). In other words, it is many times less likely that an unplanned, out of region failover would be needed for Core C&S Systems hosted in Cloud than currently hosted on-premises. (Even in the unlikely event that the Clearing Agencies needed to fail over to the secondary Cloud region, the decision and process of doing so would continue to be in the sole discretion of the Clearing Agencies.) This increased redundancy represents a material improvement in resiliency for the Clearing Agencies and a material reduction in risk for the industry.

Additionally, transitioning to Cloud offers the Clearing Agencies a more effective strategy for avoiding technical debt and system degradation because the CSP, in its role as such, would be performing regular system upgrades and maintenance, helping to ensure the Cloud's resiliency. Unlike on-premises solutions that may struggle to keep pace with evolving technology, due in part to the waning demand for on-premises infrastructure, CSPs take on the responsibility of regularly updating and maintaining their cloud infrastructure, which they do in a competitive environment. This approach helps

ensure that the CSP's cloud infrastructure remains up to date, secure, and performs at its best, minimizing the likelihood of accumulating technical debt and preventing the decline of system capabilities and resiliency over time. This is not to say that on-premises infrastructures are not updated or maintained today but, instead, that the CSP does it better and faster. CSPs excel in ensuring that systems remain up to date, secure, and perform at their best by leveraging automation, scalability, built-in security measures, service level agreements ("SLAs"), economies of scale, and continuous monitoring and improvement processes. These advantages collectively enable CSPs to provide more reliable, resilient, and high-performance services compared to traditional on-premises environments.

3. Expanded Security Capabilities

Hosting Core C&S Systems in Cloud would not change the physical and cybersecurity standards to which the Clearing Agencies currently align – the National Institute of Standards and Technology ("NIST")[17] and Center for Internet Security ("CIS").[18] Application of NIST is considered a best practice for financial services use of cloud.[19] Moreover, as discussed further below, the Clearing Agencies would continue to apply existing security processes and standards to include network and identity and

---

17 National Institute of Standards and Technology (2023) The NIST Cybersecurity Framework 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (NIST CSWP) 29 ipd, Released August 8, 2023. https://doi.org/10.6028/NIST.CSWP.29.ipd.

18 Center for Internet Security Benchmarks, cisecurity.org/cis-benchmarks.

19 U.S. Department of the Treasury, *The Financial Services Sector's Adoption of Cloud Services* (February 8, 2024), available at https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf

access management ("IAM") controls, security governance and controls for sensitive data, security configuration, provisioning, logging and monitoring, and security testing and validations.

By hosting in Cloud through the CSP that the Clearing Agencies have engaged, the Clearing Agencies would be able to add cloud-specific security capabilities and measures provided by the CSP, as well as third-party tools. For example, such capabilities and measures would include automation, monitoring, and security incident response capabilities, as well as default separation between Reg. SCI and non-Reg. SCI operating domains, and ubiquitous encryption, all of which are not available in the current on-premises data centers. Similarly, micro-segmentation of applications and infrastructure provided by the CSP, which also is not available in the Clearing Agencies data centers, limits the effect of a security incident and reduces the time to detection and recovery.[20]

4. Increased Scalability

Cloud implementation would allow for greater scalability of Compute, Storage, and Network resources that support Core C&S Systems.[21] With a Cloud Infrastructure,

---

20 For example, the CSP provides infrastructure capable of withstanding Distributed Denial of Service ("DDoS") attacks at far greater magnitudes than the Clearing Agencies' current capabilities, as the CSP has exponentially more internet bandwidth, given their business function, than the Clearing Agencies. (DDoS is a cyberattack in which the attacker floods a server with illegitimate traffic/requests to prevent legitimate users from accessing online services, websites, or computers connected to the attacked server.)

21 The Clearing Agencies would continue to follow existing policies and procedures regarding capacity planning and change management. The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the Change Management Policy and the Technology Capacity and

the Clearing Agencies could quickly provision or de-provision Compute, Storage, or Network resources to meet demands, including elevated trade volumes, and provide more flexibility to create development and test environments, as well as other system development needs.[22] 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.

The Clearing Agencies would pre-provision Compute and Storage resources proactively, in addition to scaling resources on-demand. This means that the Clearing Agencies would be able to increase Compute capacity in one or both regions via manual or automated processes for Core C&S Systems. The rapid deployment of Compute capacity would allow the Clearing Agencies to obtain access to resources far more quickly than with on-premises data centers. The Clearing Agencies would combine the pre-provisioning of primary capacity with regular capacity stress testing to verify that the

---

Demand Assessment Policy. The Clearing Agencies have provided these documents in confidential Exhibit 3 to this advance notice filing.

22 The Clearing Agencies periodically perform capacity and availability planning analyses that result in capacity baselines and forecasts, as an input to technology delivery and strategic planning to ensure cost-justifiable support of operational business needs. These analyses are based on the collection of performance data, trending, scenarios, and periodic high-volume capacity stress tests and include storage capacity for log and record retention. Results are reported to senior technology management as inputs to performance management and investment planning. In addition, each quarter, the Clearing Agencies review the CSP's capacity planning accuracy for the prior quarter and review the upcoming quarter's forecast, along with providing input to the CSP for anticipated major changes in the Clearing Agencies' proposed use of resources. The Clearing Agencies' IT Governance Committee is the designated escalation point for handling capacity management issues.

underlying Compute can sustain required business volumes. The stress testing data would be used to determine the base levels of pre-provisioned capacity.

The ability to quickly scale workloads materially improves the Clearing Agencies ability to respond to unexpected market events and external scenarios, such as a global pandemic.[23] This capability also enables the Clearing Agencies to run risk calculations more frequently, at greater speeds, and with more compute-intensive models than is economically feasible compared to the Clearing Agencies' on-premises infrastructure.

In sum, transitioning to Cloud not only enhances scalability but also significantly improves agility beyond the Clearing Agencies' on-premises capabilities. The on-demand resources provided by the CSP enable dynamic scalability, helping to ensure optimal performance during peak times, efficient resource allocation during periods of lower demand, and the ability to innovate faster to meet evolving business requirements.

C. Why a Single CSP is Appropriate

The Clearing Agencies strongly believe that hosting Core C&S Systems with a single CSP is appropriate. The Clearing Agencies have assessed the capabilities of the CSP in adherence with the Clearing Agency Risk Management Framework,[24] which

---

23 Supply chain challenges during the Covid-19 pandemic highlighted a lack of resiliency and scalability in traditional IT vendors' abilities to deliver resources when needed. Lead times of up to 18 months were experienced and delayed many efforts to expand capacity. This was not the case with CSPs, which did not experience capacity constraints or an ability to meet demand. This further demonstrates how the option to host Core C&S Systems in Cloud is a critical risk mitigation tool for managing against the long-term risk of a waning on-premises industry.

24 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the Clearing Agency Risk Management Framework. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

requires the respective Board of Directors of the Clearing Agencies to approve policies governing relationships with service providers, such as the CSP, thus helping to ensure alignment with the Clearing Agencies' risk management principles.

Beyond simply being a well-known, reputable, industry-leading, and capable CSP, the Clearing Agencies and the CSP have spent several years discussing the Clearing Agencies' needs, including operational, legal, and regulatory obligations; what-if scenarios; and commercial implications. That extensive effort led to a number of benefits, including the CSP introducing new products[25] and the establishment of an exhaustive contractual agreement between the Clearing Agencies and the CSP that addresses the Clearing Agencies' needs for hosting Core C&S Systems in Cloud ("Cloud Agreement").[26] [27]

Meanwhile, it is generally understood that in the present environment adding a secondary CSP or an on-premises backup introduces significant complexity, costs, and

---

25 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding two examples of CSP Whitepapers. The Clearing Agencies have provided these documents in confidential Exhibit 3 to this advance notice filing.

26 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the Cloud Agreement. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

27 Among other things, the Cloud Agreement sets forth the CSP's responsibility to maintain the hardware, software, networking, and facilities that run Cloud services. See also the separately submitted Table of Reg. SCI Provisions provided in confidential Exhibit 3 to this advance notice filing that provides a summary of the terms and conditions of the Cloud Agreement that the Clearing Agencies believe help enable their compliance with Reg. SCI.

risks that outweigh expected benefits.[28] An on-premises or secondary CSP backup would require the Clearing Agencies to engineer their primary Cloud Infrastructure to the lowest common denominator, so that the systems operating on the primary infrastructure also could run on a completely separate and distinct secondary, backup infrastructure. This approach would severely reduce the value that Cloud provides, introduce significant cost with little benefit, and greatly increase operational complexity, all of which would result in negative consequences for the efficiency and resiliency of the Clearing Agencies, their participants, and the industry.

Notwithstanding the extensive benefits from moving to Cloud, the Clearing Agencies fully appreciate and are committed to managing the risks presented in relying on a single CSP, as identified and discussed in Section II.A, further below.

D. Transition Timeframe

The Clearing Agencies believe that transitioning certain Core C&S Systems to the Cloud is critical to managing the risks that are inherent in technology and vendor selection. However, as stated above in Section I.A, the intent of the Cloud Proposal is not to move all Core C&S Systems to Cloud at one time. The Clearing Agencies believe that a "big-bang" transition would introduce unnecessary execution risk, primarily driven by the sheer scale and scope of such an effort. Moreover, many applications on the

---

28 As noted in the U.S. Department of Treasury's report, *The Financial Services Sector's Adoption of Cloud Services*, "No financial institution reported the capability to [run applications across multiple CSPs] for more complex use cases, such as running core operations on multiple public clouds. Running an application across multiple CSPs at the same time may also be less desirable, given the costs, staffing, and complexity involved in doing so, particularly given the complexity associated with identifying and managing risk across multiple cloud environments." Available at https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf at 6.

mainframe are still tightly coupled together and not ready to be moved to public cloud. Rather, at this time, the Clearing Agencies are proposing to move only a subset of the Core C&S Systems to the Cloud and to do so on an incremental basis, in consideration of the specifics of each application and the needs of the Clearing Agencies.[29] This approach helps enable the hosting of Core C&S Systems on the most appropriate platform, at the most appropriate time, in an efficient and secure manner.

The subset of Core C&S Systems selected for this proposal have been initially identified based on several preliminary criteria, including, but not limited to, whether:

- the application would benefit from the presence of data sets already present in Cloud;
- the application would benefit from elasticity enabled by Cloud (e.g., user interfaces); and
- the application already meets certain architectural patterns for Cloud (e.g., the application has already been modernized and currently hosted in private cloud and/or is a siloed application – little to no coupling with other applications).

Assuming the Clearing Agencies would receive no regulatory objection to this advance notice, each application of the proposed subset of Core C&S Systems then would undergo an in-depth, architectural review that would follow the Clearing

---

29 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Global Business Continuity and Resilience Policy and Standards, which defines the governance structure, high-level roles and responsibilities, and the framework for business continuity and resilience processes at the Clearing Agencies. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

Agencies' governance process, governed by the System Delivery Process.[30] The governance process includes, where applicable, a detailed review and approval by the Information Technology Architecture Review Board ("ARB"),[31] the New Initiatives process,[32] to include the Business Case Council and the Risk Assessment Council that vet the financials and risks of the proposed move, and the Investment Management Committee.[33] Further escalations would be made to the Executive Committee and applicable Board of Directors of the Clearing Agencies, as needed. Re-platforming efforts also would be communicated to regulators in accordance with the change reporting requirements of Section 1003(a)(1) of Reg. SCI, as applicable.[34]

---

30 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC System Delivery Policy. The System Delivery Policy defines requirements that support adherence to the System Delivery Process for application development projects. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

31 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the IT Architecture Policy ("ITA Policy"). The ITA Policy provides a set of controls that must be followed to adequately address applicable risks. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

32 The Clearing Agencies also have separately submitted a request for confidential treatment to the Commission regarding the New Initiatives Policy. The New Initiatives Policy provides the governance and oversight structure for the Clearing Agencies to bring initiatives to market timely and efficiently while minimizing risk. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

33 Such reviews and decisions are based on high-level architectural principles that may be applicable to more than one application.

34 17 CFR 242.1003, et seq.

The above-described governance process does not include a specific set of criteria or thresholds for the ultimate determination on whether an application should or should not be moved to Cloud – it is not a formulaic decision. Rather, the Clearing Agencies employ a more qualitative evaluation process that involves various reviews and considers high-level architectural principles that may be applicable to more than one application. However, at this time, none of the Core C&S Systems that have been initially identified as part of the Cloud Proposal, based on the preliminary criteria listed above, have completed that more detailed governance review process. Given the extensiveness of the process, it would not begin until after the Clearing Agencies would receive no regulatory objection to this advance notice.

Although the Clearing Agencies do not anticipate needing to deviate from the proposed transition schedule for the selected Core C&S Systems, the Clearing Agencies recognize that deviation may be necessary, given that the more in-depth governance review process has not completed and because risks could change over the proposed, multiyear implementation period. For example, a deviation may be necessary to address a business need or a change in industry or regulatory requirements or standards. Regardless, any deviation would follow the same detailed governance process, and the Clearing Agencies would provide notice of such deviation to Commission staff, the reason for the deviation, and how the proposed implementation schedule would be updated to account for the deviation. Further, the Clearing Agencies recognize that deviating from the proposed transition schedule 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.

Even though certain on-premises infrastructure components would be decommissioned after applications are moved to Cloud, the Clearing Agencies' private cloud, mainframe services, and data-center facilities would remain available for no less than five more years to help facilitate exit plans from Cloud that rely on an on-premises option. However, to be clear, the on-premises option would not be available to address short-term disruptions, where the Cloud is temporarily unavailable. Management of such disruptions is discussed in Section II.B, further below.

II. Expected Effects on Risks to the Clearing Agencies, their Participants, or the Market

Although the Clearing Agencies are not proposing to transition all Core C&S Systems to Cloud for the reasons described in Sections I.A and D, above, transitioning the proposed subset of Core C&S Systems from an on-premises infrastructure supported by a consolidating industry, as described in Section I.B.1, above, to a new Cloud Infrastructure maintained by an industry-leading CSP provides numerous advantages, as described in Sections I.B.2-4 and C, above. However, such transition is not without risk, as discussed below.

A. Risks Presented by the Cloud Proposal

1. Concentration Risk

The Clearing Agencies appreciate that reliance on a single CSP for hosting the subset of Core C&S Systems that are the subject of this proposal creates concentration risk, particularly in the event of the CSP choosing to terminate its services (i.e., commercial risk) or is unexpectedly unavailable (i.e., operational risk). The Clearing Agencies also appreciate that they would have some reliance on the CSP to help meet certain regulatory obligations of the Clearing Agencies (i.e., regulatory risk), thus

introducing the familiar concept of concentration risk in a relatively new context. However, concentration risk exists today as the Clearing Agencies are dependent on a single mainframe provider, a single database provider for the mainframe, and a single virtualization provider for private cloud. Moreover, the Clearing Agencies believe that they have adequately addressed these risks, as discussed throughout Sections II.B.1-4., below.

2. Cloud Management Risk

Managing the applicable subset of Core C&S Systems hosted on a Cloud Infrastructure presents different risks and challenges than managing such systems hosted on-premises because many activities and services previously provided by the Clearing Agencies would now be provided by the CSP. For example, the Clearing Agencies would be dependent upon the CSP for fulfilling all of its contractual obligations, including security of the Cloud, proper capacity planning, and protection of Cloud services from prolonged operational outages. As such, overseeing the CSP becomes a critical activity to ensure the CSP is delivering services that meet or exceed the Clearing Agencies' requirements for operating those select Core C&S Systems. As discussed in Sections II.B.1-4, below, the Clearing Agencies believe that they have adequately addressed this risk.

B. Management and Mitigation of Identified Risks

1. Cloud Agreement

The Clearing Agencies believe that the Cloud Agreement, including all its amendments and addendums, is a strong tool in helping to effectively mitigate the commercial and regulatory risks borne from the concentration risk, as described in

Section II.A.1, above, as well as risks in managing the CSP that would host the subset of selected Core C&S Systems in the Cloud, as described in Section II.A.2, above. Following is a summary of some of the key terms and conditions covered in the agreement and how they help mitigate these risks.

i. Adequate Notice

Under the Cloud Agreement, the CSP may not unilaterally terminate the relationship with the Clearing Agencies absent good cause or without sufficient notice to allow the Clearing Agencies to transition their applications elsewhere. Specifically, 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 SLA on which the Clearing Agencies rely.[35]

---

[35] The Cloud Agreement permits an exception to this sufficient notice provision in the event the CSP must terminate the individual service offering if necessary to comply with the law or requests of a government entity or to respond to claims, litigation, or loss of license rights related to third-party intellectual property rights. In this event, the CSP must provide reasonable notice to the Clearing Agencies of the termination of the individual service offering. See Reg. SCI Addendum, Section 10 *Termination*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

The CSP is permitted to terminate the Cloud Agreement with shorter notice periods in the event of a critical breach[36] or an uncured material breach[37] [38] of the Cloud Agreement. In the highly unlikely event that a critical breach or uncured material breach occurs, the Clearing Agencies would have sufficient notice to shift their operations away from the CSP. Contract provisions that allow a party to terminate for uncured material breaches are designed to limit the types of actions that could lead to contract termination and to establish a period of time to resolve an aggrieved party's claim (often 30 days) followed by an additional extended period in which to remediate the claim. This gives the parties time and incentive to address the problem without having to resort to termination. In other words, even if the CSP notifies the Clearing Agencies of an alleged breach (material or critical), termination of services is not immediate. Additionally, regardless of the need to shift operations elsewhere – convenience or breach – the Cloud Agreement

---

36 Critical breaches are material breaches (i) for which the Clearing Agencies knew their behavior would cause a material breach (such as a willful violation of Cloud Agreement terms); (ii) that cause ongoing material harm to the CSP, its services, or its customers (e.g., criminal misuse of the services); or (iii) for undisputed non-payment under the Cloud Agreement. See Reg. SCI Addendum, Section 10 *Termination*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

37 Typically, a breach is considered material only if it goes to the root of the agreement between the parties or is so substantial that it defeats the object of the parties in making the contract. See Reg. SCI Addendum, Section 10 *Termination*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

38 See Reg. SCI Addendum, Section 10 *Termination*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

provides for the parties to work together and for the CSP to provide professional services to assist with such a shift.[39]

The Clearing Agencies believe the risk of termination under the above-discussed shorter notice period is minimal. 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 ("Notice Period").[40] With respect to an alleged material breach, which requires the CSP to extend the Notice Period if the Clearing Agencies demonstrate a good faith effort to cure the alleged material breach, the Clearing Agencies would use the Notice Period to attempt to cure the alleged material breach while also preparing to transition elsewhere. As a result, it is highly unlikely that a critical breach or a material breach would remain uncured beyond the Notice Period. If one does remain uncured, however, the CSP can only terminate the rights or accounts associated with the breach, not the entire Cloud Agreement;[41] meanwhile, and the Clearing Agencies would have ample notice to shift operations to avoid a disruption to Core C&S Systems, if needed.

As explained above, adequate notice under the Cloud Agreement plays an important role in managing concentration risk by providing the Clearing Agencies with advance warning of potential disruptions or changes in the agreement or services

---

39 See Reg. SCI Addendum, Section 11 *Post-Termination Services*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

40 See Reg. SCI Addendum, Section 10 *Termination*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

41 See Amendment 1, Section 8 *Temporary Suspension*, of the Cloud Agreement. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

thereunder, which would allow the Clearing Agencies to take proactive measures in mitigating the potential impact of commercial and regulatory risk, thereby reducing concentration risk.

ii. Regulatory Compliance and CSP Oversight

The Clearing Agencies' transition to Cloud does not alter their responsibility to maintain compliance with applicable regulations. Consistent with FFIEC Guidance (as defined and discussed further below), the Clearing Agencies' will continue to fully comply with all applicable regulatory obligations, particularly Reg. SCI.[42]

The Clearing Agencies believe the combination of the following would provide them with reasonable assurance that the proposed transition to Cloud would enable them to continue to fully satisfy their regulatory obligations, including Reg. SCI, thus helping to mitigate the regulatory risk highlighted in Section II.A.1, above: (i) the Cloud Agreement; (ii) the CSP's compliance programs as described in its whitepapers[43] and

---

42 Reg. SCI imposes certain information security and incident reporting standards on the Clearing Agencies and requires them to adopt an information technology governance framework reasonably designed to ensure that "SCI systems," and for purpose of security, "indirect SCI systems," have adequate levels of capacity, integrity, resiliency, availability, and security. 17 CFR 242.1000 et seq.

43 Supra note 25.

publicly available policies (e.g., its Penetration Testing Policy),[44] [45] [46] [47] and user guides; (iii) the CSP's SLAs;[48] [49] [50](iv) the CSP's Systems Organization Controls reports (e.g.,

---

44 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the Operational & Technology Risk Technology Risk Management ("OTR CS&TRM") 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. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

45 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the EAPT Control Standards. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

46 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Information Security – Systems Acquisition Development and Maintenance Policy and Control Standards, which governs the security aspects of information systems acquisition, development, and maintenance for DTCC and its subsidiaries. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

47 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Information Security – Communications and Operations Policy and Control Standards, which helps ensure the correct and secure operation of information processing facilities. The Clearing Agencies have provided this document in confidential Exhibit 3 The Clearing Agencies have provided this document in confidential Exhibit 3to this advance notice filing.

48 The Clearing Agencies have provided the CSP's SLAs in confidential Exhibit 3 to this advance notice filing.

49 Amendment 2, Section 2.2 *To the Service Level Agreements* of the Cloud Agreement provides that the CSP may change its SLAs from time to time but must provide prior notice to the Clearing Agencies before material reducing the benefits offered under the SLAs. The Clearing Agencies have provided Cloud Agreement in confidential Exhibit 3 to this advance notice filing.

50 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Legal Review of Third Party Vendor Contracts Policy, which (1) defines the scope of Vendor Contracts, (2)

SOC 1, SOC 2, SOC 3)[51] and International Organization for Standardization ("ISO") certifications (e.g., ISO 27001);[52] (v) the CSP's size, scale, and ability to deploy extensive resources to protect and secure its facilities and services; and (vi) the CSP's commercial incentive to perform.

Moreover, as noted in Section II.B.ii., above, oversight of the CSP relationship and services has become a standing practice of the Clearing Agencies to ensure that the CSP is meeting or exceeding its contractual obligations, including helping the Clearing Agencies demonstrate their regulatory compliance. Such oversight, which also helps mitigate the cloud management risk raised in Section II.A.2, above, would include a strong relationship between the CSP and the Clearing Agencies, including between their senior management. Within the Cloud Agreement itself, there are established obligations on the CSP to provide the Clearing Agencies' information necessary for the Clearing Agencies to satisfy certain compliance and regulatory requirements, particularly Reg. SCI. For example, the Cloud Agreement obligates the CSP to provide the Clearing

---

clarifies what agreements fall outside the scope and are excluded from the definition of Vendor Contracts, (3) details the process the Clearing Agencies follow when receiving requests to review Vendor Contracts and related materials from CPS Contracts, and (4) establishes the requirements around the creation, maintenance, update, review, and use of contract templates and negotiation guidelines for third party relationships. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

51 The FFIEC Guidance provides that the Clearing Agencies may obtain SOC reports, other independent audits, or ISO certification reports to gain assurance that the CSP's controls are operating effectively. See FFIEC, Security in a Cloud Computing Environment at 7. The Clearing Agencies review the CSP's SOC-2 on an annual basis.

52 The CSP has certifications for the following frameworks: NIST, Cloud Security Alliance, Control Objectives for Information and Related Technology ("COBIT"), ISO, and the Federal Information Security Management Act ("FISMA").

Agencies with immediate notification where a systems intrusion by an unauthorized party or a systems disruption is suspected.[53] The agreement also provides for detailed quarterly briefing meetings between the Clearing Agencies and the CSP, during which the Clearing Agencies would be provided information on and could review service level performance, material systems changes, capacity management, SLA updates, and important security notices.[54]

The Cloud Agreement permits the Clearing Agencies to perform an annual review of the CSP's documentation and services to gain comfort that the CSP is meeting its contractual requirements and that the notification procedures are in place to allow the Clearing Agencies to meet their regulatory requirements, particularly Reg. SCI. The agreement also allows a regulator of the Clearing Agencies 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.[55]

2. Cloud Architecture

To mitigate operational risk associated with the concentration risk from relying on a single CSP, the Clearing Agencies would architect the Cloud Infrastructure hosting their Core C&S Systems to be highly resilient, improving the availability of such systems and related Clearing Agency services during any degradation in CSP services:

---

53 See Reg. SCI Addendum, Sections 8.1 *Systems Intrusion Notification* and 4 *Briefing Meetings*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

54 Id.

55 See Reg. SCI Addendum, Sections 3 *Customer Right of Access and Audit* and 4 *Briefing Meetings*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

- Use of multiple availability zones per region. The Clearing Agencies would use at least three availability zones, in each of the two CSP regions, with each availability zone made up of multiple data centers.
- Multi-regions. In the event of a primary region outage, the Clearing Agencies would recover in the secondary region. Out-of-region recovery would be tested annually by the Clearing Agencies, and a primary/secondary (i.e., hot/warm) model would be used to ensure continuous data replication and recovery is achieved.[56] Recovery exercises of non-Core C&S Systems currently hosted in cloud demonstrate the ability to recover applications within required recovery time objectives, including meeting a 2-hour recovery time objective for relevant applications in the event of an out-of-region recovery.
- Multi-node, high availability clusters across availability zones. Clusters (i.e., three or more servers or nodes) protect against local hardware and service failures providing uninterrupted operations. Each cluster would be distributed across three availability zones. Clusters synchronously replicate data across all nodes to protect against data loss and provide continuous availability.
- Static stability and static capacity models. Static capacity would be pre-provisioned for compute, storage, and memory for applications based on capacity stress testing results and capacity requirements. The Clearing Agencies would pre-provision capacity needed for applications and services

---

56 See Reg. SCI Addendum, Section 5 *Customer Testing of CSP Systems*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

and would not rely on capacity on-demand models, thus reducing the risk of running out of capacity.

- Exit plans. The Clearing Agencies' existing policies require that all applications hosted in Cloud have documented exit plans, with each plan updated annually.[57] The Clearing Agencies' Cloud architecture also reduces "vendor lock-in" by using capabilities such as "containers"[58] that can exist in both the public and private cloud, where appropriate and applicable. For the foreseeable future, the Clearing Agencies plan to continue to own or lease private data center space to host private cloud and mainframe capabilities. The Clearing Agencies private, on-premises data centers help enable a long-term exit plan from Cloud, if needed. However, such data centers would not be a means to address a short-term incident at the CSP. Additionally, for the second CSP that the Clearing Agencies already have contracted and connected with for hosting non-Core C&S Systems, they are now working on the contractual and operational requirements that would be necessary to possibly host Core C&S Systems in its Cloud to further enable exit plans from the primary CSP.
- Regional Isolation Architecture. A cross-regional outage is highly unlikely at the CSP, as the CSP has designed and implemented a series of controls to ensure that defects cannot be introduced to more than a single region at a

---

57 Supra note 29.

58 A container is a standard unit of software that packages up code and all its dependencies, so the application runs reliably from one computing environment to another (e.g., public and private clouds).

time.[59] Services are regionally isolated with a single exception – the IAM service. The IAM service is not regionally isolated and depends on a single region. If the primary region for the IAM service fails, the service will continue to operate but as read-only. To mitigate this risk, the Clearing Agencies would architect applications and infrastructure services in such a manner that they would not require updates (i.e., writes) to the IAM service in order to rotate out of region.

In summary, cloud architecture helps mitigate operational risk borne from concentration risk, as raised in Section II.A.1, above, by providing resilient infrastructure, scalable resources, robust security measures, and disaster recovery capabilities, all of which assist in minimizing the impact of disruptions.

3. Standing Risk Management Practices

The Clearing Agencies' standing risk management practices also help minimize operational risk by systemically identifying, assessing, mitigating, monitoring, and responding to risk. For example, the Clearing Agencies have considered the possibility of the CSP being completely and unexpectedly unavailable, whether due to technical issues or other reasons. The parallel risk exists today with respect to the Clearing Agencies' existing infrastructure. Just like with the CSP, it is possible that the Clearing Agencies' two existing data centers – one primary and one backup – become completely and unexpectedly unavailable. In fact, it is more likely that those two data centers become unavailable than the CSP's data centers because the CSP has so many more data centers

---

59 The CSP owns the control and has provided documentation of the control to the Clearing Agencies.

for each availability zone, in both its primary and secondary regions, with each data center, not just the associated region or availability zone, having its own physical infrastructure, staff, power, backup power, mechanical services, and network connectivity, as discussed in Section I.B.2, above. Even for the CSP's IAM service that runs cross regions, the applications in each region operate off read-only versions of the IAM roles and responsibilities, such that loss of the primary would not affect operation of those applications. Nevertheless, to help manage a crisis event, such as the Clearing Agencies' or the CSP's data centers becoming unavailable, the Clearing Agencies have standing risk management plans and practices already in place, as described below.[60]

In the very unlikely event of an unexpected single- or multi-region outage in which the Clearing Agencies operate, or a complete and unexpected CSP outage, the Clearing Agencies would initiate the existing Major Incident Management ("MIM") 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 ("BIMS")[61] would be activated. Depending on the severity of the event, the DTCC Global Business Continuity and Resilience ("BCR") Policy

---

60 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the Operational Response Capabilities Matrix. The Clearing Agencies have provided these documents in confidential Exhibit 3 to this advance notice filing.

61 MIM is part of the IT organization that manages technology specific incidents at the Clearing Agencies that are typically resolved at the application or hardware level with support from the appropriate subject matter experts ("SMEs"). Incidents that have a business impact are escalated to BIMS and appropriate SMEs are added to manage the impact, which includes Business Continuity and Resilience. BIMS participants can request the Crisis Management Team be activated if the incident requires discussion or has escalated to a potential disaster that may require a declaration of disaster.

would provide a predictable structure to be utilized during crises and could be leveraged to address, respond to, and manage an outage.[62] 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.[63]

The BCR Policy and Standards is structured to employ existing DTCC and Clearing Agency teams and committees, which become the tactical leadership to react, respond, and manage a crisis situation.[64] The teams are comprised of the following:

---

62 The Clearing Agencies are taking into consideration the forthcoming requirements of adopted and effective Rule 17ad–25(i) under the Exchange Act, 17 CFR 240.17ad–25(i), and anticipate that the Clearing Agencies' approach in managing the risk presented by a CSP outage for Core C&S Systems would be consistent with those requirements.

63 For example, there is an existing plan to manage a Fedwire protracted outage. A Fedwire protracted outage is an interruption or outage of Federal Reserve Bank hardware or software that prevents the bank from processing payment orders online and that is not expected to be resolved before the bank's next Fedwire Funds Service Funds Transfer Business Day. In the event of such an outage, the Clearing Agencies will assess the situation and employ, as needed and applicable, the steps outlined in the BCR Policy and Standards, the Federal Reserve Banks Operating Circulars (see, e.g., Operating Circular No. 6, available at https://www.frbservices.org/binaries/content/assets/crsocms/resources/rules-regulations/070123-operating-circular-6.pdf), and any other regulatory guidance.

64 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. The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the BCR Policy and Standards which define the governance structure, high-level roles and responsibilities, and the framework for business continuity and resilience processes at the Clearing Agencies. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

- Crisis Management Team. Comprised of the Management Committee, site General Managers, Head of the Board Risk Committee,[65] and other SMEs, as needed.
- Crisis Response Teams.
  - *Business Continuity Coordinators and Plan Approvers* – These are individuals who manage business continuity at a plan level.
  - *Fair and Orderly Markets Groups* – These are crisis teams comprised of internal stakeholders and top executives from external firms deemed necessary to ensure a fair and orderly market. They would be activated (based on impact to the legal entity) to gather information during a large systemic event when operational coordination is required with clients and the sector.
  - *IT Management Team* – Comprised of Information Technology managing directors and SMEs.
  - *Management Risk Committee* – Comprised of senior members across the enterprise.
  - *Senior Site Management Team ("SSMT")* – Each DTCC office with a facility level resilience plan ("FLRP") has an SSMT, that is comprised of senior leadership from the site.

---

65 The Board Risk Committee is a Board level committee established by the Boards of the Clearing Agencies to assist their respective Boards in fulfilling their responsibilities for oversight of risk management activities at the Clearing Agencies. This includes oversight of credit, market, liquidity, operational, and systemic risks.

- *Site Assessment Team ("SAT")* – Sites with an FLRP have a SAT that responds to site-specific events. This team is comprised of a primary/back-up site General Manager and representatives from BCR, IT, Workplace Design and Service, Global Security Management, and Human Resources. A Data Center Services representative also is added for sites that have a data center.
- *MIM and BIMS Teams* – Part of the IT organization that manages technology specific and are typically resolved at the application or hardware level with support from the appropriate SMEs.

- Crisis Communication Team. The Crisis Communication Team is comprised of officer-level members from Marketing and Communication, Human Resources, General Counsel's Office, and Regulatory Relations, as well as members of their staffs, as applicable.

The Clearing Agencies believe that these standing risk management practices are key to managing the operational risk borne from concentration risk outlined in Section II.A.1, above, by helping to promote proactive risk management culture, enhancing operational resilience, and enabling the Clearing Agencies to better navigate uncertainties and maintain business continuity.

4. Industry Standards for Cloud Management

i. Cloud Management: Federal Financial Institutions Examination Council Cloud Computing Guidance ("FFIEC")

On April 30, 2020, FFIEC[66] issued a joint statement to address the use of Cloud computing services and security risk management principles in the financial services sector ("FFIEC Guidance").[67] While the FFIEC Guidance does not contain regulatory obligations, it highlights risk management practices that financial institutions should adopt for the safe and sound use of Cloud computing services in five broad areas ("FFIEC Risk Management Categories"): Governance, Cloud Security Management, Change Management, Resilience and Recovery, and Audit and Control Assessment. As discussed below, the Clearing Agencies would implement practices consistent with the FFIEC Risk Management Categories for Core C&S Systems operated in Cloud to help address cloud management risk, as highlighted in Section II.A.2, above, by providing frameworks, guidelines, and best practices, that enhance transparency, reliability, and security.

---

66 FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Consumer Financial Protection Bureau, and to make recommendations to promote uniformity in the supervision of financial institutions.

67 Available at https://www.ffiec.gov/press/pr043020.htm.

(a) Governance

The Clearing Agencies and the CSP rely on a shared responsibility model that differentiates between security "of" the Cloud and security "in" the Cloud.[68] This model is not specific to the agreement between the Clearing Agencies and the CSP; rather, it is a more universally followed model for public cloud services. Under the model, the CSP maintains sole responsibility and control over the security and resiliency "of" the Cloud, and their customers are responsible for the security and resiliency "in" the Cloud (i.e., security and resiliency of hosted applications and data). This means that the Clearing Agencies must manage their own application architectures, data backups, change management controls, network configurations within applications, and response to application failures. In addition, the Clearing Agencies must manage their own data usage and data-at-rest encryption configuration, IAM access policies and roles, operating system upkeep, security group configurations, and network traffic encryption in transit configurations. The Clearing Agencies also manage how they place workloads onto the CSP's platform.

Meanwhile, the CSP must manage backend hardware services for Compute, Storage, Networking, database, and global architectures such as regions, availability zones, data centers, power, and HVAC, as well as backend security services that protect core infrastructures. The CSP manages the underlying infrastructure and upkeep, so that the Clearing Agencies (and other customers) can place workloads on the CSP platform

---

68 "Shared responsibility" conveys the responsibility of the Clearing Agencies and the CSP vis-à-vis each other from a business operations perspective. It does not mean that the CSP has taken on or that the Clearing Agencies have relinquished any of their Reg. SCI compliance requirements.

with proper security and separation without having to manage these traditional data center tasks. The Clearing Agencies review the CSP's policies and procedures for these functions during the quarterly reviews and during annual risk assessments.

When looking more closely at hardware management, the Clearing Agencies believe there are benefits in how the CSP manages hardware for Cloud compared to how the Clearing Agencies manage hardware for their own data centers. For example, with on-premises data centers, the Clearing Agencies must oversee a multifaceted supply chain, involving many vendors to obtain and administer physical Compute, Storage, and Network capacity. Delivery times may fluctuate, and scarcities can affect project outcomes, as seen during the Covid-19 pandemic. In contrast, with the proposed Cloud Infrastructure, the CSP controls the hardware supply chain and even partakes in key areas of the manufacturing process to circumvent typical problems such as chip shortages. Moreover, the Clearing Agencies get to review the CSP's equipment forecast for each upcoming quarter, affording the Clearing Agencies the opportunity to address potential supply chain difficulties, if any, without jeopardizing their access to adequate capacity, by leveraging capabilities such as reserved capacity. Altogether, the Clearing Agencies believe the CSP's management of Cloud hardware will be a benefit to them.

The CSP would perform its own risk and vulnerability assessments of the CSP infrastructure on which the Clearing Agencies would run their Core C&S Systems. In published documentation and in meetings conducted with the CSP, the CSP asserts that it maintains an industry-leading automated test system, with strong executive oversight, and conducts full-scope assessments of its hardware, infrastructure, internal threats, and application software. The CSP asserts that it has an aggressive program for conducting

internal adversarial assessments ("Red Team") designed not only to evaluate system security but also the processes used to monitor and defend its infrastructure. The CSP also uses external, third-party assessments as a cross-check against its own results and to ensure that testing is conducted in an independent fashion. Pursuant to the CSP's documentation, results of these processes are reviewed weekly by the CSP's Chief Information Security Officer and the Chief Executive Officer with senior CSP leaders to discuss security and action plans.[69]

The Clearing Agencies have the responsibility to perform risk assessments and technical security testing, including control validation, penetration testing, and adversarial testing of their applications running on the Cloud Infrastructure. This includes testing of the application interface layer of some CSP provided services such as storage and key management.

As mentioned, the Clearing Agencies' testing includes assessing the configuration of the CSP provided services. The Clearing Agencies' Technology Risk Management staff would work with the Clearing Agencies' Information Technology staff to ensure that the CSP tools are configured to appropriately manage and mitigate potential sources

---

69 The CSP does not provide assessment results to its customers, as doing so would constitute a breach of generally accepted security best practices. Instead, the CSP provides its customers with industry-standard reports – such as SOC2 Type II – prepared by an independent third-party auditor to provide relevant contextual information to its customers. The CSP also conducts periodic audit meetings specifically designed to discuss security concerns with its customers discussed later during the "CSP Audit Symposium." Additionally, the Clearing Agencies have certain audit rights (pursuant to Section 3 *Customer Rights of Access and Audit* of the Reg. SCI Addendum) to review information about the nature and scope of the CSP's vulnerability management program.

of risk and will assess the effectiveness of those configurations.[70] The Technology Risk Management staff has developed an application, Cloud Governance Insights ("CGI"), to continuously monitor all Cloud Infrastructure for alignment to security baselines and configurations best practices.[71] The CGI dashboard allows Information Technology and Technology Risk Management staff to understand the environment risk posture and reporting of key risk indicators ("KRIs"). The Clearing Agencies' Red Team would operate freely "in the Cloud," attempting to subvert or circumvent controls.[72] The testing would include probing of the CSP provided services to look for weaknesses in the Clearing Agencies' deployment of those tools.

Technology Risk Management staff would routinely report test results to the Technology Risk Management Steering Committee and the Management Risk Committee, appropriate functional Operations and Information Technology management,

---

70 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the OTR TRM Core Process Procedure – Security Configuration Violation Rules, which is used to manage enterprise information security risk by ensuring a consistent configuration violation scoring process that provides timely identification of configuration violations and their severity ratings. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

71 CGI is the Clearing Agencies' internally developed solution to perform Cloud Security Posture Management and assess Cloud Infrastructure compliance against TRM Control Standards and Security Baselines in near real-time.

72 Supra note 47.

senior management, and the Board of Directors of the Clearing Agencies.[73] [74] Automated vulnerability scanning reports, source code analysis, and results of specific assessments would be risk-rated and assigned a priority for remediation in accordance with Clearing Agency Information Security Program requirements.[75] [76]

Management and oversight of the Cloud implementation follows the Clearing Agencies' standard governing principles for large information technology projects.[77] To maintain accountability over the CSP's performance, regular reporting to the Boards of the Clearing Agencies by senior management is essential and required, pursuant to the

---

73 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Information Security – Information Security Management Policy and Control Standards, which defines the roles, responsibilities, and accountabilities for DTCC's security practices and organization structure suited to protect DTCC's critical systems and business assets. Information Security Management evaluates DTCC's information security program's overall effectiveness, and establishes, maintains, communicates, and periodically reassesses information security policies and a comprehensive information security program that are approved by management. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

74 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Information Security – Risk Management Policy and Control Standards, which provides (i) requirements for establishing, implementing, maintaining, and continually improving the information risk management program, (ii) a governance structure utilized for the escalation of information risks to an appropriate management level, and (iii) organizational roles and responsibilities for the delivery of comprehensive information security and technology risk management program. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

75 Supra note 46.

76 Supra note 47.

77 Supra note 32.

DTCC Third Party Risk Procedures.[78] Such reporting helps ensure that senior management takes appropriate actions to address significant performance deterioration, changing risks, or material issues identified through ongoing monitoring, thereby helping to ensure proactive risk management and continuous improvement.[79] The Clearing Agencies' Board of Directors has established a Technology and Cyber Committee to assist the Board of Directors in overseeing information technology and cybersecurity strategy and capabilities.

Information Technology and the Enterprise Program Management Office ("EPMO") are responsible for the identification, management, monitoring, and reporting on the risks associated with the modernization and migration of applications to Cloud. To that end, reports on the status and progress of these efforts are reported to applicable Clearing Agency committees based on escalation criteria in the EPMO Procedure.[80] These reports include overall risk and issue summaries and analysis of key risk indicators for the migration of applications to the public cloud.

---

78 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Third Party Risk Procedures, which establish the standards and practices to be used by certain business line departments and/or functional units to manage the potential risks associated with engaging with an external service provider. The Clearing Agencies have provided these documents in confidential Exhibit 3 to this advance notice filing.

79 Supra note 62.

80 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the Enterprise Program Management Office Procedure, which outlines the minimum standards and practices the Clearing Agencies use to manage, measure, and monitor the performance of key processes aligned to the Enterprise Program Management Office Policy. The Clearing Agencies have provided these documents in confidential Exhibit 3 to this advance notice filing.

Finally, the Clearing Agencies' Internal Audit Department ("IAD"), as the independent third line of defense, is responsible for assessing and challenging the firm's control environment and risk management and control frameworks, which include those related to the Cloud, including, but not limited to, security controls and configurations, and report the results of those assessments to management and the Audit Committee of the Board.[81]

Ultimately, there is no primary/secondary relationship, as the Clearing Agencies and the CSP each have their own set of responsibilities which, when combined, address the entire risk space.

(b) Cloud Security Management

The Clearing Agencies have established a robust Cloud security program to (i) manage the security of the Core C&S Systems that would be running on the Cloud Infrastructure hosted by the CSP, and (ii) assess and monitor the CSP management of security of the Cloud Infrastructure that it operates. The security program is built upon Clearing Agency Information Security Policies and Control Standards that establish requirements that apply to any technology system as well as any tool that provides

---

[81] The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the Internal Audit Department Policies and Procedures, which contains the policies and guidance that direct the activities of the Clearing Agencies' IAD. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

technology services.[82] [83] [84] [85] Below describes elements of the Clearing Agencies' Cloud security management in the areas of (i) IAM controls (i.e., determining who is accessing the systems, granting access to the applications, and then controlling what information they can access); (ii) security governance and controls for sensitive data; (iii) security configuration, provisioning, logging, and monitoring; and (iv) security testing.

(1) Network and IAM Controls

The Clearing Agencies recognize that robust network security configuration and IAM would provide reasonable assurance that users – including Clearing Agency

---

82 Supra notes 46-47, 73-74.

83 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Information Security – Asset Security Policy and Control Standards, which governs management of security for the information assets of the Clearing Agencies. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

84 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Information Security – Monitoring and Incident Management Policy and Control Standards, which governs DTCC's 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. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

85 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Information Security – Asset Access Control Policy and Standards, which governs management of security for the information assets of the DTCC and its subsidiaries. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

employees, market participants, and service accounts for systems[86] – are granted least-privileged access[87] to the network, applications, and data in the Cloud. The Clearing Agencies would use third-party tools to automate appropriate role-based access to the Core C&S Systems running in the Cloud. By enforcing strict separation of duties and least-privileged access for infrastructure, applications, and data, the Clearing Agencies would protect the confidentiality, availability, and integrity of the data in the Cloud.

The Clearing Agencies have established IAM requirements that build upon the least-privileged model.[88] As part of the IAM program, all users must be assigned an appropriate enterprise identification. Additionally, the Clearing Agencies have established Highly Privileged Access Management capabilities and policies to further restrict highly privileged access to be used only in pre-determined scenarios that must be tied to a change, incident, request, or release records.[89]

Cloud users would be granted access to systems via a standardized and auditable approval process. The user identifications and granted access would be managed through their full lifecycle from a centralized IAM system maintained and administered by the Clearing Agencies. Role-, attribute-, and context-based access controls would be used as

---

86 Service accounts are non-interactive accounts that permit application access to support activities such as monitoring, logging, or backup. Service accounts are also used for machine-to-machine communications.

87 Least-privileged access means users only have the permission needed to perform their work, and no more.

88 Supra note 85.

89 Id.

defined by internal standards[90] consistent with industry recommended practices to promote the principles of least-privileged access and separation of duties.[91]

The Clearing Agencies would use and manage third-party tools not otherwise provided by nor managed by the CSP for single sign-on and least-privileged access.[92] The network also would include hardware and software to limit and monitor ingress and egress traffic, encrypt data in transmission, and isolate traffic between the Clearing Agencies and the Cloud.[93] Since the Clearing Agencies would continue to provide cryptographic services, including key management, the CSP and other network service providers would not be able to decrypt Clearing Agency data either at rest or while in transit.

(2) Security Governance and Controls for Sensitive Data

The Clearing Agencies' data governance framework that would apply to Cloud implementation is identified within the Clearing Agency Information Security Policies and Control Standards.[94] The Clearing Agency Information Security Policies and Control

---

90 Id.

91 (1) ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security controls; (2) NIST Cybersecurity Framework (CSF) Version 1.1; (3) NIST Special Publication 800-53 Revision 4 – Security and Privacy Controls for Federal Information Systems and Organizations.

92 For example, the Clearing Agencies currently use Bravura Security Privileged Access Management (a/k/a PAM) for highly privileged access management.

93 Supra notes 47, 84-85.

94 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Data Risk Management Policy, which establishes requirements for the sound management of data risk across the

Standards address data moving between systems within the Cloud as well as data transiting and traversing both trusted and untrusted networks. For example, the Clearing Agencies' Information Security Policies and Control Standards require a system or Software as a Service (i.e., SaaS) to (i) store data and information, including all copies of data and information in the system, in the U.S., throughout its lifecycle; (ii) be able to retrieve and access the data and information throughout its lifecycle; (iii) for data in the system hosted in the Cloud, encrypt such data with key pairs kept and owned by the Clearing Agencies; (iv) comply with U.S. federal and applicable state data regulations regarding data location; and (v) enable secure disposition of non-records in accordance with the Clearing Agencies' Information Governance Policy.[95]

Furthermore, the Clearing Agencies' policies establish the overall data governance framework applied to the management, use, and governance of Clearing Agency information to include digital instantiations, storage media, or whether the information is located, processed, stored, or transmitted on the Clearing Agencies' information systems and networks; public, private, or hybrid cloud infrastructures; third-party data centers and data repositories; or SaaS applications.[96] The Information Classification and Handling Policy[97] classifies the Clearing Agencies' information into categories. System owners of technology that enable classification and/or labeling of

---

data lifecycle. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

95 Supra note 85.

96 Supra note 46.

97 Supra note 83.

information are responsible for ensuring the correct classification level is designated in the system of record and the applicable controls are enforced. All information requiring disposal is required to be disposed of securely in accordance with all applicable procedures. Sensitive data must be handled in a manner consistent with requirements in the Information Classification and Handling Policy.

The Clearing Agencies would implement key security components, namely ubiquitous authentication, and encryption via use of an automated public key infrastructure, coupled with responsive, highly available authentication, authorization tools, and key management strategies to ensure appropriate industry standard security controls are in place for sensitive data both in transit to and at rest in Cloud.[98]

External connectivity to the Clearing Agencies' systems hosted by the CSP would be provided, as it is now, through dedicated private circuits or over encrypted tunnels through the Internet. These network links also would have additional security controls, including encryption during transmission and restrictions on network access to and from the Cloud. Additionally, the Clearing Agencies would use dedicated redundant private network connections between the Clearing Agencies data centers and the CSP infrastructure. The Clearing Agencies currently maintains two data centers and will do so in the near term to provide redundant, geographically diverse connectivity for market participants.

All network communications between the Clearing Agencies and the Cloud Infrastructure would rely on industry standard encryption for traffic while in transit. Data at rest would be safeguarded through pervasive encryption. The Clearing Agencies'

---

98 Supra note 47.

Encryption Standards[99] describe requirements for implementation of the minimum required strengths, encryption at rest, and cryptographic algorithms approved for use in cryptographic technology deployments across the Clearing Agencies. All Clearing Agency identifying data is encrypted in transit using industry standard methods. The Key Management Service ("KMS") Strategy[100] dictates that all CSP endpoints support HTTPS for encrypting data in transit. The Clearing Agencies also secure connections to the endpoint service by using virtual private computer endpoints and ensures client applications are properly configured to ensure encapsulation between minimum and maximum Transport Layer Security versions pursuant to the Clearing Agencies' encryption standard.

The Clearing Agencies would have exclusive control over the encryption keys; only Clearing Agency authorized users and approved third parties would be able to access Clearing Agency data. The CSP systems and staff would not have access to the Clearing Agencies' certificates or keys.[101] The Clearing Agencies would be responsible for the application architecture, software, configuration, and use of the CSP services, and for the maintenance of the environment, including ongoing monitoring of the application environment to achieve the appropriate security posture. To do this, the Clearing

---

99 Supra note 91.

100 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Information Security – Public Key Infrastructure Policy and Control Standards, which governs the public key infrastructures implemented and used within DTCC and its subsidiaries. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

101 Certificate management is the process of creating, monitoring, and handling digital keys (certificates) to encrypt communications.

Agencies would follow (i) existing security design and controls; (ii) Cloud-specific information security controls defined in the Clearing Agencies' Information Security Policies and Control Standards;[102] and (iii) regulatory compliance requirements detailed in sources or information technology practices that are widely available and issued by an authoritative body that is a U.S. governmental entity or agency including NIST-CSF,[103] COBIT,[104] and the FFIEC Guidelines.[105]

The Clearing Agencies would use third-party and custom developed tools for CSP security compliance monitoring, security scanning, and reporting. Alerts and all API-level actions would be gathered using both CSP provided, Clearing Agency developed, and third-party monitoring tools. The CSP provided monitoring tool would be enabled by default at the organization level to monitor all CSP services activity. Centralized logging provides near real-time analysis of events and contains information about all aspects of user and role management, detection of unauthorized, security relevant configuration changes, and inbound and outbound communication.

As discussed just above, the Clearing Agencies would use a KMS Strategy to encrypt data in transit and at rest in the Cloud. KMS is designed so that no one, including CSP employees, can retrieve customer plaintext keys and use them. The Federal Information Processing Standards 140-2 validated Host Security Modules ("HSMs") in

---

102 Supra note 91.

103 NIST Cybersecurity Framework Version 1.1.

104 *COBIT 2019 Framework: Governance and Management Objectives.*

105 FFIEC Information Technology Examination Handbook – Information Security (September 2016).

KMS protect the confidentiality and integrity of Clearing Agency customer keys.[106] Customer plaintext keys are not written to disk and are only used in protected, volatile memory of the HSMs for the time needed to perform the customer's requested cryptographic operation. KMS keys are not transmitted outside of Cloud regions in which they were created. Updates to the KMS HSM firmware will be controlled by quorum-based access control[107] that is audited and reviewed by an independent group within the CSP.

(3) Security Configuration, Provisioning, Logging, and Monitoring

Automated delivery of business and security capability via the use of "Infrastructure as Code" and continuous integration/continuous deployment pipeline methods would permit security controls to be consistently and transparently deployed on-demand. The Clearing Agencies would provision Cloud Infrastructure using pre-established system configurations that are deployed through Infrastructure as Code, then scanned for compliance to secure baseline configuration standards. The Clearing Agencies also would employ continuous configuration monitoring and periodic vulnerability scanning. The Clearing Agencies would perform regular reviews and testing of Clearing Agency systems running in Cloud while relying upon information provided by the CSP through the CSP's SOC2 and Audit Symposiums. Finally, configuration,

---

106 The HSM is analogous to a safe to which only the Clearing Agencies have the combination and the ability to access the keys to locks stored within.

107 A quorum-based access mechanism requires multiple users to provide credentials over a fixed period in order to obtain access.

security incident, and event monitoring would rely on a blend of CSP native and third-party solutions.

The Clearing Agencies also plan to use tools offered by the CSP, developed by the Clearing Agencies, and third parties to monitor the Core C&S Systems running in Cloud. The Clearing Agencies would track metrics, monitor log files, set alarms, and have the ability to act on changes to Core C&S Systems and the environment in which they operate. The CSP would provide a dashboard to reflect-general health (e.g., up/down status of a region and CSP provided services running in that region) but would not give additional insights into performance of services and applications which run on those services. The Clearing Agencies' centralized logging system would provide for a single frame of reference for log aggregation, access, and workflow management by ingesting the CSP's logs coming from native detective tools and the Clearing Agencies' instrumented controls for logging, monitoring, and vulnerability management. This instrumentation would give the Clearing Agencies a real-time view into the availability of Cloud services as well as the ability to track historical data. By using the enterprise monitoring tools that the Clearing Agencies have in place, the Clearing Agencies would be able to integrate the availability and capacity management of Cloud into the Clearing Agencies' existing processes, hosted in Cloud, to respond to issues in a timely manner.

The Clearing Agencies also would use specialized third-party tools, as discussed just above, to programmatically configure Cloud services and securely deploy infrastructure. This automation of configuration and deployment would help ensure that Cloud services are repeatably and consistently configured securely and validated. Change

detection tools providing event logs into the incident management system also are vital for reacting to and investigating unexpected changes to the environment.

The Clearing Agencies would implement tools for the Core C&S Systems and back-office environments that would be hosted on the Cloud Infrastructure, notably, IAM, monitoring and Security Information and Event Management systems, the workflow system of record for incident handling, KMS, and enterprise Data Loss Prevention.

Finally, the CSP prioritizes assurance programs and certifications, underscoring its ability to comply with financial services regulations and standards and to provide the Clearing Agencies with a secure Cloud Infrastructure.[108]

(4) Security Testing and Verification

Security testing is integrated into business-as-usual processes as outlined in relevant policy and procedures.[109] These documents define how testing is initiated, executed, and tracked.

For new assets and application (or code) releases, Technology Risk Management determines whether and what type of security testing is required through a risk-based analysis.[110] If required, testing would be conducted prior to implementation. The different testing techniques are outlined below:

---

108 The CSP has certifications for the following frameworks: NIST, Cloud Security Alliance, COBIT, ISO, and FISMA.

109 Supra note 46.

110 Supra note 30.

- Automated Security Testing. Using industry standard security testing tools and/or other security engineering techniques specifically configured for each test, the Clearing Agencies would test to identify vulnerabilities and deliver payloads with the intent to break, change, or gain access to unauthorized areas within an application, data, or system.
- Manual Penetration Testing. Using information gathered from automated testing and/or other information sources, the Clearing Agencies would manually test to identify vulnerabilities and deliver payloads with the intent to break, change, or gain access to the unauthorized area within an application or system.
- Blue Team Testing. The Blue Team identifies security threats and risks in the operating environment and analyzes the network, system, and SaaS environments and their current state of security readiness. Blue Team assessment results guide risk mitigation and remediation, validate the effectiveness of controls, and provide evidence to support authorization or approval decisions. Blue Team testing ensures that the Clearing Agencies' networks, systems, and SaaS solutions are as secure as possible before deploying to a production environment.

The results of the Clearing Agencies' security controls testing are risk-rated and managed to remediation via two separate control standards.[111]

---

111 Supra notes 46-47.

(c) Change Management: Software Development and Release Process

Consistent with FFIEC Guidance, the Clearing Agencies' use of Cloud would have sufficient change management controls in place to effectively transition systems and information assets to Cloud and would help ensure the security and reliability of applications in Cloud.[112] The Clearing Agencies' enterprise software development lifecycle processes[113] would help ensure the same control environment for all Clearing Agency resources. The Clearing Agencies would establish baselines for design inputs and control requirements and enforce workload isolation and segregation through Cloud using existing Cloud native technical controls and added new tools. The Clearing Agencies also would plan to use other specialized platform monitoring tools for logging, scanning of configuration, and systems process scanning. The Clearing Agencies also would have oversight as the code owner and would have final review and approval for related changes and code merges before deployment into production. Finally, the Clearing Agencies would periodically conduct static code scanning and perform vulnerability scanning for external dependencies prior to deployment in production, along with manual penetration testing of the provided application code. In addition, the Clearing Agencies would perform routine scans of Compute resources with the existing enterprise scanning tools. Any identified vulnerabilities would be reviewed for severity, prioritized, and logged for remediation tracking in upcoming development releases.

---

112 Supra note 30.

113 Id.

The Clearing Agencies would create a "user acceptance plan" prior to promoting code to Cloud production. This user acceptance plan would include tests of all major functions, processes, and interfacing systems, as well as security tests. Through acceptance tests, the Clearing Agencies' users would be able to simulate complete application functionality of the live environment. The change would move to the next stage of the Clearing Agencies' delivery model only after satisfying the criteria for this phase.[114]

The Clearing Agencies would have internal projects that would address change management of the various applications and services. In particular, the Clearing Agencies would run a suite of supporting services that enable building, running, scaling, and monitoring of the Clearing Agencies' business applications in Cloud, in an automated, resilient, and secure manner.[115] The application platform relies on various CSP and third-party tools for different components, including IaaS, Infrastructure as Code, CI/CD, Container as a Service, Continuous Delivery, and Platform Monitoring.

With respect to software development in Cloud, the Clearing Agencies would establish a closed, non-production Cloud environment that would enable the Clearing Agencies to develop, test, and integrate new capabilities, including those related to security capabilities. This non-production Cloud environment would focus on the foundational security, operations, and infrastructure requirements with the intent to take lessons learned to implement into future production. The Clearing Agencies would

---

114 The "user acceptance plan" represents only one aspect of the overall change management program at the Clearing Agencies.

115 Supra note 30.

maintain a Cloud Reference Architecture that defines necessary capabilities and controls required to securely host Core C&S Systems. The minimum foundational security requirements would be based on the NIST-CSF and CIS benchmarks and include the design and implementation requirements of a secure Cloud account structure within a multi-region Cloud environment. The Clearing Agencies would maintain enterprise security requirements that provide structure for current and future development. As the Cloud environment is further developed and expanded, there would be a comprehensive process to identify any incremental risks and develop and implement controls to manage and mitigate those risks.

(d) Resilience and Recovery

As noted earlier, given the Clearing Agencies' roles as systemically important financial market utilities, it is vital that operations moved to the Cloud have appropriately robust resilience and recovery capabilities. As discussed in Section II.B.ii.2, above, the Cloud Infrastructure would be architected to include (i) two autonomous and geographically diverse regions; (ii) three availability zones per region, with each availability zone comprised of multiple data centers; (iii) multi-node, high availability clusters across each availability zone; (iv) static stability and static capacity models; and (v) regional isolation, all to help ensure the persistent availability of Compute, Storage, and Network capabilities in Cloud.

Additionally, the CSP's practice in deploying service updates to Cloud would help ensure that the consequences of any incidents would be limited to the fullest extent

possible.[116] The CSP achieves this by (i) fully automating the build and deployment process and (ii) deploying services to production in a phased manner.

CSP service updates are first deployed to cells, which minimizes the chance that a disruption from a service update in one cell would disrupt other cells. Following a successful cell-based deployment, service updates are next deployed to a specific availability zone, which limits any potential disruption to that zone. Following a successful availability zone deployment, service updates are then deployed in a staged manner to other availability zones, starting with the same region and later within other regions until the process is complete.

The Clearing Agencies would meet regularly with the CSP, in addition to formal quarterly briefing meetings with the CSP, as described in the Reg. SCI Addendum.[117] The informal discussions and quarterly briefing meetings would permit the Clearing Agencies to gather information in advance of the quarterly systems change report. Most reportable systems changes would continue to occur based on changes to Compute, Storage, Network, or applications controlled by the Clearing Agencies.

(e) Audit Controls and Assessment

The Clearing Agencies would regularly test security controls and configurations, including by monitoring the CSP's technical, administrative, and physical security controls that support the Clearing Agencies' systems in the Cloud Infrastructure.

---

116 The Clearing Agencies would continue to retain responsibility for patching, configuration, and monitoring of the operating systems and applications in Cloud.

117 See Reg. SCI Addendum, Section 4 *Briefing Meetings*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

(1) Internal Risk Assessments

As part of their existing third-party vendor risk activities, the Clearing Agencies' Third-Party Risk department ("TPR") would assess the operational risks of the CSP as a critical vendor annually.[118] [119] [120] Additionally, as a critical vendor, the CSP is subject to heightened risk management requirements, as defined in the DTCC Third Party Risk CriticalPlus Program Procedures,[121] which include an executive sponsor that must be at the Managing Director level or higher, documented annual meetings, quarterly reporting, and monthly notifications. Issues rated moderate or above, negative news, performance

---

118 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Third Party Risk Governance & Monitoring Procedures, which describes the minimum requirements for practices and standards to be used by business owners to monitor and manage third party relationships for DTCC and its subsidiaries. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

119 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Third Party Risk Policy and the DTCC Third Party Risk Procedures, which establish the standards and practices to be used by certain business line departments and/or functional units to manage the potential risks associated with engaging with an external service provider. The Clearing Agencies have provided these documents in confidential Exhibit 3 to this advance notice filing.

120 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the Third Party Risk – Technology and Resilience Procedure, which supplements the "DTCC Third Party Risk Policy", "DTCC Third Party Risk Procedures", and "DTCC Third Party Risk Governance and Monitoring Procedures" and covers the following: standard technology risk assessments (e.g., due diligence), fourth party reviews, NYDFS cyber security assessments, and onsite assessments. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

121 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the DTCC Third Party Risk CriticalPlus Program Procedures. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

concerns or remediations are directly escalated to the Management Risk Committee monthly.[122]

(2) Internal Audit Department

As mentioned in Section II.B.ii.4.(a), above, the Clearing Agencies' IAD, as the third line of defense, is independent from the Clearing Agencies' business lines, support areas, and controls functions, and promotes resiliency and security through the assessment of risk management and control frameworks to raise awareness of control risks and changes for improving controls and governance processes.

IAD assesses the risks of the Clearing Agencies, at least annually, as part of the development of the risk-based audit plan, which is reviewed and refreshed, as needed, on a quarterly basis.[123] The development of the audit plan includes the consideration of IADs risk assessment results, which informs cycle coverage requirements for Cloud. Additional considerations include, but are not limited to, regulatory requirements and expectations, initiatives, and institutional and industry risk trends, including risks associated with technology and cloud-based processes.

IAD's specific reviews of Cloud Infrastructure have not identified any material deficiencies and the scope of the reviews have included, but are not limited to, consideration of governance and oversight, contagion risk and logical separation, access management, security configuration and monitoring, concentration risk, exit strategy, business continuity and disaster recovery. IAD also has assessed the design of controls

---

122 Supra note 62.

123 Supra note 81.

for a cloud platform scheduled for use in 2024 and is proposing a Cloud Security audit for 2024.[124]

(3) Key Risk and Key Performance Indicators[125]

The Clearing Agencies have established processes to evaluate the Clearing Agencies' management of CSPs. Cloud vendors are rated through a quarterly TPR survey. If a survey results in a poor rating, then it is reported to the Management Risk Committee ("MRC").[126] TPR is responsible for the timely reporting and escalation of third-party risks. On a regular basis, TPR will review all active assessments to identify any high risks or potential issues that may require further discussion or escalation to senior management, Corporate Procurement Services ("CPS"), or internal stakeholders. The DTCC Third Party Risk Procedures provide a list of events that must be presented to the MRC.[127]

The Clearing Agencies have developed key performance indicators ("KPIs") for Cloud and socialized these KPIs internally. The KRIs already exist for Core C&S Systems and are aligned to overall systems availability, capacity, data integrity, and security.[128] The CSP KPIs would feed into existing KRIs and would be used to evaluate

---

124 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the Clearing Agencies' Cloud Platform Internal Audit Report. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

125 Supra note 62.

126 Supra note 119.

127 Supra note 78.

128 The Clearing Agencies have separately submitted a request for confidential treatment to the Commission regarding the IT-Q4 2023 Risk Tolerance. The

the CSP's performance after Cloud implementation. KPIs would be added to monitor the performance and risks of the CSP services for which the Clearing Agencies have contracted. These post-Cloud implementation KRIs and KPIs would allow the Clearing Agencies to assess their ongoing use of the CSP against their operational and security requirements and would help demonstrate the effectiveness of risk controls and the CSP's performance against commitments in the SLAs, and will be reported on a regular basis to the Clearing Agencies' Management Committee, Board of Directors, and Technology and Risk Committees of the Board of Directors.

(4) Auditing the CSP and Access Rights[129]

The CSP hosts an annual Audit Symposium. The Cloud Agreement gives the Clearing Agencies the right to attend the symposium so that the Clearing Agencies may inspect and verify evidence of the design and effectiveness of the CSP's control environment.[130] The CSP also hosts an annual Cloud security conference focused on security, governance, risk and compliance, which the Clearing Agencies would attend. Through preparation for and attendance at these events, the Clearing Agencies could provide feedback and make requests of the CSP for future modifications of its control environment.

Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

129 Supra note 62.

130 See Reg. SCI Addendum, Section 3 *Customer Right of Access and Audit*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

The Clearing Agencies' Information Technology staff currently meets with CSP representatives weekly to focus on technical issues related to the Clearing Agencies' proposed Cloud environment. As required under the Cloud Agreement, the Clearing Agencies hold quarterly compliance briefings with the CSP, wherein the Clearing Agencies receive information, including any necessary documentation, from the CSP to help assure the Clearing Agencies that the CSP is meeting its obligations.[131] The information provided includes updates to services and SLAs, CSP performance, and details that help the Clearing Agencies meet their reporting obligations under Section 1003(a)(1) of Reg. SCI. The Clearing Agencies' management, including Security, Information Technology, TPR, and the Internal Audit Department, coordinate to ensure appropriate representation during such briefings. The CSP is required under Cloud Agreement to maintain records showing its compliance with the agreements for a period of five years.[132]

The CSP would be required to maintain an information security program, including controls and certifications, that is as protective as the program evidenced by the CSP's SOC-2 report. The CSP must make available on demand to the Clearing Agencies its SOC-2 report as well as the CSP's other certifications from accreditation bodies and information on its alignment with various frameworks, including NIST-CSF, and ISO.[133]

---

131 Supra note 117.

132 See Reg. SCI Addendum, Section 7.3 *CSP Records*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

133 The FFIEC Guidance provides that the Clearing Agencies may obtain SOC reports, other independent audits, or ISO certification reports to gain assurance that the CSP's controls are operating effectively. See FFIEC, Security in a Cloud Computing Environment, at 7. The Clearing Agencies review the CSP's SOC-2 on an annual basis. See Reg. SCI Addendum, Section 2 *CSP Information Security*

As part of the annual risk assessment of the CSP, TPR collects risk and control related assurance documents from the CSP and coordinates review with the Clearing Agencies' respective subject matters specialists. TPR, Security, and Business Continuity would determine the adequacy and reasonableness of the documentation received to complete the Third-Party Risk Assessment. Finally, the Cloud Agreement provides that the Clearing Agencies' and their regulators may visit the facilities of the CSP under specified conditions. TPR would help coordinate bi-annual visits of the data centers.[134]

The Clearing Agencies plan to use the CSP's services combined with additional third-party tools to monitor systems deployed by ingesting logs into a security incident and event monitoring tool to provide a "single pane of glass" view into the Cloud Infrastructure. When incidents are detected, the Clearing Agencies would follow their existing incident response governance to identify, detect, contain, eradicate, and recover from incidents.

III. Consistency with the Clearing Supervision Act

The stated purpose of the Clearing Supervision Act is to mitigate systemic risk in the financial system and promote financial stability by, among other things, promoting uniform risk management standards for systemically important financial market utilities

---

Program. The SOC reports, along with other artifacts showing compliance with these sections, are available to the Clearing Agencies on demand. In addition, during each Briefing Meeting (See Reg. SCI Addendum Section 4 *Briefing Meetings*), updates are provided on any material changes to certification standards, policies, procedures, controls or security standards at the CSP. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

134 See Reg. SCI Addendum, Sections 3 *Customer Right of Access and Audit* and 9 *Regulatory Supervision*. The Clearing Agencies have provided this document in confidential Exhibit 3 to this advance notice filing.

and strengthening the liquidity of systemically important financial market utilities.[135] Section 805(a)(2) of the Clearing Supervision Act[136] also authorizes the Commission to prescribe risk management standards for the payment, clearing and settlement activities of designated clearing entities, like the Clearing Agencies, for which the Commission is the supervisory agency. Section 805(b) of the Clearing Supervision Act[137] states that the objectives and principles for risk management standards prescribed under Section 805(a) shall be to:

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

The Commission adopted Rule 17ad-22 under Section 805(a)(2) of the Clearing Supervision Act and the Exchange Act in furtherance of these objectives and principles.[138] Rule 17ad-22 under the Exchange requires covered clearing agencies, like the Clearing Agencies, to establish, implement, maintain, and enforce written policies

---

135 12 U.S.C. 5461(b).

136 12 U.S.C. 5464(a)(2).

137 12 U.S.C. 5464(b).

138 17 CFR 240.17ad-22. Exchange Act Release Nos. 68080 (October 22, 2012), 77 FR 66220 (November 2, 2012) (S7-08-11) (Clearing Agency Standards); 78961 (September 28, 2016), 81 FR 70786 (October 13, 2016) (S7-03-14) (Standards for Covered Clearing Agencies).

and procedures that are reasonably designed to meet certain minimum requirements for their operations and risk management practices on an ongoing basis.[139]

The Clearing Agencies believe that the Cloud Proposal is consistent with Section 805(b)(1) of the Clearing Supervision Act[140] and the requirements of Rules 17ad-22(e)(17)(ii) under the Exchange Act.[141]

A. Consistency with Section 805(b)(1) of the Clearing Supervision Act

Promote Robust Risk Management. As described above, the Clearing Agencies believe that the Cloud Proposal promotes robust risk management, specifically operational risk management, by providing scalable and secure infrastructure for hosting Core C&S Systems. The Cloud Proposal would add additional security capabilities, allow for regular updates and maintenance of applications, and reduce the risk of data breaches while also ensuring compliance with industry standards. Additionally, transitioning to Cloud would offer flexibility in scaling resources, which can enable the Clearing Agencies to adapt quickly to changing security needs and allocate resources more efficiently.

Today, the Clearing Agencies' ability to risk manage extreme market events is directly tied to their ability to scale their on-premises resource during such events, which is directly tied to the Clearing Agencies having previously expended enough capital to build enough capacity based on earlier performance testing of their applications to

---

139 17 CFR 240.17ad-22.

140 12 U.S.C. 5464(b)(1).

141 17 CFR 240.17ad-22(e)(17)(ii).

withstand such extreme market events. Although the Clearing Agencies would continue to performance test their applications regardless of where the applications are hosted, by hosting the applications in Cloud, the number of scalable resources is already available, when needed, without the Clearing Agencies having to pre-purchase it or build it. This level of nearly unbounded, on-demand scalability provides a much-welcomed risk-management feature for extreme events, such as a global pandemic as noted above.

Overall, risk management is inherently strengthened by hosting in Cloud through advanced security features, real-time monitoring, on-demand scalability, and compliance standards implemented by the CSP. By leveraging these capabilities, the Clearing Agencies can better proactively identify and address risks, ensuring data integrity and regulatory compliance.

Promote Safety and Soundness. The Clearing Agencies also believe that the Cloud Proposal promotes safety and soundness. As discussed above, transitioning to Cloud provides centralized management and improved scalability. The CSP provides cloud-specific security capabilities, including encryption, access controls, and regular updates, reducing the risk of security breaches. Centralized monitoring allows for better visibility into potential threats, enabling quick response and mitigation. The agility afforded by Cloud would allow the Clearing Agencies to respond to performance challenges more efficiently and effectively. For instance, as noted above, in the face of unexpected surges in demand, Cloud scalability would allow the Clearing Agencies to seamlessly adjust resources, helping to prevent service disruptions and loss of operations. Such agility not only enhances the effectiveness of operations but also mitigates the risks associated with unexpected fluctuations in workload performance. These benefits improve the Clearing

Agencies abilities to maintain operational continuity and resilience, which help promote safety and soundness.

Reduce Systemic Risk. The Clearing Agencies also believe that the Cloud Proposal would reduce systemic risk by improving overall resilience and security. As described above, hosting Core C&S Systems in Cloud would provide distributed infrastructure and data redundancy (i.e., multiple availability zones, supported by many data centers, across two regions), making the systems less susceptible to single points of failure. Moreover, disaster recovery would be streamlined, minimizing the effect of potential disruptions, while automatic backup systems, geographic redundancy, and faster data recovery mechanisms would all contribute to a more resilient infrastructure. In the event of a localized issue, the distributed nature of Cloud would help prevent widespread disruptions.

Production resiliency also is greatly improved in Cloud compared to the Clearing Agencies' on-premises capabilities, where a single location hosts an application, on a single copy of primary storage. Instead, Cloud would host an application across three primary availability zones, made of up of many data centers, each of which contain actively running instances and synchronous copies of the data. If the Clearing Agencies' primary, on-premises data center fails, an out of region recovery will be necessary and will likely result in approximately two hours of downtime. By comparison, in Cloud, even if an entire availability zone fails (meaning the failure of multiple data centers), Core C&S Systems would continue to operate within the region, thus avoiding an out of region recovery and any downtime.

The Clearing Agencies would employ meaningful security capabilities and measures provided by the CSP and third-party tools to further enhance the security of the Clearing Agencies' Core C&S Systems. This approach to security would help reduce systemic risks associated with operational outages and significantly reduce the risk associated with data loss or downtime. Additionally, the Cloud environment facilitates regular updates and patch management, ensuring that security measures stay current. This proactive maintenance helps mitigate vulnerabilities that could otherwise contribute to systemic risk. Overall, the adoption of Cloud enhances the stability and security of IT infrastructure, contributing to a reduction in systemic risks.

Altogether, the Clearing Agencies believe that the benefits afford from operating in a Cloud Infrastructure would help the Clearing Agencies reduce systemic risk.

Support the Stability of the Broader Financial System. The Clearing Agencies believe that the Cloud Proposal supports the stability of the broader financial system by enhancing efficiency, resilience, and security of the Clearing Agencies' Core C&S Systems. Cloud services would provide the Clearing Agencies with scalable and flexible infrastructure, allowing for more efficient resource allocation and cost management, which supports operational resiliency and stability. With the ability to rapidly deploy new applications and services, the Clearing Agencies would become more agile in adapting to market trends and participant and customer needs.

In terms of resilience, the Cloud Infrastructure offers distributed data storage and failover solutions, reducing the impact of localized disruptions and improving recovery capabilities. This resilience is crucial for the Clearing Agencies' Core C&S Systems to continue functioning even in the face of unforeseen events. Moreover, the CSP's

strengthened security capabilities help protect sensitive data, mitigating the risk of cyberattack or data breaches that could undermine the stability of the financial system. Overall, the transition to Cloud fosters improved operational efficiency, resilience, and robust security practices, contributing to the stability of the broader financial system.

Accordingly, the proposed changes provided in this Cloud Proposal are consistent with (i) promoting robust risk management; (ii) promoting safety and soundness; (iii) reducing systemic risks; and (iv) promoting the stability of the broader financial system, all in support of the objectives and principles of Section 805(b) of the Clearing Supervision Act.[142]

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

Rule 17ad-22(e)(17)(ii) requires the Clearing Agencies to establish, implement, maintain, and enforce written policies and procedures reasonably designed to manage the Clearing Agencies' operational risk by "ensuring that systems have a high degree of security, resiliency, operational reliability, and adequate, scalable capacity."[143]

Security. As described above and in policies and procedures confidentially filed, the Clearing Agencies have established a robust Cloud security program to manage the security of the Core C&S Systems that would be running in Cloud and to monitor the CSP's management of security of the Cloud Infrastructure that it operates. Processes are

---

142 12 U.S.C. 5464(b).

143 17 CFR 240.17ad-22(e)(17)(ii). The Clearing Agencies maintain several policies specifically designed to manage the risks associated with maintaining adequate levels of system functionality, confidentiality, integrity, availability, capacity, and resiliency for systems that support core clearing, risk management, and data management services.

formally defined, automated to the fullest extent, repeatable with minimal variation, accessible, adhered to, and timely. The enterprise security program encompasses all of the Clearing Agencies' assets existing in the Clearing Agencies' offices, data centers, and within the Cloud Infrastructure, and IAM controls ensure least-privileged user access to applications in Cloud. The Clearing Agencies have appropriate controls in place to help ensure the security of confidential information in-transit between the Clearing Agencies' data centers and the Cloud Infrastructure, between systems within the Cloud Infrastructure, and at-rest. All network communications between the Clearing Agencies and Cloud would rely on industry standard encryption for traffic while in transit, and data at rest would be safeguarded through pervasive encryption. Finally, automated delivery of business and security capability via the use of the Infrastructure as Code, Cloud agnostic tools, and continuous integration/continuous deployment pipeline methods help ensure security controls are consistently and transparently deployed.

Resiliency and Operational Reliability. As stated above, resiliency and operational reliability of the Cloud Infrastructure is built into the system with functionality for the Clearing Agencies' Core C&S Systems to run in multiple availability zones within multiple regions. Regions are segregated from one another and are designed to minimize the possibility of a multi-region outage. The Clearing Agencies have designed their Cloud Infrastructure to have primary (hot)/secondary (warm) regions, at all times, ensuring Compute, Storage, and Network resources would be available in a new redundant region in the event of a primary region failure. As a result, the Cloud Infrastructure offers the Clearing Agencies multiple redundancies within which to run

Core C&S Systems, while simultaneously restricting the effect of an incident at the CSP to the smallest footprint possible.

Scalability. As described above, since additional computing power can be launched on demand, the scalability in a Cloud computing environment is considerable and instantaneous. The Clearing Agencies could provision or de-provision Compute, Storage, and Network resources to meet demand at any given point in time. In the current on-premises environment, immediate scalability is limited by the capacity of the on-premises hardware. Additional physical servers and network equipment would be needed to scale beyond the limits of the on-premises hardware, potentially affecting the ability to quickly adapt to evolving market conditions, including spikes in trading volume.

For these reasons, the Clearing Agencies believe that the Cloud Proposal would help ensure that the Clearing Agencies' systems have a high degree of security, resiliency, operational reliability, and adequate, scalable capacity, consistent with Rule 17ad-22(e)(17)(ii) under the Exchange Act.[144]

III. Date of Effectiveness of the Advance Notice, and Timing for Commission Action

The proposed change may be implemented if the Commission does not object to the proposed change within 60 days of the later of (i) the date that the proposed change was filed with the Commission or (ii) the date that any additional information requested by the Commission is received. The clearing agency shall not implement the proposed change if the Commission has any objection to the proposed change.

The Commission may extend the period for review by an additional 60 days if the proposed change raises novel or complex issues, subject to the Commission providing the

144 17 CFR 240.17ad-22(e)(17)(ii).

clearing agency with prompt written notice of the extension. A proposed change may be implemented in less than 60 days from the date the advance notice is filed, or the date further information requested by the Commission is received, if the Commission notifies the clearing agency in writing that it does not object to the proposed change and authorizes the clearing agency to implement the proposed change on an earlier date, subject to any conditions imposed by the Commission.

The clearing agency shall post notice on its website of proposed changes that are implemented.

IV. Solicitation of Comments

Interested persons are invited to submit written data, views and arguments concerning the foregoing, including whether the advance notice is consistent with the Clearing Supervision Act. Comments may be submitted by any of the following methods:

Electronic Comments:

- Use the Commission's Internet comment form (http://www.sec.gov/rules/sro.shtml); or
- Send an e-mail to rule-comments@sec.gov. Please include File Number SR-DTC-2024-801 on the subject line.

Paper Comments:

- Send paper comments in triplicate to Secretary, Securities and Exchange Commission, 100 F Street, NE, Washington, DC 20549.

All submissions should refer to File Number SR-DTC-2024-801. This file number should be included on the subject line if e-mail is used. To help the Commission process and review your comments more efficiently, please use only one method. The Commission

will post all comments on the Commission's Internet website (http://www.sec.gov/rules/sro.shtml). Copies of the submission, all subsequent amendments, all written statements with respect to the advance notice that are filed with the Commission, and all written communications relating to the advance notice between the Commission and any person, other than those that may be withheld from the public in accordance with the provisions of 5 U.S.C. 552, will be available for website viewing and printing in the Commission's Public Reference Room, 100 F Street, NE, Washington, DC 20549 on official business days between the hours of 10:00 a.m. and 3:00 p.m. Copies of the filing also will be available for inspection and copying at the principal office of DTC and on DTCC's website (dtcc.com/legal/sec-rule-filings). Do not include personal identifiable information in submissions; you should submit only information that you wish to make available publicly. We may redact in part or withhold entirely from publication submitted material that is obscene or subject to copyright protection. All submissions should refer to File Number SR-DTC-2024-801 and should be submitted on or before [insert date 21 days from publication in the Federal Register].

By the Commission.

Secretary

EXHIBIT 3

The information contained in this Exhibit 3 is subject to exemption from mandatory disclosure under Exemptions #4 and #8 of the Freedom of Information Act because the information concerns (i) trade secrets and commercial information that is privileged or confidential and (ii) the supervision of The Depository Trust Company, Fixed Income Clearing Corporation, and National Securities Clearing Corporation (collectively, the "Clearing Agencies"), which are financial institutions. This Exhibit 3 contains one or more electronic files embedded in a one-page document for filing efficiency, as listed below. The information contained in the embedded file or files is not intended for public disclosure. Accordingly, this Exhibit 3 has been redacted and confidential treatment requested pursuant to 17 CFR 240.24b-2. An unredacted version was filed separately and confidentially with the Securities and Exchange Commission. Notwithstanding the request for confidential treatment, the Clearing Agencies believe the substance of this Exhibit 3 is clearly and adequately described in the accompanying Exhibit 1A and Form 19b-4 narrative to the advance notice filing, thus allowing for meaningful public comment.

Embedded File(s):

1. Proposed Transition Schedule of Core C&S Systems to Move to Cloud; 1 page
2. Change Management Policy; 9 pages
3. Technology Capacity and Demand Assessment Policy; 8 pages
4. Clearing Agency Risk Management Framework; 19 pages
5. Whitepaper-1; 30 pages
6. Whitepaper-2; 17 pages
7. Enterprise Agreement with Attachments (Cloud Agreement and Amd. No. 1); 16 pages
8. Amendment No. 2 to Enterprise Agreement; 7 pages
9. Amendment No. 3 to Enterprise Agreement; 3 pages
10. Amendment No. 4 to Enterprise Agreement; 3 pages
11. Amendment No. 5 to Enterprise Agreement; 3 pages
12. Amendment No. 6 to Enterprise Agreement; 3 pages
13. Amendment No. 7 to Enterprise Agreement; 4 pages
14. Amendment No. 8 to Enterprise Agreement; 5 pages
15. Amendment No. 9 to Enterprise Agreement; 5 pages

16. DTCC Reg. SCI Addendum; 23 pages
17. DTCC Global Business Continuity and Resilience Policy; 9 pages
18. DTCC System Delivery Policy; 9 pages
19. IT Architecture Policy; 7 pages
20. New Initiatives Policy; 22 pages
21. OTR CS&TRM Procedure – Application Penetration Test; 15 pages
22. DTCC Information Security – Systems Acquisition Development and Maintenance Policy and Control Standards; 20 pages
23. DTCC Information Security – Communications and Operations Policy and Control Standards; 56 pages
24. SLA Compendium; 5 pages
25. DTCC Legal Review of Third Party Vendor Contracts Policy; 19 pages
26. DTCC Corporate Risk Management Policy; 118 pages
27. Operational Response Capabilities Matrix; 4 pages
28. Fedwire Funds Protracted Outage Procedures; 33 pages
29. OTR TRM Core Process Procedure – Security Configuration Violation Rules; 14 pages
30. DTCC Information Security – Information Security Management Policy and Control Standards; 15 pages
31. DTCC Information Security – Risk Management Policy and Control Standards; 16 pages
32. DTCC Third Party Risk Procedures; 64 pages
33. Enterprise Program Management Office Policy; 13 pages
34. Enterprise Program Management Office Procedure; 19 pages
35. Internal Audit Department Policies and Procedures; 97 pages
36. DTCC Information Security – Asset Security Policy and Control Standards; 36 pages
37. DTCC Information Security – Monitoring and Incident Management Policy and Control Standards; 18 pages
38. DTCC Information Security – Asset Access Control Policy and Standards; 43 pages

39. DTCC Data Risk Management Policy; 13 pages
40. DTCC Information Security – Public Key Infrastructure Policy and Control Standards; 39 pages
41. DTCC Third Party Risk Governance & Monitoring Procedures; 27 pages
42. Third Party Risk – Technology and Resilience Procedures; 11 pages
43. DTCC Third Party Risk Policy; 20 pages
44. DTCC Third Party Risk CriticalPlus Program Procedures; 15 pages
45. Internal Audit Report DTCC Cloud Platform; 12 pages
46. IT-Q4 2023 Risk Tolerance; 16 pages
47. Amendment to Private Pricing Addendum S3 Capacity; 3 pages
48. DTCC Information Security – Business Continuity Policy and Control Standards; 9 pages
49. Incident Management Policy; 6 pages
50. Mutual Nondisclosure Agreement; 2 pages
51. Clearing Agencies' Responses to SEC RFI Re Cloud Proposal; 19 pages
52. Failure Scenario(s) – SEC Advance Notice; spreadsheet file

PAGE REDACTED IN ITS ENTIRETY