SECURITIES AND EXCHANGE COMMISSION
(Release No. 34-93433; File No. SR-OCC-2021-802)

October 27, 2021

Self-Regulatory Organizations; The Options Clearing Corporation; Notice of Filing and Extension of Review Period of Advance Notice Relating to OCC's Adoption of Cloud Infrastructure for New Clearing, Risk Management, and Data Management Applications

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" or "Act"),[3] notice is hereby given that on October 8, 2021, the Options Clearing Corporation ("OCC") filed with the Securities and Exchange Commission ("SEC" or "Commission") an advance notice as described in Items I, II and III below, which Items have been prepared primarily by OCC. The Commission is publishing this notice to solicit comments on the advance notice from interested persons and to extend the review period of the advance notice.

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

This advance notice is submitted in connection with a proposed adoption of Cloud infrastructure for OCC's new clearing, risk management, and data management applications with an on-demand network of configurable information technology resources running on virtual infrastructure hosted by a third party. The proposed changes

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.

are described in detail in Item II below. All terms with initial capitalization not defined herein have the same meaning as set forth in OCC's By-Laws and Rules.[4]

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

In its filing with the Commission, OCC 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. OCC has prepared summaries, set forth in sections A and B below, of the most significant aspects of these statements.

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

Written comments were not and are not intended to be solicited with respect to the advance notice and none have been received. OCC will notify the Commission of any written comments received by OCC.

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

Description of the Proposed Change

OCC is proposing to adopt an on-demand network of configurable information technology resources running on infrastructure ("Cloud" or "Cloud Infrastructure") hosted by a third party ("Cloud Service Provider" or "CSP") to support OCC's new core clearing, risk management, and data management applications. OCC will provision logically isolated sections of the Cloud Infrastructure that will provide it with the virtual

[4] OCC's By-Laws and Rules can be found on OCC's public website: https://www.theocc.com/Company-Information/Documents-and-Archives/By-Laws-and-Rules.

equivalent of physical data center resources ("Virtual Private Cloud"),[5] including scalable resources that: (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"). Additionally, OCC will maintain an on-premises data center to enable OCC to support core clearing, risk management, and data management applications in the event of a multi-region outage of Compute, Storage, and Network services impacting OCC operations at the CSP.

Background

ENCORE, consisting of OCC's core clearing, risk management, and data management applications running in traditional data centers, was launched in 2000 and has operated as OCC's real-time processing engine receiving trade and post-trade data from a variety of sources on a transaction-by-transaction basis, maintaining clearing member positions, calculating margin and clearing fund requirements, and providing reporting to OCC staff, regulators, and clearing members. Two geographically diverse on-premises data centers located in Illinois and Texas house the Compute, Storage, and Network resources required to run all of these applications.[6]

---

5 The Virtual Private Cloud is the virtual equivalent of a traditional data center, albeit with the scalability benefits of the CSP's infrastructure. The Virtual Private Cloud will provide OCC with a dedicated and secure space within the Cloud for OCC to operate.

6 OCC is not proposing changes to these services in connection with this Advance Notice. As appropriate, OCC will file proposals related to processing enhancements contemplated by the new core clearing, risk management, and data management applications separately. See, e.g., Securities Exchange Act Release No. 88654 (Apr. 15, 2020), 85 FR 22197, 98 n.7 (Apr. 21, 2020) (File No. SR-OCC-2020-004) (stating that a proposed rule change was designed to help

As the platform running OCC's core applications for approximately twenty years, ENCORE has accommodated growth in average daily transaction volumes[7] and OCC has managed periods of extreme market volatility and stress, including during the 2007-2008 financial crisis and the COVID-19 global pandemic of 2020-21, without incident. Nevertheless, as ENCORE was designed to operate in traditional on-premises data centers that require the acquisition and installation of additional hardware and systems software to accommodate scaled resources or new applications, the resiliency and scalability of the current infrastructure is less flexible than that offered by Cloud Infrastructure. OCC's objective is the retirement of ENCORE and its replacement with a resilient solution that meets market participants' needs and the regulatory expectations of a systemically important financial market utility ("SIFMU"). Given advances in Cloud technology and information security since 2000, OCC's proposed adoption of Cloud Infrastructure will offer more resiliency, security, and scalability.

Proposed Changes

Proposed Cloud Infrastructure. Cloud implementation will enable OCC to leverage the Compute, Storage, and Network capabilities of a CSP, supplemented with compatible third-party vendor solutions, to maintain a modular architecture with delineated domains that will result in (i) improved resiliency, (ii) enhanced security, and

---

facilitate the ability to run OCC's current clearing system, known as ENCORE, in parallel with a new clearing system on which OCC is working).

7 As of September 30, 2021, approximately 38,846,212 contracts per day were processed through the clearing and risk applications on ENCORE, an increase of over 34.6% of daily contract volume for the same date of the prior year, which itself represented approximately a 50% increase of daily contract volume from the prior year.

(iii) increased scalability for OCC's new core clearing, risk management, and data management applications.[8] Additionally, OCC will maintain an on-premises data center to support core clearing, risk management, and data management services in the event of a multi-region outage at the CSP that impacts OCC operations.

i. Improved Resiliency

As a SIFMU, OCC must ensure core applications on the Cloud Infrastructure have resiliency and recovery capabilities commensurate with OCC's importance to the functioning of the US financial markets.[9] As explained in more detail below, OCC believes the Cloud Implementation will enhance the resiliency of OCC's core clearing, risk management, and data management applications by virtue of OCC's architectural design decisions and the Cloud's built-in redundancy, guarantee of persistent availability, and disciplined approach to deployment of Cloud Infrastructure. In particular, the Cloud Implementation will enhance OCC's ability to withstand and recover from adverse conditions by provisioning redundant Compute, Storage, and Network resources in three zones in each of two autonomous and geographically diverse regions. This will afford OCC six levels of redundancy in the Cloud with a primary and secondary Virtual Private Cloud running in a hot/warm configuration. The hot Virtual Private Cloud will be

---

8 OCC has separately submitted a request for confidential treatment to the Commission regarding a diagram that depicts the future state architecture following conclusion of the proposed Cloud Implementation, which OCC has provided in confidential Exhibit 3a to File No. SR-OCC-2021-802.

9 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).

operational and accepting traffic, while the warm Virtual Private Cloud will simultaneously receive the same incoming data and receive replicated data from the hot Virtual Private Cloud with applications on stand-by. This solution significantly reduces operational complexity, mitigates the risk of human error, and provides resiliency and assured capacity. Finally, the on-premises data center will operate as a separate, logically isolated backup to the six levels of redundancy provided for in the Cloud – a backup to backups. The on-premises data center will also simultaneously receive incoming data and the replicated data from the CSP hosted Virtual Private Clouds. The on-premises data center is intended to be used only in the unlikely and extraordinary event that OCC completely loses access to the CSP.

ii. Enhanced Security

The physical and cyber security standards that OCC has designed to align with the National Institute of Standards and Technology ("NIST"), Cyber Security Framework ("CSF"), and Center for Internet Security ("CIS") benchmarks will not change in the Cloud Infrastructure. OCC will add meaningful security capabilities and measures provided by the CSP and selected third-party tools to enhance the security of OCC's core clearing, risk management, and data management applications.[10] Given the scope of their service, CSPs leverage economies of scale and offer infrastructure and services with

---

[10] Examples of enhanced cloud security capabilities include automated infrastructure deployment that is monitored for change, creating a standardized baseline; default separation between SCI and non-SCI operating domains; and automated and ubiquitous encryption.

OCC has separately submitted a request for confidential treatment to the Commission regarding the Future State: CSP and On-Premises Security Architecture, which OCC has provided in confidential Exhibit 3b to File No. SR-OCC-2021-802.

specialized configuration, monitoring, prevention, detection, and response tools.[11] Furthermore, unique Cloud-specific capabilities, such as services for provisioning credentials and end-to-end configuration change management and scanning, will provide OCC enhanced levels of protection not available in traditional on-premises solutions. Finally, the on-premises data center will be physically isolated from other on-premises networks, such as the development network, with consistent controls and equivalent security tools to that of the Virtual Private Clouds. Specific security-based risks are examined in more detail below.

iii. Increased Scalability

The Cloud Implementation will allow for more scalability of Compute, Network, and Storage resources that support OCC's core clearing, risk management, and data management applications.[12] With a Cloud Infrastructure, OCC can quickly provision or de-provision Compute, Storage, or Network resources to meet demands, including elevated trade volumes, and provide more flexibility to model and create development and test environments for back testing and stress testing, as well as other systems

---

11 For example, CSPs generally build infrastructure capable of withstanding Distributed Denial of Service ("DDoS") attacks to far greater magnitudes than any one company can. In February 2020, one CSP stated that its infrastructure was targeted by and withstood a sustained DDoS attack of up to 2.3 terabytes per second.

12 OCC will continue to follow existing policies and procedures regarding capacity planning and change management. OCC periodically performs 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 technology and security leadership as input to performance management and investment planning.

development needs. For example, the CSP can support elastic workloads and scale dynamically without the need for OCC to procure, test, and install additional servers or other hardware. This means that OCC may increase Compute capacity in one or both regions where it operates via manual or automated processes for core clearing, risk management, and data management applications. The rapid deployment of Compute capacity will allow OCC to obtain access to resources far more quickly than with existing physical data centers. The efficiency gains from the increased scalability of the Cloud Infrastructure will allow OCC to run certain back testing processes at a fraction of the time currently required. These and additional efficiency gains are discussed in more detail below.

Implementation Timeframe

OCC expects to launch the new core clearing, risk management, and data management applications into production no earlier than April 1, 2024. The proposed timeline to launch includes several milestones, such as connectivity testing in the first quarter of 2023, external testing in the second quarter of 2023, and certification of readiness from clearing members and exchanges in the first quarter of 2024. OCC will communicate frequently with stakeholders during this timeframe and will confirm the production implementation date of the proposed launch by Information Memorandum posted to its public website at least eight weeks prior to implementation.[13]

---

[13] See, "Timeline to Launch," available at: https://www.theocc.com/Participant-Resources.

Anticipated Effect on and Management of Risk

Federal Financial Institutions Examination Council Cloud Computing Guidance

On April 30, 2020, the Federal Financial Institutions Examination Council ("FFIEC")[14] issued a joint statement to address the use of Cloud computing services and security risk management principles in the financial services sector ("FFIEC Guidance").[15] 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"). As discussed in the next section, the OCC is implementing practices for its proposed Cloud deployment consistent with this guidance.

- **Governance:** strategies for using Cloud computing services as part of the financial institution's information technology strategic plan and architecture.
- **Cloud Security Management:** (i) appropriate due diligence and ongoing oversight and monitoring of CSP's security; (ii) contractual responsibilities, capabilities, and restrictions for the financial institution and CSP; (iii) inventory process for systems and information assets residing in the Cloud; (iv) security configuration, provisioning, logging, and monitoring; (v)

---

14 The Council 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.

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

identity and access management ("IAM") and network controls; (vi) security controls for sensitive data; and (vii) information security awareness and training programs.

- **Change Management:** (i) change management and software development lifecycle processes and (ii) security and reliability of microservice[16] architecture.
- **Resiliency and Recovery:** (i) business resiliency and recovery capabilities and (ii) incident response capabilities.
- **Audit and Controls Assessment:** (i) regular testing of financial institution controls for critical systems; (ii) oversight and monitoring of CSP-managed controls; and (iii) oversight and monitoring of controls unique to Cloud computing services, including those related to (a) management of the virtual infrastructure; (b) use of containers in the Cloud Infrastructure; (c) use of managed security services for the Cloud Infrastructure; (d) consideration of interoperability and portability of data and services; and (e) data destruction or sanitization.

Governance

OCC's ongoing Cloud Implementation is a natural progression of its information technology strategy and aligns seamlessly with its overall corporate strategy. OCC's

---

16 OCC's use of microservices include specialized third-party applications and a set of containers that work together to compose an application. A container 'holds' both an application and all the elements the application needs to run properly, including system libraries, system settings, and other dependencies. See Application Container Security Guide, NIST SP 800-190.

information technology strategy fully supports OCC's corporate strategy to: (i) reinforce OCC's foundational capabilities and deliver effective and efficient services; (ii) deliver product and service enhancements that enable growth in OCC's core capabilities and provide capital efficiencies to market participants; and (iii) demonstrate thought leadership in the delivery of innovative solutions that provide long-term value and efficiencies for OCC and its stakeholders. The corporate strategy is fortified by six guiding principles: (i) operating solutions that deliver reliability, predictability, and integrity; (ii) designing efficiency into OCC processes through automation and near-frictionless capabilities; (iii) providing outcome-focused solutions; (iv) prioritizing collaboration and accountability within the information technology team; (v) ensuring protection for OCC, its clearing members, and the broader financial market; and (vi) incorporating a "continuous learning" mindset.

As a SIFMU and the only provider of clearance and settlement services for listed options in the US, it is vital that OCC's critical services remain continuously available with sufficient security measures in place to detect and defend against possible security threats. The Cloud Implementation will present OCC with an agile operating environment that can scale throughput to match workloads nearly instantaneously and that will enable OCC to build a "secure by design" pervasive security methodology that incorporates the NIST Cybersecurity Framework's functions, categories, and subcategories as a roadmap for Cloud security. Movement to an agile, Cloud-based operating environment further reinforces OCC's commitment to building in a comprehensive and adaptable risk-based security methodology instead of a traditional perimeter-centric model.

OCC's Cloud Implementation does not alter OCC's responsibility to maintain compliance with applicable regulations. Consistent with FFIEC Guidance, OCC's plan for Cloud Implementation supports OCC's ability to comply with the SEC's Regulation Systems, Compliance, and Integrity ("Reg SCI")[17] and the CFTC's Systems Safeguards.[18] Reg SCI imposes certain information security and incident reporting standards on OCC and requires OCC 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.[19] As the "SCI Entity," OCC remains solely responsible for meeting all Regulation SCI obligations.[20] Similarly, Systems Safeguards requires OCC to have cybersecurity programs with risk analysis and oversight that ensure automated systems are secure, reasonably reliable, and have adequate scalable capacity. Within its agreement with the CSP ("Cloud Agreement"), OCC has established obligations on the

---

17 17 CFR 242.1000 et seq.

18 17 CFR 39.18 et seq.

19 See 17 CFR 242.1001(a). SCI Systems are "all computer, network, electronic, technical, automated, or similar systems of, or operated by or on behalf of, an SCI entity that, with respect to securities, directly support trading, clearance and settlement, order routing, market data, market regulation, or market surveillance." Indirect SCI Systems are "systems of, or operated by or on behalf of, an SCI entity that, if breached, would be reasonably likely to pose a security threat to SCI systems."

20 References herein to "Shared Responsibility" conveys the responsibility of OCC and the CSP vis-à-vis each other from a business operations perspective and it not intended to suggest the CSP has taken on, or that OCC has relinquished, any of OCC's Reg SCI compliance requirements.

CSP to provide support for OCC's compliance with all applicable regulations.[21]

OCC believes the combination of the following provides OCC reasonable assurance that the proposed Cloud Implementation would enable OCC to continue to fully satisfy its Regulation SCI obligations: (i) the Cloud Agreement; (ii) CSP's compliance programs as described in its Whitepapers[22] and publicly available policies (e.g., its Penetration Testing Policy), user guides, and other documents; (iii) CSP's Service Level Agreements; (iv) CSP's Systems Organization Controls reports (e.g., SOC 1, SOC 2, SOC 3) and ISO certifications (e.g., ISO 27001); (v) CSP's size, scale, and ability to deploy extensive resources to protect and secure its facilities and services;[23] and (vi) CSP's commercial incentive to perform.

OCC and the CSP rely on the shared responsibility model, which differentiates

---

21 OCC has separately submitted a request for confidential treatment to the Commission regarding the Cloud Agreement. OCC has provided these documents in confidential Exhibit 3c to File No. SR-OCC-2021-802, confidential Exhibit 3d to File No. SR-OCC-2021-802, confidential Exhibit 3e to File No. SR-OCC-2021-802, and confidential Exhibit 3f to File No. SR-OCC-2021-802. Among other things, the Cloud Agreement sets forth the CSP's responsibility to maintain the hardware, software, networking, and facilities that run the Cloud services. See also the separately submitted Table of Reg SCI Provisions, confidential Exhibit 3g to File No. SR-OCC-2021-802 that provides a summary of the terms and conditions of the Cloud Agreement that OCC believes enables OCC to comply with Reg SCI.

22 OCC has separately submitted requests for confidential treatment to the Commission regarding two examples of CSP Whitepapers, which OCC has provided in confidential Exhibit 3h to File No. SR-OCC-2021-802 and confidential Exhibit 3i to File No. SR-OCC-2021-802.

23 The OCC has contracted to work with a top-tier CSP that provides Cloud hosting services to Fortune 500 companies and the U.S. Government, amongst many others.

between the security "of" the Cloud and security "in" the Cloud.[24] The CSP maintains sole responsibility and control over the security "of" the Cloud, and their customers are responsible for the security "in" the Cloud; i.e., security of hosted applications and data. Thus, OCC remains responsible for managing and maintaining the operating system and all applications, including security and patching, running in the Cloud. There is no primary/secondary relationship as each partner has a specific set of responsibilities which, when combined, address the entire risk space.

The CSP performs its own risk and vulnerability assessments of the CSP infrastructure on which OCC will run its core clearing, risk management, and data management applications. In published documentation and in meetings conducted with members of CSP's staff, 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. Per the CSP's documentation, results of these processes are reviewed weekly by

---

[24] References herein to "Shared Responsibility" conveys the responsibility of OCC and the CSP vis-à-vis each other from a business operations perspective and it not intended to suggest the CSP has taken on, or that OCC has relinquished, any of OCC's Reg SCI compliance requirements. See supra, footnote 20.

OCC has separately submitted a request for confidential treatment to the Commission regarding a diagram that provides a summary of the "shared responsibility" model between OCC and the CSP, which OCC has provided in confidential Exhibit 3j to File No. SR-OCC-2021-802.

the CSP CISO and the CEO with senior CSP leaders to discuss security and action plans.[25]

OCC has the responsibility to perform risk assessments and technical security testing, including control validation, penetration testing, and adversarial testing, of OCC applications running on the CSP. This includes testing of the application interface layer of some CSP provided services such as storage and key management. OCC's security testing model will remain as it is for the on-premises operations: the Security Engineering team will define security control requirements and validate their correct implementation on OCC systems and deployed core clearing, risk management, and data management applications; automated tools will be used to scan OCC application code and open source for security defects during the development process; and automated vulnerability management tools will conduct periodic scans of deployed software and devices to ensure that security patches and fixes are correctly implemented within required timelines.

As mentioned, OCC's testing includes assessing the configuration of CSP provided services: Security Services will work with Information Technology staff to ensure that CSP tools are configured to appropriately manage and mitigate potential sources of risk and will assess the effectiveness of those configurations. The OCC Red Team will operate freely "in the Cloud," attempting to subvert or circumvent controls;

---

[25] 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."

their testing will include probing of CSP provided services to look for weaknesses in OCC's deployment of those tools.

Security Services will routinely report test results to Enterprise Risk Management, appropriate functional Operations and Information Technology management, senior management, and the Board of Directors. Automated vulnerability scanning reports, source code analysis, and results of specific assessments will be risk-rated and assigned a priority for remediation in accordance with OCC policy.

Management and oversight of the Cloud Implementation follows standard governing principles for large information technology projects. OCC's Board of Directors has established a Technology Committee to assist the Board of Directors in overseeing OCC's information technology strategy and other company-wide operational capabilities. The Risk and Technology Committees are responsible for different aspects of the oversight of the Cloud Implementation. Information Technology and Security Services, in collaboration with Enterprise Risk Management, are responsible for the identification, management, monitoring, and reporting on the risks associated with the Cloud Implementation. To that end, management presents the Technology Committee (with copies to the Risk Committee and the Board of Directors) with reports on the status and progress of the Cloud Implementation on at least a quarterly basis. This report includes an overall risk and issue summary and an analysis of key risk indicators for the Cloud Implementation.[26] Finally, OCC's Internal Audit Department is responsible for

---

[26] OCC has separately submitted a request for confidential treatment to the Commission regarding an example of this Cloud Implementation risk report, which OCC has provided in confidential Exhibit 3k to File No. SR-OCC-2021-802.

auditing security controls and configurations, including those related to the Cloud, prior to OCC's planned Cloud Implementation. Starting in 2021 and going forward, the Internal Audit Annual Plan is designed to assess important elements of the new core clearing, risk management, and data management application roll-out. For example, the 2021 Audit Plan includes an audit on the Cloud Implementation. These audits will help assess OCC's readiness for the Cloud Implementation as discussed below, in "Audit and Controls Assessment."

Cloud Security Management

OCC has established a robust Cloud security program to both: (i) manage the security of the core clearing, risk management, and data management applications that will 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 designed to encompass all OCC assets existing in OCC offices, data centers, and within the CSP's Cloud Infrastructure. The security program is built upon enterprise security standards that establish requirements that apply to any technology system as well as any tool that provides technology services. The following paragraphs in this section describe elements of OCC's Cloud security management in the areas of: (i) network and IAM controls (e.g., 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,

---

OCC has also submitted a request for confidential treatment to the Commission regarding Risk Appetite Statements and Risk Tolerances for Cloud Services, which OCC has provided in confidential Exhibit 3l to File No. SR-OCC-2021-802.

provisioning, logging, and monitoring; and (iv) security testing.

i. Network and IAM Controls

OCC recognizes that robust network security configuration and IAM will provide reasonable assurance that users – including OCC employees, market participants, and service accounts for systems[27] – are granted least-privileged access[28] to the network, applications, and data. OCC will use third-party tools to automate appropriate role-based access to the core clearing, risk management, and data management applications running in the Cloud. By enforcing strict separation of duties and least-privileged access for infrastructure, applications, and data, OCC will protect the confidentiality, availability, and integrity of the data.

The maintenance of an on-premises backup data center necessitates additional network controls. The on-premises data center will be physically separate from networks supporting routine business functions, which will make the overall protection of the environment easier simply by eliminating connectivity other than for critical operations. OCC will explicitly provision all connectivity and will manage and mitigate risks through use of jump hosts that are heavily monitored (e.g., data feeds in and out, provisioned mechanisms for the delivery of the software, and a minimum management interface that requires multi-factor authentication for access). This connection model, coupled with limited access via dedicated private circuits, eliminates the most common threat exposures such as Internet connectivity and email. The default physical separation

---

[27] Service accounts are non-interactive accounts that permit application access to support activities such as monitoring, logging, or backup.

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

defined in the on-premises backup architecture will be overlaid with industry standard monitoring and blocking tools to ensure that lateral movement between SCI and non-SCI environments is controlled in accordance with the risk.

OCC has established IAM requirements that build upon the least-privileged model. As part of the IAM program, all users must be assigned an appropriate enterprise identification. Users will be granted access to systems via a standardized and auditable approval process. The user identifications and granted access will be managed through their full lifecycle from a centralized IAM system maintained and administered by OCC. Role-, attribute-, and context-based access controls will be used as defined by internal standards consistent with industry recommended practices to promote the principles of least-privileged access and separation of duties.

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

ii. Security Governance and Controls for Sensitive Data

OCC's data governance framework that applies to the Cloud Implementation is identified within the OCC Enterprise Security Standards.[29] The Enterprise Security

[29] OCC has separately submitted a request for confidential treatment to the Commission regarding the Enterprise Security Standards, which OCC has provided in confidential Exhibit 3m to File No. SR-OCC-2021-802. OCC

Standards address data moving between systems within the Cloud as well as data transiting and traversing both trusted and untrusted networks. For example, the Enterprise Security Standards require a system or Software as a Solution to: (i) store data and information, including all copies of data and information in the system, in the United States 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 OCC; (iv) comply with United States federal and applicable state data regulations regarding data location; and (v) enable secure disposition of non-records in accordance with OCC's Information Governance Policy.[30]

Furthermore, OCC policies establish the overall data governance framework applied to the management, use, and governance of OCC information to include digital instantiations, storage media, or whether the information is located, processed, stored, or transmitted on OCC's information systems and networks, public, private, or hybrid Cloud infrastructures, third-party data centers and data repositories, or Software-as-a-Service (SaaS) applications.[31] The Information Classification and Handling Policy classifies OCC's information into three categories. System owners of technology that enable classification and/or labeling of information are responsible for ensuring the correct

---

security controls and standards are created, published, and managed in accordance with applicable OCC policies.

30 OCC has separately submitted a request for confidential treatment to the Commission regarding the Information Governance Policy, which OCC has provided as confidential Exhibit 3n to File No. SR-OCC-2021-802.

31 OCC has separately submitted a request for confidential treatment to the Commission regarding the Information Classification and Handling Policy, which OCC has provided in confidential Exhibit 3o to File No. SR-OCC-2021-802.

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.

OCC will implement key components of a "zero trust" control environment, 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 and at rest. External connectivity to OCC systems hosted by the CSP will be provided as it is now, through dedicated private circuits or over encrypted tunnels through the Internet. These network links will also have additional security controls, including encryption during transmission and restrictions on network access to and from the Virtual Private Cloud. Additionally, OCC will use dedicated redundant private network connections between OCC data centers and the CSP infrastructure. OCC currently maintains two data centers and will do so in the future to provide redundant, geographically diverse connectivity for market participants. All network communications between OCC and the Cloud Infrastructure will rely on industry standard encryption for traffic while in transit. Data at rest will be safeguarded through pervasive encryption. OCC's Encryption Standards describe requirements for implementation of the minimum required strengths, encryption at rest, and cryptographic algorithms approved for use in cryptographic technology deployments across OCC.[32] All

[32] OCC has separately submitted a request for confidential treatment to the Commission regarding the Encryption Standards, which OCC has provided in confidential Exhibit 3p to File No. SR-OCC-2021-802.

OCC identifying data is encrypted in transit using industry standard methods. The Key Management Service ("KMS") Strategy dictates that all CSP endpoints support HTTPS for encrypting data in transit.[33] OCC also secures 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 (TLS) versions per OCC encryption standard. OCC will have exclusive control over the key management system; only OCC authorized users will be able to access that data. CSP systems and staff will not have access to the OCC certificate management and/or key management system.[34] OCC is 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, OCC follows: (i) existing security design and controls; (ii) Cloud-specific information security controls defined in "Enterprise Security Controls;" 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, COBIT, and the FFIEC Guidelines.

OCC uses third-party tools for CSP security compliance monitoring, security scanning, and reporting. Alerts and all API-level actions are gathered using both CSP

---

33 OCC has separately submitted a request for confidential treatment to the Commission regarding OCC Key Management Service (KMS) Strategy, which OCC has provided in confidential Exhibit 3q to File No. SR-OCC-2021-802.

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

provided and third-party monitoring tools. The CSP provided monitoring tool is 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 previously discussed, OCC uses 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 ("FIPS") 140-2 validated Host Security Modules (HSMs) in KMS protect the confidentiality and integrity of OCC customer keys.[35] Customer plaintext keys are never written to disk and only ever used in protected, volatile memory of the HSMs for the time needed to perform the customer's requested cryptographic operation. KMS keys are never transmitted outside of the Cloud regions in which they were created. Updates to the KMS HSM firmware are controlled by quorum-based access control[36] that is audited and reviewed by an independent group within the CSP. This tightly controlled deployment process minimizes the risk that the security properties of the service will be changed as new software, firmware, or hardware is introduced. With these security measures, only users granted access by OCC to the core clearing, risk management, or data management applications will be able to interact with the information contained therein.

---

35 The HSM is analogous to a safe that only OCC has knowledge of the combination and the ability to access the keys to locks stored within.

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

iii. 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 will permit security controls to be consistently and transparently deployed on-demand. OCC will provision Cloud Infrastructure using pre-established system configurations that are deployed through infrastructure as code, then scanned for compliance to secure baseline configuration standards. OCC also employs continuous configuration monitoring and periodic vulnerability scanning. OCC will continue to perform regular reviews and testing of OCC systems running on the Cloud while relying upon information provided by the CSP through the CSP's SOC2 and Audit Symposiums. Finally, configuration, security incident, and event monitoring will rely on a blend of CSP native and third-party solutions.

OCC also plans to use tools offered by the CSP and third-parties to monitor the core clearing, risk management, and data management applications run on the Cloud Infrastructure. OCC will track metrics, monitor log files, set alarms, and have the ability to act on changes to OCC core clearing, risk management, and data management applications and the environment in which they operate.[37] The CSP will provide a dashboard to reflect- general health (e.g., up/down status of a region) but will not give additional insights into performance of services and applications which run on those services. The OCC operated centralized logging system will provide for a single frame

[37] OCC has separately submitted a request for confidential treatment to the Commission regarding the Draft Cloud Provider Logging and Alerting Test Environment, which OCC has provided in confidential Exhibit 3r to File No. SR-OCC-2021-802.

of reference for log aggregation, access, and workflow management by ingesting the CSP's logs coming from native detective tools and OCC instrumented controls for logging, monitoring, and vulnerability management. This instrumentation will give OCC 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 OCC has in place, OCC will be able to integrate the availability and capacity management of Cloud into OCC's existing processes, whether hosted on the Cloud or running in the local on-premises backup, and respond to issues in a timely manner.

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

Security has implemented tools for the core clearing, risk management, and data management applications and back office environments that will be hosted at the CSP; notably, the IAM system, monitoring and Security Information and Event Management ("SIEM") systems, the workflow system of record for incident handling, KMS, and enterprise Data Loss Prevention ("DLP"). Most of these services can also be run on-premises in a fully Cloud-independent mode, and Security Services has identified potential alternatives for those that will be needed for isolated on-premises operations and cannot operate independently. All required technical controls deployed via or reliant on CSP services will be replaced or supplemented to ensure equivalent independent

operation of the on-premises backup.[38]

Finally, the CSP prioritizes assurance programs and certifications, underscoring its ability to comply with financial services regulations and standards and to provide OCC with a secure Cloud Infrastructure.[39]

iv. Security Testing and Verification by the 2nd and 3rd Line

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

For new assets and application (or code) releases, Security determines whether and what type of security testing is required through a risk-based analysis. If required, testing is conducted prior to implementation and 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, Security will 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, Security will manually test to identify

---

38 OCC has separately submitted a request for confidential treatment to the Commission regarding the Key Technologies, which OCC has provided in confidential Exhibit 3s to File No. SR-OCC-2021-802.

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

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 OCCs networks, systems, and SaaS solutions are as secure as possible before deploying to a production environment.

The results of Security controls testing are risk-rated and managed to remediation via the Security Observation Risk Tracking process.

Change Management

Consistent with FFIEC Guidance, OCC's use of the Cloud will have sufficient change management controls in place to effectively transition systems and information assets to the Cloud and will help ensure the security and reliability of microservices in the Cloud. OCC's enterprise software development lifecycle processes help ensure the same control environment for all OCC resources, irrespective of whether they reside in an on-premises environment or in the Cloud. OCC has established baselines for design inputs and control requirements and enforces workload isolation and segregation through a Virtual Private Cloud using existing Cloud native technical controls and added new tools. OCC also plans to use other specialized platform monitoring tools for logging, scanning of configuration, and systems process scanning. OCC also has oversight as a code owner for the OCC infrastructure security containers and will have final review and approval for

related changes and code merges before deployment of secure containers into production. Finally, OCC will 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, OCC will perform routine scans of Compute resources with the existing enterprise scanning tools. Any identified vulnerabilities will be reviewed for severity, prioritized, and logged for remediation tracking in upcoming development releases.

OCC will create a "user acceptance plan" prior to promoting code to production. This user acceptance plan will include tests of all major functions, processes, and interfacing systems, as well as security tests. Through acceptance tests, OCC users will be able to simulate complete application functionality of the live environment. The change will move to the next stage of the OCC delivery model only after satisfying the criteria for this phase.[40]

OCC plans to use microservices in its use of the Cloud. OCC has internal projects that will address change management of the various microservices. In particular, OCC runs a suite of supporting services that enable building, running, scaling, and monitoring of OCC's business applications in the Cloud in an automated, resilient, and secure manner. The application platform relies on various CSP and third-party tools for different components, including Infrastructure as a Service, Infrastructure as Code, CI/CD, Container as a Service, Continuous Delivery, and Platform Monitoring. For example, OCC will use a third-party tool for managing containers and a different third-

---

[40] The "user acceptance plan" represents only one aspect of the overall change management program at the OCC.

party tool for distributing containers and workloads to assist with platform automation. Security measures for planned production microservices are already incorporated within the overall security architecture and Enterprise Security Standards.[41]

With respect to software development in the Cloud, OCC has established a closed Virtual Private Cloud non-production environment that allows OCC to develop, test, and integrate new capabilities, including those related to security enhancements, while preventing direct external access to the development environment and tightly controlling on-premises access from OCC to the non-production environment. This OCC Virtual Private Cloud non-production environment (hosted in the Cloud) focuses on the foundational security, operations, and infrastructure requirements with the intent to take lessons learned to implement into future production. OCC developed and maintains a Cloud Reference Architecture that defines necessary capabilities and controls required to securely host core clearing, risk management, and data management applications on the CSP. The minimum foundational security requirements are 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. OCC maintains enterprise security requirements that provide structure for current and future development. As the Virtual Private Cloud environment is further developed and expanded, there is a comprehensive process to identify any incremental risks and develop

---

41 The minimal security control architecture reflects awareness of the need to consider data storage and management outside of containers, configuration management to prevent unintended container interactions, and routine monitoring and replacement of containers when appropriate.

and implement controls to manage and mitigate those risks.[42]

Resiliency and Recovery

As noted earlier, given OCC's role as a SIFMU, it is vital that OCC work to ensure operations moved to Cloud Infrastructure have appropriately robust resilience and recovery capabilities. Below is a discussion of how OCC has evaluated resiliency including: (i) the steps taken by OCC and the CSP to help ensure the persistent availability of Compute, Storage, and Network capabilities in the Cloud; (ii) the resiliency of the CSP's method for deploying updates to help ensure that consequences of incidents are limited to the fullest extent possible; (iii) the on-premises backup; and (iv) the use of "store and forward"[43] messaging technology.

i. Resiliency of the Cloud Infrastructure

OCC believes the Cloud Implementation will enhance the resiliency of OCC's core clearing, risk management, and data management applications by virtue of its built-in six levels of redundancy that will provide OCC with easy access to multiple zones within multiple and geographically diverse regions. The redundancy provided to OCC in the Cloud Infrastructure helps ensure that Compute, Storage, and Network resources will be available to OCC on a persistent basis.

OCC will provision Compute, Storage, and Network resources in two autonomous and geographically diverse regions, in a hot/warm configuration to increase resources on

---

42 OCC has separately submitted a request for confidential treatment to the Commission discussing the status of security projects which OCC has provided in confidential Exhibit 3t to File No. SR-OCC-2021-802.

43 "Store and forward" messaging refers to messaging technology that retains copies of messages until confirmation of receipt, thus limiting the likelihood of loss during transmission.

demand, maintained by the CSP. Each region will maintain independent and identical copies of all applications that are deployed by OCC, allowing OCC to transition its core clearing, risk management, and data management applications from one region to another seamlessly. Production workloads would be run across and shifted between regions regularly to protect OCC against disruptions from regionalized incidents. In the unlikely event that a region is temporarily disabled as a result of an extreme event, OCC would failover to run core clearing, risk management, and data management applications in the other region. This will necessarily require that both regions be maintained with full and expansion capacity. At any point, OCC will have active primary and standby instances of the core clearing, risk management, and data management applications that can be moved to any of the six instances (i.e. three zones in each of the two regions). This is analogous to having six physical data centers with primary and backup running out of any two instances at a given point in time.

Each region consists of three zones, each of which has a physical infrastructure with separate and dedicated connections to utility power, standalone backup power sources, independent mechanical services, and independent network connectivity. While not dependent on one another, zones are connected to one another with private fiber-optic networking, enabling the architecture of core clearing, risk management, and data management applications to automatically failover between zones without interruption. Since each zone can operate independently of one another but failover capability is near instantaneous, a loss of one zone will not affect operation in another zone; however, no core clearing, risk management, or data management application will be reliant on the functioning of a single zone. This structural framework offers OCC a wide expanse

within which to run its core clearing, risk management, and data management applications while simultaneously restricting the effect of an incident at the CSP to the smallest footprint possible.[44]

As core clearing, risk management, and data management applications will be deployed in a primary (hot) /secondary (warm) mode, each environment will be active, run the same software, and receive the same data, enabling a failover or switch from one region to another within two hours. Software and Infrastructure will be deployed via automated processes to ensure both are identical in each region.

Additional capacity will always be available to support the resiliency of OCC's core clearing, risk management, and data management applications by way of the six-way redundancy. OCC will continue to periodically test the CSP's capacity scaling features and failover capabilities to ensure adequate capacity is always available to OCC.[45]

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. The notice provision in the Cloud Agreement for terminations that are not for cause would give OCC sufficient

---

[44] 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. OCC's applications will run using data plane services; control plane services are used by the CSP to configure the environment. Resources and requests are further partitioned into cells, or multiple instantiations of a service that are isolated 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.

[45] OCC will 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.

time to consider and transition[46] its core clearing, risk management, and data management applications to another CSP or to its backup on-premises data center. Specifically, the CSP must provide notice OCC believes is sufficient to transition if it wishes to terminate the Cloud Agreement for convenience or if it wishes to terminate an individual CSP service offering on which OCC relies for all of its Cloud customers.[47]

The CSP is permitted to terminate the Cloud Agreement with shorter notice periods in the event of a critical breach or an uncured material breach of the Cloud Agreement. In the highly unlikely event that a critical breach or uncured material breach occurs, OCC would have sufficient notice to shift operations to the on-premises data center. 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 (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) and to establish a short period of time to resolve an aggrieved party's claim (often 30 days). This gives the parties time and incentive to address the problem without having to resort to termination. Critical breaches are material breaches: (i) for which OCC knew its behavior would cause a material breach (such as a willful violation of

---

46 The possible transition of core clearing, risk management, and data management applications either from the CSP back to an on-premises solution or to another CSP is discussed below.

47 The CSP 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 los [sic] of license rights related to third-party intellectual property rights. In this event, the CSP must provide reasonable notice to OCC of the termination of the individual service offering.

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. Even if the CSP notifies OCC of an alleged breach (material or critical), termination of services is not immediate.

OCC believes the risk of termination with a shorter notice period is mitigated by the following factors. In all cases of an alleged breach, the CSP must notify OCC in writing and provide time for OCC to cure the alleged breach ("Notice Period"). With respect to an alleged critical breach, OCC would use the Notice Period to attempt to cure the alleged critical breach while also preparing for a seamless transition to the on-premises data center. With respect to an alleged material breach, which requires the CSP to extend the Notice Period if OCC demonstrates a good faith effort to cure the alleged material breach, OCC would use the Notice Period to attempt to cure the alleged material breach while also preparing for a seamless transition to the on-premises data center. 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, however, OCC would have ample notice to shift operations to the on-premises data center to avoid a disruption to core clearing, risk management, and data management applications.

ii. Resiliency of the Deployment of Cloud Infrastructure Updates

The CSP will update the Cloud Infrastructure from time to time[48] using a conservative approach for update deployment that helps to ensure that any potential effects of possible incidents are contained to the greatest extent possible. The CSP

[48] OCC will continue to retain responsibility for patching, configuration, and monitoring of the operating systems and applications in the Cloud.

achieves this by: (i) fully automating the build and deployment process; and (ii) deploying services to production in a phased manner.

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

OCC will continue to meet regularly with staff of the CSP, in addition to formal quarterly Briefing Meetings with the CSP as described in the Reg SCI Addendum.[49] The informal discussions and quarterly Briefing Meetings will permit OCC to gather information in advance of the quarterly Systems Change report. Most reportable systems changes will continue to occur based on changes to Compute, Storage, Network, or applications controlled by OCC.

iii. Resiliency through the build out of an on-premises data center

OCC will maintain an on-premises data center to provide the ability to support core clearing, risk management, and data management applications in the unlikely and extraordinary event of either the termination of the Cloud Agreement for uncured breach or a multi-region outage at the CSP that simultaneously impacts OCC operations within all three zones in both regions.[50]

---

49 See confidential Exhibit 3f.

50 OCC, with the assistance of an external consultant, conducted an analysis of the benefits and risks of a multi-CSP infrastructure. The key findings indicated that a

OCC has designed the on-premises data center to operate 30 or more days to permit a smooth transition back to the Cloud (once the Cloud disruption is remediated) on a low volume day. From an architectural perspective, the on-premises data center is similar to adding a third CSP region with a single zone. While most technologies will remain the same with a failover to on-premises, there are several technologies that are only available at the CSP and for which alternative solutions must be devised. All equivalent on-premises core platform technologies that enable Compute, Network, and Storage will be operated by OCC with synchronous data replication between the Cloud and on-premises while member connectivity would remain unchanged.[51] OCC will ensure adequate capacity in the on-premises data center for up to two and a half times observed peak volume. If the circumstances that required OCC to rely on the on-premises data center persist beyond seven days, OCC would take steps necessary to enhance its Storage to enable seamless operation of the on-premises data center for longer than 30 days.

iv. Resiliency through the use of "store and forward" messaging technology

OCC has designed the architecture to ensure it is able to support zero message loss and a quick recovery time. To meet these requirements the architecture places a premium on data integrity and throughput over the latency of any one transaction. The established

---

multi-CSP infrastructure would not significant improver resiliency and could create additional risks, including: (i) increased functionality and delivery risks; (ii) increased operational and cybersecurity risks; (iii) human capital risks; (iv) third-party and legal risks; and (v) general business risks.

51 OCC has separately submitted a request for confidential treatment to the Commission for a diagram that the presents draft Failover Architecture which OCC has provided in confidential Exhibit 3u to File No. SR-OCC-2021-802.

techniques for this are “store and forward” messaging technology where messages are preserved until delivered to servers that consume the messages and synchronous writes to multiple servers. Unlike OCC’s current system, the core clearing, risk management, and data management applications do not rely on block storage replication across CSP regions. The solution is entirely message based and message replication achieves the data redundancy required to deliver high availability services.

OCC will continue to rely on the existing “store and forward” messaging technology as the primary technology for exchanging messages with both exchanges & clearing members for the intake of clearing and settlement related information. The “store and forward” messaging technology manager is hosted on-premises and is replicated across all OCC on-premises data centers. The “store and forward” messaging technology will then forward messages to the hot/warm instances at the CSP and the redundant on-premises data center applications.

Core clearing, risk management, and data management applications rely on a platform for managing containerized workloads and messaging services. This platform enables multi-region message replication with synchronous acknowledgement. The platform will treat the on-premises data center as another region, with messages being replicated to all three regions (the two Cloud regions and on-premises).

The core clearing, risk management, and data management application architecture deployed across the two CSP regions and on-premises will maximize data integrity and throughput during routine operations and enhance failover should it be necessary.

Audit and Controls Assessment

OCC has a plan in place to continually test the Cloud security controls and OCC's readiness for the Cloud Implementation, and also has processes in place to regularly audit and test security controls and configurations,[52] including by monitoring the CSP's technical, administrative, and physical security controls that support OCC's systems in the Cloud Infrastructure.

i. Internal Risk Assessments

In addition to existing OCC Third Party Vendor Risk Management activities, OCCs Third Party Risk Management department ("TPRM") will assess the operational risks of the CSP as a critical vendor annually. Additionally, OCC conducts a technology risk assessment, which is an evaluation of risks to OCC's critical systems, monitoring of key risk indicators ("KRI"), risk events, security events, and key controls, and which will encompass all risks presented by the CSP, on an annual basis.[53]

ii. External Risk Assessment

OCC engaged a third-party familiar with Cloud Infrastructure best practices to conduct a design effectiveness review of the OCC's proposed Cloud strategy, application architecture, and related security and resiliency controls.[54] The External Risk

---

52 Internal Audit will assess plans during the 2021 Cloud Transition Audit, and more in-depth in early 2022 when the processes are modified to operate in the Cloud.

53 This annual risk assessment is provided to the Board of Directors and the Technology Committee.

54 OCC has separately submitted a request for confidential treatment to the Commission regarding the External Risk Assessment, which OCC has provided in confidential Exhibit 3v to File No. SR-OCC-2021-802 and regarding OCC's response to the External Risk Assessment recommendations, which OCC has provided in confidential Exhibit 3w to File No. SR-OCC-2021-802.

Assessment focused on: (i) Cloud reference architecture, capabilities, and controls required to host applications in the Cloud; (ii) existing and planned resiliency capabilities to meet a two-hour recovery time objective of OCC's critical services; and (iii) design of the existing and planned security controls during and after the Cloud Implementation.[55]

The External Risk Assessment identified strengths in OCC's planned Cloud Implementation, including that OCC incorporated several leading security practices as well as support for elastic capacity and the ability to scale effectively into its plan. The External Risk Assessment also included recommendations to supplement OCC's execution plan for the Cloud Implementation and were broadly categorized into six technical areas: (i) workload isolation and networking; (ii) automation and pipelines; (iii) data fabric and data lifecycle management; (iv) platform shared services and support model; (v) security shared services and support model; and (vi) resiliency. Recommendations were categorized across two dimensions: (i) program priority (high, medium, or low) and (ii) implementation action (start, accelerate, or continue). A recommendation does not necessarily mean OCC would not have implemented the recommended action absent the recommendation, as several of the recommendations were for OCC to continue an activity it had already begun. OCC has a plan in place to address the recommendations provided in the External Risk Assessment and will track the plan to completion.

---

[55] The External Risk Assessment included five discovery workshops, thirty design review sessions, discussions with over forty-eight OCC stakeholders, and review of one hundred sixty documents ranging from strategy materials to configuration builds.

iii. Internal Audit Department Plan Related to Cloud Implementation

As mentioned above, starting in 2021 and going forward, the Internal Audit Annual Plan is designed to assess important elements of the new core clearing, risk management, and data management applications roll-out. For example, the 2021 Audit Plan includes an audit on the Cloud Implementation. This audit included an analysis of OCC's disposition of the findings in the External Risk Assessment, determined if the risks associated with findings have been adequately addressed, evaluated OCC's strategy in the event it needs to transition from the CSP at any time, evaluated the adequacy of OCC's remediation plans and timelines, and OCC's assessment of the third-party CSP attestation report (SOC). The Internal Audit Department plans to augment internal resources with co-source resources with specific expertise in Cloud-based controls and has conducted a department-wide training of Cloud auditing, with additional training to be conducted as necessary.

iv. Audit Symposium and Access Rights

The CSP hosts an annual Audit Symposium, which will allow OCC to review evidence supporting the CSP's control environment. The CSP also hosts an annual Cloud security conference focused on Security, Governance, Risk and Compliance.

OCC Information Technology staff currently meets with CSP representatives weekly to focus on technical issues related to OCC's proposed Cloud environment. In addition, OCC will be holding compliance briefings with the CSP quarterly, wherein the CSP will provide OCC with documentation (e.g., SOC 2 Report) and assist OCC's preparation for the Audit Symposium. OCC management, including Security, Information Technology, and the Internal Audit Department, will coordinate to ensure

appropriate representation during the planned briefings. TPRM will help initiate and orchestrate the annual reviews.

v. Key Risk and Key Performance Indicators

OCC has also established several key risk indicators ("KRI") and key performance indicators ("KPI") to evaluate OCC's management of risk and the CSP's performance during the Cloud implementation and ongoing operation.[56] The KRIs are approved by and regularly reported to OCC's Management Committee, Board of Directors, and the Risk Committee of the Board of Directors.

OCC has developed Cloud KPIs and socialized these KPIs internally. The KRIs already exist for core clearing, risk management, and data management applications and are aligned to overall systems availability, capacity, data integrity, and security. The CSP KPIs feed into existing KRIs and will continue to be used to evaluate the CSP's performance after the Cloud Implementation.[57] KPIs will be added to monitor the performance and risks of the CSP services for which OCC has contracted. These post-Cloud Implementation KRIs and KPIs will allow OCC to assess its ongoing use of the CSP against its operational and security requirements and will demonstrate the effectiveness of risk controls and the CSP's performance against commitments in the

---

56 These KRIs and KPIs are contained in the Cloud Implementation risk report. OCC has separately submitted a request for confidential treatment to the Commission regarding the Cloud Implementation risk report, which OCC has provided in confidential Exhibit 3k to File No. SR-OCC-2021-802. See supra note 26.

57 OCC has established metrics for monitoring CSP systems capacity and availability in each zone in Risk Appetite Statements and Risk Tolerance for Cloud Services which OCC has provided in confidential Exhibit 3l to File No. SR-OCC-2021-802. Data integrity and systems incidents are monitored through OCC's Quality Standards Program and Systems Incident Program, respectively.

Service Level Agreements, and will be reported on a regular basis to OCC's Management Committee, Board of Directors, and Technology and Risk Committees of the Board of Directors.[58]

vi. Auditing the CSP Post Cloud-Implementation

OCC's Cloud Agreement gives OCC the right to attend the CSP Audit Symposium annually so that OCC may inspect and verify evidence of the design and effectiveness of the CSP's control environment and physical security controls in place at the CSP's data centers. Through preparation for and attendance at this symposium, OCC may also provide feedback and make requests of the CSP for future modifications of the control environment. The CSP is also 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 OCC 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.[59] TPRM will coordinate an annual risk assessment of OCC's relationship with the CPS. TPRM, Security, and Business Continuity will determine the adequacy and reasonableness of the documentation received to complete the Third-Party Risk Assessment. Finally, the Cloud Agreement provides that OCC's regulators may visit the

---

58 OCC has separately submitted a request for confidential treatment to the Commission regarding metrics and reporting that OCC will use to monitor the security and performance of the CSP after adoption, which OCC has provided in confidential Exhibit 3x to File No. SR-OCC-2021-802.

59 The FFIEC Guidance provides that OCC 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, page 7. OCC reviews the CSP's SOC-2 on an annual basis.

facilities of the CSP under specified conditions.

OCC plans 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 (and the on-premises data center to the extent it is used). When incidents are detected, OCC will follow its existing incident response governance to identify, detect, contain, eradicate, and recover from incidents.

Consistency with the Payment, Clearing and Settlement 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.[60] Section 805(a)(2) of the Clearing Supervision Act[61] also authorizes the Commission to prescribe risk management standards for the payment, clearing and settlement activities of designated clearing entities, like OCC, for which the Commission is the supervisory agency. Section 805(b) of the Clearing Supervision Act[62] 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;

60 12 U.S.C. 5461(b).

61 12 U.S.C. 5464(a)(2).

62 12 U.S.C. 5464(b).

- reduce systemic risks; and
- support the stability of the broader financial system.

The Commission has adopted risk management standards under Section 805(a)(2) of the Clearing Supervision Act and the Exchange Act in furtherance of these objectives and principles.[63] Rule 17Ad-22 requires registered clearing agencies, like OCC, to 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.[64] Therefore, the Commission has stated[65] that it believes it is appropriate to review changes proposed in advance notices against Rule 17Ad-22 and the objectives and principles of these risk management standards as described in Section 805(b) of the Clearing Supervision Act.[66]

OCC believes that the proposed changes are consistent with Section 805(b)(1) of the Clearing Supervision Act[67] and the requirements of Rules 17Ad-22(e)(17) and (e)(21)

---

63 17 CFR 240.17Ad-22. See 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").

64 17 CFR 240.17Ad-22.

65 See e.g., Exchange Act Release No. 86182 (June 24, 2019), 84 FR 31128, 31129 (June 28, 2019) (SR-OCC-2019-803).

66 12 U.S.C. 5464(b). Reg SCI was not adopted under the Payment, Clearing and Settlement Supervision Act and thus is not analyzed in this section. However, an analysis of the compliance requirements of Reg SCI and the provisions of the Cloud Agreement that enable OCC to meet them are provided in confidential Exhibit 3d to File No. SR-OCC-2021-802, for which OCC has separately submitted a request for confidential treatment from the Commission.

67 12 U.S.C. 5464(b)(1).

under the Act because the Cloud Implementation would provide OCC with resilient, secure, and scalable core clearing, risk management, and data management systems that far exceeds what is currently possible in an on-premises infrastructure.

Rule 17Ad-22(e)(17)(ii) requires OCC to establish, implement, maintain, and enforce written policies and procedures reasonably designed to manage OCC's operational risk by "ensuring that systems have a high degree of security, resiliency, operational reliability, and adequate, scalable capacity."[68] OCC maintains 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.[69] As stated above, resiliency of the Cloud Infrastructure is built into the system with functionality for OCC's core clearing, risk management, and data management applications to run in multiple zones within multiple regions. Regions are isolated from one another and are designed in part to minimize the possibility of a multi-region outage. OCC has designed the infrastructure to have primary (hot)/ secondary (warm) zones 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 OCC multiple redundancies within which to run its core clearing,

---

68 17 CFR 240.17Ad-22(e)(17)(ii).

69 OCC has separately submitted a request for confidential treatment to the Commission regarding the IT Operational Risk Management Policy, which OCC has provided as confidential Exhibit 3y to File No. SR-OCC-2021-802, the Technology Operations Policy, which OCC has provided as confidential Exhibit 3z to File No. SR-OCC-2021-802, and the Business Continuity Procedure, which OCC has provided as confidential Exhibit 3aa to File No. SR-OCC-2021-802.

risk management, and data management applications while simultaneously restricting the effect of an incident at the CSP to the smallest footprint possible. Furthermore, in the unlikely and extraordinary event OCC loses access to each of the six levels of resiliency within the CSP environment, OCC can failover to an on-premises backup that will permit continued operations of core clearing, risk management, and data management applications.

OCC has established a robust Cloud security program to manage the security of the core clearing, risk management, and data management applications that will be running in the 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.[70] The enterprise security program encompasses all OCC assets existing in OCC offices, data centers, and within the Cloud Provider's Cloud Infrastructure, and IAM controls ensure least-privileged user access to applications on the Cloud. OCC has appropriate controls in place to ensure the security of confidential information in-transit between OCC data centers and the Cloud Infrastructure, between systems within the Cloud Infrastructure, and at-rest. All network communications between OCC and the Cloud will rely on industry standard encryption for traffic while in transit, and data at rest will 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

---

[70] For example, vulnerability scanning, automated secrets management including certificate encryption, and incident triage management and handling process.

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

Since additional computing power can be launched on demand, the scalability in a Cloud computing environment is considerable and instantaneous. OCC 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: OCC would need to obtain additional physical servers and network equipment 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.

Rule 17Ad-22(e)(21) requires OCC to establish, implement, maintain, and enforce written policies and procedures reasonably designed to "be efficient and effective in meeting the requirements of its participants and the markets it serves," and to have OCC's management regularly review the "efficiency and effectiveness of, [*inter alia*,] its (i) clearing and settlement arrangements and (ii) operating structure, including risk management policies, procedures, and systems."[71] OCC maintains policies designed to enable the regular review of the efficiency and effectiveness of the arrangements and operating structures supporting OCC's identified goals and objectives.[72] There are

---

71 17 CFR 240.17Ad-22(e)(21).

72 OCC has separately submitted a request for confidential treatment to the Commission regarding the Annual Planning Policy, which OCC has provided as confidential Exhibit 3bb to File No. SR-OCC-2021-802, the Balanced Scorecard Procedure, which OCC has provided as confidential Exhibit 3cc to File No. SR-OCC-2021-802, the Enterprise Portfolio Management Procedure, which OCC has provided as confidential Exhibit 3dd to File No. SR-OCC-2021-802, the New Business and New Exchange Procedure, which OCC has provided as confidential Exhibit 3ee to File No. SR-OCC-2021-802, and the New Product Procedure,

several significant efficiency benefits to the Cloud Implementation, including:

- Ad-hoc reporting capability with new filtering functionality and application programming interfaces to make it easier to procure and submit data to and from the system.
- The capability to quickly add or remove Compute, Storage, or Network resources to meet changing application needs and market volatility.
- The capability to (i) run certain back testing processes that used to take days to months in a few hours; (ii) manage multiple back testing processes the same time; and (iii) eliminate any undue delay in the evaluation of potential risk management enhancements for the industry.
- The scalability to more efficiently meet historical data storage needs, provide data access through standard data services, and the ability to respond quickly to regulatory requests.
- Easy and secure access to high-quality, high-fidelity data, including a centralized, enterprise-wide repository to store and provide timely access to system of record data.

Accordingly, the proposed changes: (i) are designed to promote robust risk management; (ii) are consistent with promoting safety and soundness; and (iii) are consistent with reducing systemic risks and promoting the stability of the broader financial system. The proposed changes also ensure that OCC systems have a high degree of security, resiliency, operational reliability, and adequate, scalable capacity, and enable OCC to be

---

which OCC has provided as confidential Exhibit 3ff to File No. SR-OCC-2021-802.

efficient and effective in meeting the requirements of its participants and the markets it serves. For the foregoing reasons, OCC believes that the proposed changes are consistent with Section 805(b)(1) of the Clearing Supervision Act[73] and Rules 17Ad-22(e)(17)[74] and (e)(21)[75] under the Exchange Act.

III. Date of Effectiveness of the Advance Notice

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 the proposed change was filed with the Commission or (ii) the date any additional information requested by the Commission is received.[76] OCC shall not implement the proposed change if the Commission has any objection to the proposed change.[77]

OCC shall post notice on its website of proposed changes that are implemented. The proposal shall not take effect until all regulatory actions required with respect to the proposal are completed.

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:

---

73 12 U.S.C. 5464(b).

74 17 CFR 240.17Ad-22(e)(17).

75 17 CFR 240.17Ad-22(e)(21).

76 12 U.S.C. 5465(e)(1)(G).

77 12 U.S.C. 5465(e)(1)(F).

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-OCC-2021-802 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-OCC-2021-802. 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 the self-regulatory organization.

All comments received will be posted without change. Persons submitting comments are cautioned that we do not redact or edit personal identifying information

from comment submissions. You should submit only information that you wish to make available publicly.

V. Date of Timing for Commission Action

Section 806(e)(1)(G) of the Clearing Supervision Act provides that OCC may implement the changes if it has not received an objection to the proposed changes within 60 days of the later of (i) the date that the Commission receives the Advance Notice or (ii) the date that any additional information requested by the Commission is received,[78] unless extended as described below.

Pursuant to Section 806(e)(1)(H) of the Clearing Supervision Act, the Commission may extend the review period of an advance notice for an additional 60 days, if the changes proposed in the advance notice raise novel or complex issues, subject to the Commission providing the clearing agency with prompt written notice of the extension.[79]

Here, as the Commission has not requested any additional information, the date that is 60 days after OCC filed the Advance Notice with the Commission is December 7, 2021. However, the Commission finds the issues raised by the Advance Notice complex because OCC proposes to migrate its clearing, risk management, and data management applications to a cloud infrastructure with an on-demand network of configurable information technology resources running on virtual infrastructure hosted by a third party. The Commission also finds the issues raised by the Advance Notice novel because the proposed migration of a covered clearing agency's clearing, risk management, and

78 12 U.S.C. 5465(e)(1)(G).

79 12 U.S.C. 5465(e)(1)(H).

data management applications to a third-party-hosted cloud infrastructure represents a novel circumstance in the U.S. markets that would require careful scrutiny and consideration of its associated risks. Therefore, the Commission finds it appropriate to extend the review period of the Advance Notice for an additional 60 days under Section 806(e)(1)(H) of the Clearing Supervision Act.[80]

Accordingly, the Commission, pursuant to Section 806(e)(1)(H) of the Clearing Supervision Act,[81] extends the review period for an additional 60 days so that the Commission shall have until February 5, 2022 to issue an objection or non-objection to advance notice SR-OCC-2021-802.

80 Id.

81 Id.

All submissions should refer to File Number SR- OCC-2021-802 and should be submitted on or before [insert date 21 days from publication in the Federal Register].

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.[82]

J. Matthew DeLesDernier
Assistant Secretary

[82] 17 CFR 200.30-3(a)(91).