SECURITIES AND EXCHANGE COMMISSION
(Release No. 34-96113; File No. SR-OCC-2021-802)

October 20, 2022

Self-Regulatory Organizations; The Options Clearing Corporation; Notice of Filing of Partial Amendments No. 1, 2, 3, and 4 and Notice of No Objection to Advance Notice, as Modified by Partial Amendments No. 1, 2, 3, and 4 Relating to OCC's Adoption of Cloud Infrastructure for New Clearing, Risk Management, and Data Management Applications

I. INTRODUCTION

On October 8, 2021, the Options Clearing Corporation ("OCC") filed with the Securities and Exchange Commission ("Commission") advance notice SR-OCC-2021-802 ("Advance Notice") pursuant to Section 806(e)(1) of Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act, entitled Payment, Clearing and Settlement Supervision Act of 2010 ("Clearing Supervision Act"),[1] and Rule 19b-4(n)(1)(i)[2] under the Securities Exchange Act of 1934 ("Exchange Act"),[3] in connection with a proposed adoption of third-party-hosted cloud infrastructure (also generally referred to as the "Cloud") for OCC's new clearing, risk management, and data management applications. On November 2, 2021, the Commission published notice of the Advance Notice in the Federal Register to solicit public comment and to extend the

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.

review period for the Advance Notice.[4] The Commission has received no comments regarding the changes proposed in the Advance Notice.

On November 16, 2021, OCC filed Partial Amendment No. 1 to the Advance Notice.[5] On December 13, 2021, OCC filed Partial Amendment No. 2 to the Advance Notice.[6] On July 1, 2022, OCC filed Partial Amendment No. 3 to the Advance Notice.[7] On September 12, 2022, OCC filed Partial Amendment No. 4 to the Advance Notice.[8]

---

4 Securities Exchange Act Release No. 93433 (Oct. 27, 2021), 86 FR 60503 (Nov. 2, 2021) (File No. SR-OCC-2021-802) ("Notice of Filing").

5 Partial Amendment No. 1 appended an Exhibit 2 to documents previously filed as part of the Advance Notice on October 8, 2021. The Exhibit 2 consists of a communication from OCC to its Clearing Members concerning the changes discussed in the Advance Notice. Partial Amendment No. 1 did not change the purpose of or basis for the Advance Notice.

6 Partial Amendment No. 2 replaced confidential Exhibits 3f and 3g previously filed as part of the Advance Notice on October 8, 2021 with revised confidential Exhibits 3f and 3g and added new confidential Exhibit 3gg to the Advance Notice. Exhibits 3f and 3gg are two of the documents that collectively comprise the agreement with the Cloud service provider ("CSP") and were updated as OCC further negotiated and modified the terms of that agreement. Exhibit 3g provides a summary of the terms and conditions of OCC's agreement with the CSP designed to enable OCC to comply with Regulation SCI. Partial Amendment No. 2 did not change the purpose of or basis for the Advance Notice.

7 Partial Amendment No. 3 replaced the revised confidential Exhibits 3f and 3g that were previously filed in connection with Partial Amendment No. 2 with further revised confidential Exhibits 3f and 3g and added new confidential Exhibit 3hh to the Advance Notice. Exhibit 3hh is a Gantt chart regarding OCC's Cloud transition plan. Partial Amendment No. 3 did not change the purpose of or basis for the Advance Notice.

8 Partial Amendment No. 4 again replaced confidential Exhibit 3f filed as part of the Advance Notice, as modified by Partial Amendments Nos. 2 and 3, with revised confidential Exhibit 3f. Partial Amendment No. 4 did not change the purpose of or basis for the Advance Notice.

On January 27, 2022, the Commission requested that OCC provide it with additional information regarding the Advance Notice, pursuant to Section 806(e)(1)(D) of the Clearing Supervision Act,[9] which tolled the Commission's period of review of the Advance Notice until 120 days[10] from the date the requested information was received by the Commission.[11] The Commission received OCC's response to the Commission's request for additional information on March 3, 2022.[12] On June 14, 2022, the Commission made a second request for OCC to provide additional information regarding the Advance Notice, which tolled the Commission's period of review of the Advance Notice until 120 days[13] from the date the requested information was received by the

---

9 12 U.S.C. 5465(e)(1)(D).

10 The Commission may extend the review period for an additional 60 days (to 120 days total) for proposed changes that raise novel or complex issues. See 12 U.S.C. 5465(e)(1)(H).

11 See 12 U.S.C. 5465(e)(1)(E)(ii) and (G)(ii); Memorandum from Office of Clearance and Settlement, Division of Trading and Markets, titled "Commission's Request for Additional Information" (Jan. 27, 2022), available at https://www.sec.gov/comments/sr-occ-2021-802/srocc2021802-20113044-265605.pdf.

12 See Memorandum from Office of Clearance and Settlement, Division of Trading and Markets, titled "Response to the Commission's Request for Additional Information" (Mar. 4, 2022), available at https://www.sec.gov/comments/sr-occ-2021-802/srocc2021802-20118637-271511.pdf.

13 See supra note 10.

Commission.[14] OCC responded to the request, and the Commission received the information on June 22, 2022.[15]

The Commission is publishing this notice to solicit comments on Partial Amendments No. 1, 2, 3, and 4 from interested persons and, for the reasons discussed below, is hereby providing notice of no objection to the Advance Notice.[16]

II. BACKGROUND[17]

OCC is the only clearing agency for standardized U.S. securities options listed on Commission-registered national securities exchanges ("listed options"). In addition to clearing and settling listed options, OCC serves other financial markets, including the commodity futures, commodity options, security futures, securities lending, and the over-the-counter options markets. Further, OCC provides central counterparty ("CCP") clearing services for all of these markets and performs critical functions in the clearance and settlement process. OCC's role as the sole CCP for these markets is operationally

---

14 See 12 U.S.C. 5465(e)(1)(E)(ii) and (G)(ii); Memorandum from Office of Clearance and Settlement, Division of Trading and Markets, titled "Commission's Second Request for Additional Information" (June 14, 2022), available at https://www.sec.gov/comments/sr-occ-2021-802/srocc2021802-20132534-303027.pdf.

15 See Memorandum from Office of Clearance and Settlement, Division of Trading and Markets, titled "Response to the Commission's Request for Additional Information" (June 23, 2022), available at https://www.sec.gov/comments/sr-occ-2021-802/srocc2021802-20138832-308537.pdf.

16 References to the Advance Notice from this point forward refer to the Advance Notice as modified by Partial Amendments Nos. 1, 2, 3, and 4.

17 Capitalized terms used but not defined herein have the meanings specified in OCC's Rules and By-Laws, available at https://www.theocc.com/about/publications/bylaws.jsp.

complex and makes OCC an integral part of the national system for clearance and settlement.

The current iterations of OCC's core clearing, risk management, and data management applications ("ENCORE") were launched in 2000 and designed to operate in on-premises data centers.[18] As part of a larger technology initiative it calls "Renaissance," OCC now proposes essentially to migrate ENCORE's functions to the virtual equivalent of a traditional on-premises data center (a "Virtual Private Cloud") hosted by a third party CSP by utilizing Cloud-based hardware and systems software instead of its current on-premises hardware and systems software. OCC refers to the migration of ENCORE's functionality to a Virtual Private Cloud as the adoption of a "Cloud Infrastructure." OCC's proposed adoption of a Cloud Infrastructure would offer more resiliency,[19] security, and scalability than OCC's current on-premises infrastructure, in part, because the on-premises data centers require the acquisition and installation of additional hardware and systems software to accommodate scaled resources or new applications, while the Virtual Private Cloud does not. Although OCC is not proposing changes to ENCORE's *functionality* at this time (only to migrate that functionality to a Virtual Private Cloud, utilizing cloud-based hardware and systems

---

18 See Notice of Filing, 86 FR at 60504. ENCORE receives trade and post-trade data from various sources on a transaction-by-transaction basis; maintains clearing member positions; calculates margin and clearing fund requirements; and provides reporting to OCC staff, regulators, and clearing members.

19 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).

software), OCC's goal is to eventually retire ENCORE and implement new, improved clearing, risk management, and data management applications to replace ENCORE. In part because of the improved resiliency, security, and scalability noted above, the adoption of Cloud Infrastructure is a necessary building block for that goal.

The proposed migration of ENCORE's functions to a Virtual Private Cloud would include scalable resources that would: (i) handle various computationally intensive applications with load-balancing and resource management ("Compute"); (ii) provide configurable storage ("Storage"); and (iii) host network resources and services ("Network"). At the same time, reliance on a single CSP for OCC's core clearing, risk management, and data management applications also introduces certain risks. To mitigate those risks, OCC also proposes to retain a physical on-premises data center as a backup to the primary Cloud system, which would be utilized in the unlikely event of a multi-region outage of the Compute, Storage, and Network services at the CSP that affect OCC operations. Taken together, the move to a Cloud Infrastructure combined with the proposed backup on-premises data center would affect various aspects of OCC's operations including (i) resiliency, (ii) security, and (iii) scalability while mitigating one of the primary risks associated with relying on a single CSP. The move to a Cloud Infrastructure also would introduce additional risks associated with a migration to a Cloud Infrastructure, which OCC has identified and addressed through various controls, mitigation efforts, and policies and procedures. A summary of each of these aspects of OCC's operations, as well as the primary attendant risks associated with the proposed migration to a Cloud Infrastructure, is provided below.

A. Resiliency

OCC currently operates ENCORE in two on-premises data centers located in Texas and Illinois. OCC proposes to provision Compute, Storage, and Network resources in two separate, logically isolated Virtual Private Clouds that are capable of operating autonomously from each other and are located in geographically diverse regions.[20] Specifically, OCC would operate in three availability zones within each region, effectively providing for six levels of redundancy within a Cloud Infrastructure. The two Virtual Private Clouds would run in a "hot/warm" configuration. The "hot" Virtual Private Cloud would be operational and accept data traffic, while the "warm" Virtual Private Cloud would have applications on stand-by while simultaneously receiving the same incoming data and receiving replicated data from the "hot" Virtual Private Cloud. OCC believes that this proposed systems architecture would significantly reduce operational complexity, mitigate the risk of human error, and provide increased resiliency and assured capacity.[21]

In addition to the Virtual Private Clouds, OCC would operate an on-premises backup data center that would be separate from the Cloud Infrastructure. Like the "warm" Virtual Private Cloud, the on-premises data center would receive the same

---

[20] In this context, "separate" refers to the physical separation of the hardware housing the Virtual Private Clouds. "Logically isolated" is a similar concept from a network perspective, where the Virtual Private Clouds are virtually "separated" from each other on the network. The purpose of physically and logically separating the Virtual Private Clouds is to minimize the degree to which one event could impair both Clouds at the same time. This is similar to the concept of locating OCC's current data centers far enough apart that a natural or manmade disaster affecting one data center is unlikely to affect the other.

[21] Notice of Filing, 86 FR at 60505.

incoming data and replicated data from the "hot" Virtual Private Cloud. The on-premises data center would provide continuity of operations in the event that OCC loses access to its Cloud Infrastructure. For example, OCC might rely on the on-premises data center to maintain continuity of services in response to either a brief operational disruption of OCC's Virtual Private Clouds or a longer outage resulting from termination of OCC's relationship with the CSP.[22]

B. Security

OCC has developed a Cloud security program to allow OCC to manage the security of the core applications that would run on the Cloud Infrastructure. OCC's Cloud security program also would provide OCC with tools to assess and monitor the CSP's management of the Cloud Infrastructure's security.[23] As described below, the proposed Cloud security program focuses on four elements: (i) access controls; (ii) data governance; (iii) configuration management; and (iv) testing.

---

22 In the Notice of Filing, OCC specifically addresses the potential risk of its CSP terminating its relationship with OCC. See id. at 60511. The CSP may not unilaterally terminate the relationship with OCC absent good cause or without sufficient notice to allow OCC to transition to an alternate CSP or to the on-premises solution for its Compute, Storage, and Network needs. In the additional information it provided on March 3, 2022, OCC represents that, in the event the CSP ceases to support OCC's proposed Cloud Infrastructure, the on-premises data center would be capable of independently operating OCC's core clearing, risk management, and data management applications until such time as OCC is able to implement a new Cloud Infrastructure with another CSP.

23 OCC is not proposing to change or remove its current physical and cyber security standards, which OCC states are designed to align with the National Institute of Standards and Technology ("NIST"), Cyber Security Framework, and Center for Internet Security benchmarks. See Notice of Filing, 86 FR at 60505.

OCC is also proposing to implement tools provided by the CSP and selected third parties that are not currently available for use in OCC's on-premises data centers.[24]

1. *Access Controls*

OCC proposes to enforce a strict separation of duties and least-privileged access[25] for infrastructure, applications, and data to protect the confidentiality, availability, and integrity of the data. Using third-party tools, OCC would automate appropriate role-based access to the core applications running in the Cloud. For the on-premises data center, OCC would implement additional risk management measures. Specifically, OCC would explicitly set up the infrastructure for all connectivity to and from the on-premises data center and rely on heavily monitored "jump hosts" (e.g., data feeds in and out, mechanisms for the delivery of the software, and a minimum management interface that requires multi-factor authentication for access). OCC would also limit access to approved users of the on-premises data center via dedicated private circuits.

2. *Data Governance*

OCC's Enterprise Security Standards describe the data governance framework applicable to OCC's proposed Cloud Infrastructure, such as data moving between

---

[24] For example, OCC intends to implement Cloud security capabilities designed to automate and standardize how OCC deploys and monitors IT system configurations as well as how OCC encrypts data. The proposed Cloud Infrastructure would also allow OCC to take advantage of services for setting up credentials and end-to-end configuration change management and scanning.

[25] "Least-privileged access" means users will have only the permissions needed to perform their work, and no more.

systems within the Cloud.[26] For example, the Enterprise Security Standards require any system related to the Cloud Infrastructure to: (i) store data and information in the United States throughout its lifecycle; (ii) be able to retrieve and access the data and information throughout its lifecycle; (iii) encrypt data in the Cloud with key pairs kept and owned by OCC; (iv) comply with United States federal and applicable state data regulations regarding data location; and (v) enable secure disposition of non-records. Other OCC policies, such as its existing Information Classification and Handling Policy,[27] establish the overall data governance framework applied to the management, use, and governance of OCC information accessed, stored, or transmitted through the Cloud Infrastructure.

3. *Configuration Management*

To improve configuration management, OCC proposes to rely on pre-established system configurations, specifically the use of automated delivery of business and security capability via "Infrastructure as Code,"[28] to consistently and transparently deploy security controls on demand. OCC would also employ continuous configuration monitoring and periodic vulnerability scanning. Further, OCC would perform regular reviews and testing of its systems running in the Cloud while also relying on regular

---

26 OCC provided its Enterprise Security Standards in a confidential exhibit to File No. SR-OCC-2021-802.

27 OCC provided its Information Classification and Handling Policy in a confidential exhibit to File No. SR-OCC-2021-802.

28 "Infrastructure as Code" is the process of managing and setting up computer data centers through machine-readable definition files, rather than through physical hardware configuration or interactive configuration tools.

reviews and testing reports provided by the CSP.[29] OCC also proposes to use third-party solutions and CSP tools to track metrics, monitor log files, set alarms, and act on changes to OCC's core applications and the environment in which they operate.

4. *Testing*

OCC proposes the use of various security testing techniques for the Cloud Infrastructure. Through a risk-based analysis, an OCC team dedicated to security testing would determine what types of security testing techniques are appropriate for new assets and applications. Such techniques include automated security testing;[30] manual penetration testing;[31] and Blue Team testing.[32] OCC would employ processes for managing and remediating the results of its security testing.

Moving to a third-party-hosted Cloud infrastructure does present the risk that OCC would be overly reliant on the CSP to provide test results reliably and consistently. However, as indicated in confidential information provided by OCC, the CSP agreement

---

29 As confidential exhibits to File No. SR-OCC-2021-802, OCC provided documents governing the CSP's obligations to provide such information to OCC. See supra note 6.

30 Automated security testing uses industry standard security testing tools and/or other security engineering techniques specifically configured for each test.

31 Manual penetration testing uses information gathered from automated testing or other sources to identify vulnerabilities and deliver payloads with the intent to break, change, or gain access to the unauthorized area within a system.

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

provides assurances that the CSP would provide OCC with test cases, test planning, and auditable evidence of testing execution, including test results.[33] These test results would allow OCC to work with the CSP to make any changes, as needed, to rectify any technical issues that arise. Additionally, the CSP agreement includes provisions related to business continuity testing and intrusion reporting to facilitate the flow of security information to OCC.

C. Scalability

OCC's proposal to migrate from their current on-premises infrastructure to the Cloud represents a tradeoff in risk management. Accommodating scaled resources or new applications in OCC's current on-premises data centers would require OCC to acquire and install additional hardware and software. The availability of on-demand scaling in a Virtual Private Cloud could present a risk if OCC were not to receive resources from the CSP when requested. However, based on the confidential information provided by OCC in connection with the Advance Notice, OCC will contract with the CSP for at least as much capacity as it maintains in its current on-premises facilities, as well as for a plan to provide additional capacity.

Increasing the capability of OCC's current on-premises data centers, which are designed to handle a capacity in excess of prior peak transaction volumes, would require the acquisition and installation of additional hardware and software. In contrast, operating in a Cloud Infrastructure would allow OCC to quickly provision or de-provision Compute, Storage, or Network resources to meet demands, including elevated

---

[33] As confidential exhibits to File No. SR-OCC-2021-802, OCC provided documents governing the CSP's obligations to provide such information to OCC. See supra note 6.

trade volumes. Moving to a third-party-hosted Cloud Infrastructure does present a novel risk: that the CSP does not deliver the additional capacity that OCC might need at a moment's notice. However, OCC asserts that the fact that it will contract with the CSP for at least as much capacity as OCC currently maintains in its current on-premises facilities, combined with the CSP's contractual obligation to provide additional capacity to OCC on demand, would mitigate this risk significantly.[34]

The Cloud Infrastructure would also provide more flexibility for OCC to model and create development and test environments for backtesting and stress testing, as well as other systems development needs because of OCC's ability to increase capacity on demand under the express terms of the contract with the CSP. OCC also states that the increased scalability of the Cloud Infrastructure would allow OCC to run certain backtesting processes at a fraction of the time currently required.[35]

III. DISCUSSION AND NOTICE OF NO OBJECTION

Although the Clearing Supervision Act does not specify a standard of review for an advance notice, the stated purpose of the Clearing Supervision Act is instructive: to mitigate systemic risk in the financial system and promote financial stability by, among other things, promoting uniform risk management standards for systemically important financial market utilities ("SIFMUs") and strengthening the liquidity of SIFMUs.[36]

---

34 As confidential exhibits to File No. SR-OCC-2021-802, OCC provided documents governing the CSP's obligations to provide capacity to OCC. See supra note 6.

35 See Notice of Filing, 86 FR at 60505.

36 See 12 U.S.C. 5461(b).

Section 805(a)(2) of the Clearing Supervision Act authorizes the Commission to prescribe regulations containing risk management standards for the payment, clearing, and settlement activities of designated clearing entities engaged in designated activities for which the Commission is the supervisory agency.[37] Section 805(b) of the Clearing Supervision Act provides the following objectives and principles for the Commission's risk management standards prescribed under Section 805(a):[38]

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

Section 805(c) provides, in addition, that the Commission's risk management standards may address such areas as risk management and default policies and procedures, among other areas.[39]

The Commission has adopted risk management standards under Section 805(a)(2) of the Clearing Supervision Act and Section 17A of the Exchange Act (the "Clearing Agency Rules").[40] The Clearing Agency Rules require, among other things, each

---

37 12 U.S.C. 5464(a)(2).

38 12 U.S.C. 5464(b).

39 12 U.S.C. 5464(c).

40 17 CFR 240.17Ad-22. See Exchange Act Release No. 68080 (Oct. 22, 2012), 77 FR 66220 (Nov. 2, 2012) (S7-08-11). See also Exchange Act Release No. 78961 (Sep. 28, 2016), 81 FR 70786, 70806 (Oct. 13, 2016) (S7–03–14) ("Covered Clearing Agency Standards"). OCC is a "covered clearing agency" as defined in Rule 17Ad-22(a)(5).

covered clearing agency to establish, implement, maintain, and enforce written policies and procedures that are reasonably designed to meet certain minimum requirements for its operations and risk management practices on an ongoing basis.[41] As such, it is appropriate for the Commission to review advance notices against the Clearing Agency Rules and the objectives and principles of these risk management standards as described in Section 805(b) of the Clearing Supervision Act. As discussed below, the Commission believes the changes proposed in the Advance Notice are consistent with the objectives and principles described in Section 805(b) of the Clearing Supervision Act,[42] and in the Clearing Agency Rules, in particular Rule 17Ad-22(e)(17)(ii).[43]

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

The Commission believes that the proposal contained in OCC's Advance Notice is consistent with the stated objectives and principles of Section 805(b) of the Clearing Supervision Act. Specifically, as discussed below, the Commission believes that the changes proposed in the Advance Notice are consistent with promoting robust risk management, promoting safety and soundness, reducing systemic risks, and supporting the stability of the broader financial system.[44]

The Commission believes that OCC's proposal to host its core clearing, risk management, and data management applications in a Cloud Infrastructure is consistent with robust risk management, specifically operational risk management, and the

---

41 17 CFR 240.17Ad-22.

42 12 U.S.C. 5464(b).

43 17 CFR 240.17Ad-22(e)(17)(ii).

44 12 U.S.C. 5464(b).

promotion of safety and soundness. The Commission believes that, when supported by the appropriate legal agreements and system configurations, OCC's proposed Cloud Infrastructure may provide opportunities for improvements in resiliency, security, and scalability compared to infrastructures in traditional, on-premises data centers. Based on a careful review of the complete record, including the confidential information provided by OCC, the Commission believes the proposed systems architecture—comprising of a virtual multi-zone Cloud Infrastructure, with an on-premises data center as a physical backup—would provide a level of security and resiliency to the OCC's applications beyond that provided by OCC's current on-premises-only infrastructure. The Commission further believes that the legal agreements underlying the relationship between OCC and the CSP are designed to support OCC's ability to comply with its regulatory obligations related to the management of operational risk. Additionally, the inclusion of an on-premises backup provides an additional layer of redundancy to mitigate the low-probability risk of a multi-region outage at a single CSP.

Moreover, the Commission believes that, to the extent the proposed changes are consistent with promoting OCC's robust risk management as well as safety and soundness, they are also consistent with supporting the stability of the broader financial system. OCC has been designated as a SIFMU, in part, because its failure or disruption could increase the risk of significant liquidity or credit problems spreading among financial institutions or markets.[45] The Commission believes that the proposed changes would support OCC's ability to continue providing services to the U.S. options markets

---

45 See Financial Stability Oversight Council ("FSOC") 2012 Annual Report, Appendix A, https://home.treasury.gov/system/files/261/here.pdf (last visited Feb. 17, 2022).

by establishing multiple backup systems across the proposed Cloud Infrastructure and an on-premises backup while also allowing OCC to quickly set up additional capacity or applications as necessary. OCC's continued operations would, in turn, help support the stability of the financial system by reducing the risk of significant operational problems spreading among market participants that rely on OCC's central role in the options market.

Accordingly, and for the reasons stated above, the Commission believes the changes proposed in the Advance Notice are consistent with Section 805(b) of the Clearing Supervision Act.[46]

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

Rule 17Ad-22(e)(17)(ii) under the Exchange Act requires that a covered clearing agency establish, implement, maintain, and enforce written policies and procedures reasonably designed to manage the covered clearing agency's operational risks by ensuring that systems have a high degree of security, resiliency, operational reliability, and adequate, scalable capacity.[47]

As described in Section II.A. above, OCC proposes to increase the resiliency of its systems by migrating from two on-premises data centers to two separate, logically isolated Virtual Private Clouds with an on-premises backup data center. As described in Section II.B. above, OCC proposes to expand its existing physical and cyber security program with a focus on: (i) access controls; (ii) data governance; (iii) configuration management; and (iv) testing, as well as the implementation of additional tools not

---

46 12 U.S.C. 5464(b).

47 17 CFR 240.17Ad-22(e)(17)(ii).

currently available for use in OCC's on-premises data centers. As described in Section II.C. above, operating in a Cloud Infrastructure would allow OCC to quickly scale resources to meet elevated trade volumes as well as run risk management processes, such as backtesting, more quickly than is currently possible.

Accordingly, the Commission believes that the changes proposed in the Advance Notice are consistent with Rule 17Ad-22(e)(17)(ii) under the Exchange Act.[48]

IV. CONCLUSION

IT IS THEREFORE NOTICED, pursuant to Section 806(e)(1)(I) of the Clearing Supervision Act, that the Commission DOES NOT OBJECT to Advance Notice (SR-OCC-2021-802), as modified by Partial Amendments No. 1, 2, 3, and 4 and that OCC is AUTHORIZED to implement the proposed change as of the date of this notice.

By the Commission.

J. Matthew DeLesDernier,

Deputy Secretary.

---

[48] Id.