This document is scheduled to be published in the Federal Register on 04/05/2023 and available online at **federalregister.gov/d/2023-05767**, and on **govinfo.gov**

8011-01p

SECURITIES AND EXCHANGE COMMISSION

17 CFR Parts 232, 240, 242 and 249

[Release No. 34-97142; File No. S7-06-23]

RIN 3235-AN15

Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents

AGENCY: Securities and Exchange Commission.

ACTION: Proposed rule.

SUMMARY: The Securities and Exchange Commission ("Commission") is proposing a new rule and form and amendments to existing recordkeeping rules to require broker-dealers, clearing agencies, major security-based swap participants, the Municipal Securities Rulemaking Board, national securities associations, national securities exchanges, security-based swap data repositories, security-based swap dealers, and transfer agents to address cybersecurity risks through policies and procedures, immediate notification to the Commission of the occurrence of a significant cybersecurity incident and, as applicable, reporting detailed information to the Commission about a significant cybersecurity incident, and public disclosures that would improve transparency with respect to cybersecurity risks and significant cybersecurity incidents. In addition, the Commission is proposing amendments to existing clearing agency exemption orders to require the retention of records that would need to be made under the proposed cybersecurity requirements. Finally, the Commission is proposing amendments to address the potential availability to security-based swap dealers and major security-based swap participants of substituted compliance in connection with those requirements.

DATES: Comments should be received on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: Comments may be submitted by any of the following methods:

Electronic Comments:

- Use the Commission's internet comment form (https://www.sec.gov/rules/submitcomments.htm); or
- Send an email to rule-comments@sec.gov. Please include File Number S7-06-23 on the subject line.

Paper Comments:

- Send paper comments to Secretary, Securities and Exchange Commission, 100 F Street, NE, Washington, DC 20549-1090.

All submissions should refer to File Number S7-06-23. The file number should be included on the subject line if email is used. To help the Commission process and review your comments more efficiently, please use only one method of submission. The Commission will post all comments on the Commission's website (https://www.sec.gov/rules/proposed.shtml). Comments are also 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 a.m. and 3 p.m. Operating conditions may limit access to the Commission's Public Reference Room. All comments received will be posted without change; the Commission does not edit personal identifying information from submissions. You should submit only information that you wish to make available publicly.

Studies, memoranda, or other substantive items may be added by the Commission or staff to the comment file during this rulemaking. A notification of the inclusion in the comment file of any such materials will be made available on the Commission's website. To ensure direct electronic receipt of such notifications, sign up through the "Stay Connected" option at www.sec.gov to receive notifications by email.

FOR FURTHER INFORMATION CONTACT: Randall W. Roy, Deputy Associate Director and Nina Kostyukovsky, Special Counsel, Office of Broker-Dealer Finances (with respect to the proposed cybersecurity rule and form and the aspects of the proposal unique to broker-dealers); Matthew Lee, Assistant Director and Stephanie Park, Senior Special Counsel, Office of Clearance and Settlement (with respect to aspects of the proposal unique to clearing agencies and security-based swap data repositories); John Guidroz, Assistant Director and Russell Mancuso, Special Counsel, Office of Derivatives Policy (with respect to aspects of the proposal unique to major security-based swap participants and security-based swap dealers); Michael E. Coe, Assistant Director and Leah Mesfin, Special Counsel, Office of Market Supervision (with respect to aspects of the proposal unique to national securities associations and national securities exchanges); Moshe Rothman, Assistant Director, Office of Clearance and Settlement (with respect to aspects of the proposal unique to transfer agents) at (202) 551-5500, Division of Trading and Markets; and Dave Sanchez, Director, Adam Wendell, Deputy Director, and Adam Allogramento, Special Counsel, Office of Municipal Securities (with respect to aspects of the proposal unique to the Municipal Securities Rulemaking Board) at (202) 551-5680, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-7010.

SUPPLEMENTARY INFORMATION: The Commission is proposing to add the following new rule and form under the Securities Exchange Act of 1934 ("Exchange Act"): (1) 17 CFR 242.10 ("Rule 10"); and (2) 17 CFR 249.642 ("Form SCIR"). The Commission also is proposing related amendments to the following rules: (1) 17 CFR 232.101; (2) 17 CFR 240.3a71-6; (3) 17 CFR 240.17a-4; (4) 17 CFR 240.17Ad-7; (5) 17 CFR 240.18a-6; and (6) 17 CFR 240.18a-10. Further, the Commission is proposing to amend certain orders that exempt clearing agencies from registration.

Commission Reference	CFR Citation (17 CFR)
Regulation S-T	§ 232.101
Rule 3a71-6	§ 240.3a71-6
Rule 17a-4	§ 240.17a-4
Rule 17Ad-7	§ 240.17Ad-7

Rule 18a-6	§ 240.18a-6
Rule 18a-10	§ 240.18a-10
Rule 10	§ 242.10
Form SCIR	§ 249.624

TABLE OF CONTENTS

I. INTRODUCTION
- A. Cybersecurity Risk Poses a Threat the U.S. Securities Markets
  1. In General
  2. Critical Operations of Market Entities are Exposed to Cybersecurity Risk
- B. Overview of the Proposed Cybersecurity Requirements

II. DISCUSSION OF PROPOSED CYBERSECURITY RULE
- A. Definitions
  1. "Covered Entity"
  2. "Cybersecurity Incident"
  3. "Significant Cybersecurity Incident"
  4. "Cybersecurity Threat"
  5. "Cybersecurity Vulnerability"
  6. "Cybersecurity Risk"
  7. "Information"
  8. "Information Systems"
  9. "Personal Information"
  10. Request for Comment
- B. Proposed Requirements for Covered Entities
  1. Cybersecurity Risk Management Policies and Procedures
  2. Notification and Reporting of Significant Cybersecurity Incidents
  3. Disclosure of Cybersecurity Risks and Incidents
  4. Filing Parts I and II of Proposed Form SCIR in EDGAR Using a Structured Data Language
  5. Recordkeeping
- C. Proposed Requirements for Non-Covered Broker-Dealers
  1. Cybersecurity Policies and Procedures, Annual Review, Notification, and Recordkeeping
  2. Request for Comment
- D. Cross-Border Application of the Proposed Cybersecurity Requirements to SBS Entities
  1. Background on the Cross-Border Application of Title VII Requirements
  2. Proposed Entity-Level Treatment
  3. Availability of Substituted Compliance
- E. Amendments to Rule 18a-10
  1. Proposal
  2. Request for Comment
- F. Market Entities Subject to Regulation SCI, Regulation S-P, Regulation ATS, and Regulation S-ID
  1. Discussion
  2. Request for Comment
- G. Cybersecurity Risk Related to Crypto Assets

III. GENERAL REQUEST FOR COMMENT

IV. ECONOMIC ANALYSIS
- A. Introduction
- B. Broad Economic Considerations
- C. Baseline
  1. Cybersecurity Risks and Current Relevant Regulations
  2. Market Structure
- D. Benefits and Costs of Proposed Rule 10, Form SCIR, and Rule Amendments
  1. Benefits and Costs of the Proposals to the U.S. Securities Markets
  2. Policies and Procedures and Annual Review Requirements for Covered Entities
  3. Regulatory Reporting of Cybersecurity Incidents by Covered Entities
  4. Public Disclosure of Cybersecurity Risks and Significant Cybersecurity Incidents
  5. Record Preservation and Maintenance by Covered Entities
  6. Policies and Procedures, Annual Review, Immediate Notification of Significant Cybersecurity Incidents, and Record Preservation Requirements for Non-Covered Broker-Dealers
  7. Substituted Compliance for Non-U.S. SBS Entities

E. Effects on Efficiency, Competition, and Capital Formation
F. Reasonable Alternatives
1. Alternatives to the Policies and Procedures Requirements of Proposed Rule 10
2. Alternatives to the Requirements of Proposed Form SCIR and Related Notification and Disclosure Requirements of Proposed Rule 10
3. General Request for Comment
V. PAPERWORK REDUCTION ACT ANALYSIS
A. Summary of Collections of Information
1. Proposed Rule 10
2. Form SCIR
3. Rules 17a-4, 17ad-7, 18a-6 and Clearing Agency Exemption Orders
4. Substituted Compliance (Rule 3a71-6)
B. Proposed Use of Information
C. Respondents
1. Broker-Dealers
2. Clearing Agencies
3. The MSRB
4. National Securities Exchanges and National Securities Associations
5. SBS Entities
6. SBSDRs
7. Transfer Agents
D. Total Initial and Annual Reporting Burdens
1. Proposed Rule 10
2. Form SCIR
3. Rules 17a-4, 17ad-7, 18a-6, and Clearing Agency Exemption Orders (and Existing Rules 13n-7 and 17a-1)
4. Substituted Compliance- Rule 3a71-6
E. Collection of Information is Mandatory
F. Confidentiality of Responses to Collection of Information
G. Retention Period for Recordkeeping Requirements
H. Request for Comment
VI. INITIAL REGULATORY FLEXIBILITY ACT ANALYSIS
A. Reasons for, and Objectives of, Proposed Action
1. Proposed Rule 10 and Parts I and II of Proposed Form SCIR
2. Rules 17a-4, 17ad-7, 18a-6 and Clearing Agency Exemption Orders
B. Legal Basis
C. Small Entities Subject to Proposed Rule, Form SCIR, and Recordkeeping Rule Amendments
1. Broker-Dealers
2. Clearing Agencies
3. The MSRB
4. National Securities Exchanges and National Securities Associations
5. SBS Entities
6. SBSDRs
7. Transfer Agents
D. Reporting, Recordkeeping, and Other Compliance Requirements
1. Proposed Rule 10 and Parts I and II of Proposed Form SCIR
2. Rules 17a-4, 17ad-7, and 18a-6
E. Duplicative, Overlapping, or Conflicting Federal Rules
1. Proposed Rule 10 and Parts I and II of Proposed Form SCIR
2. Rules 17a-4, 17ad-7, 18a-6 and Clearing Agency Exemption Orders
F. Significant Alternatives
1. Broker-Dealers
2. Clearing Agencies
3. The MSRB
4. National Securities Exchanges and National Securities Associations
5. SBS Entities
6. SBSDRs
7. Transfer Agents
G. Request for Comment
VII. SMALL BUSINESS REGULATORY ENFORCEMENT FAIRNESS ACT
VIII. STATUTORY AUTHORITY

I. INTRODUCTION

A. Cybersecurity Risk Poses a Threat the U.S. Securities Markets

1. In General

Cybersecurity risk has been described as "an effect of uncertainty on or within information and technology."[1] This risk can lead to "the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and [thereby to] potential adverse impacts to organizational operations (*i.e.*, mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation."[2] The U.S. Financial Stability Oversight Counsel ("FSOC") in its 2021 annual report stated that a destabilizing cybersecurity incident could potentially threaten the stability of the U.S. financial system through at least three channels:

- First, the incident could disrupt a key financial service or utility for which there is little or no substitute. This could include attacks on central banks; exchanges; sovereign and subsovereign creditors, including U.S. state and local governments; custodian banks;

---

[1] *See* the National Institute of Standards and Technology ("NIST"), U.S. Department of Commerce, *Computer Security Resource Center Glossary*, *available at* https://csrc.nist.gov/glossary ("NIST Glossary") (definition of "cybersecurity risk"). The NIST Glossary consists of terms and definitions extracted verbatim from NIST's cybersecurity and privacy-related publications (*i.e.*, Federal Information Processing Standards (FIPS), NIST Special Publications (SPs), and NIST Internal/Interagency Reports (IRs)) and from the Committee on National Security Systems (CNSS) Instruction CNSSI-4009. The NIST Glossary may be expanded to include relevant terms in external or supplemental sources, such as applicable laws and regulations. The Cybersecurity Enhancement Act of 2014 ("CEA") updated the role of NIST to include identifying and developing cybersecurity risk frameworks for voluntary use by critical infrastructure owners and operators. The CEA required NIST to identify "a prioritized, flexible, repeatable, performance based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks." *See* 15 U.S.C. 272(e)(1)(A)(iii). In response, NIST has published the *Framework for Improving Critical Infrastructure Cybersecurity* ("NIST Framework"). *See also* NIST, *Integrating Cybersecurity and Enterprise Risk Management (ERM)* (Oct. 2020), *available at* https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf ("All types of organizations, from corporations to federal agencies, face a broad array of risks. For federal agencies, the Office of Management and Budget (OMB) Circular A-11 defines risk as 'the effect of uncertainty on objectives'. The effect of uncertainty on enterprise mission and business objectives may then be considered an 'enterprise risk' that must be similarly managed…Cybersecurity risk is an important type of risk for any enterprise.") (footnotes omitted).

[2] *See* NIST Glossary (definition of "cybersecurity risk"). *See also* The Board of the International Organization of Securities Commissions ("IOSCO"), *Cyber Security in Securities Markets – An International Perspective* (Apr. 2016), *available at* https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf ("IOSCO Cybersecurity Report") ("In essence, cyber risk refers to the potential negative outcomes associated with cyber attacks. In turn, cyber attacks can be defined as attempts to compromise the confidentiality, integrity and availability of computer data or systems.") (footnote omitted).

payment clearing and settlement systems; or other firms or services that lack substitutes or are sole service providers.

- Second, the incident could compromise the integrity of critical data. Accurate and usable information is critical to the stable functioning of financial firms and the system; if such data is corrupted on a sufficiently large scale, it could disrupt the functioning of the system. The loss of such data also has privacy implications for consumers and could lead to identity theft and fraud, which in turn could result in a loss of confidence.

- Third, a cybersecurity incident that causes a loss of confidence among a broad set of customers or market participants could cause customers or participants to question the safety or liquidity of their assets or transactions, and lead to significant withdrawal of assets or activity.[3]

The U.S. securities markets are part of the *Financial Services Sector*, one of the sixteen critical infrastructure sectors "whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[4] These markets are over $100 trillion in total size, and more than a trillion dollars' worth of transactions flow through them each day. For example, the market capitalization of the U.S. equities market was valued at $49 trillion as of the first quarter of 2022,[5] and as of May 2022, the average daily trading dollar volume in the U.S. equities market was $659 billion.[6] The market capitalization of the U.S. fixed income market was valued at

---

[3] FSOC, *Annual Report (2021)*, at 168, *available at* https://home.treasury.gov/system/files/261/FSOC2021AnnualReport.pdf ("FSOC 2021 Annual Report").

[4] Cybersecurity and Infrastructure Security Agency ("CISA"), U.S. Department of Homeland Security, *Critical Infrastructure Sectors*, *available at* https://www.cisa.gov/critical-infrastructure-sectors. *See also* Presidential Policy Directive – Critical Infrastructure Security and Resilience, Presidential Policy Directive, PPD-21 (Feb. 12 2013).

[5] *See* Securities Industry and Financial Markets Association ("SIFMA"), Research Quarterly: Equities (Apr. 27, 2022), *available at* https://www.sifma.org/resources/research/research-quarterly-equities/.

[6] *See* SIFMA, US Equity and Related Statistics (June 1, 2022), *available at* https://www.sifma.org/resources/research/us-equity-and-related-securities-statistics/.

$52.9 trillion as of the fourth quarter of 2021,[7] and as of May 2022, the average daily trading dollar volume in the U.S. fixed income market was $897.8 billion.[8]

The sizes of these markets are indicative of the central role they play in the U.S. economy in terms of the flow of capital, including the savings of individual investors who are increasingly relying on them to, for example, build wealth to fund their retirement, purchase a home, or pay for college for themselves or their family. Therefore, it is critically important to the U.S. economy, investors, and capital formation that the U.S. securities markets function in a fair, orderly, and efficient manner.[9]

The fair, orderly, and efficient operation of the U.S. securities markets depends on different types of entities performing various functions to support, among other things, disseminating market information, underwriting securities issuances, making markets in securities, trading securities, providing liquidity to the securities markets, executing securities transactions, clearing and settling securities transactions, financing securities transactions, recording and transferring securities ownership, maintaining custody of securities, paying dividends and interest on securities, repaying principal on securities investments, supervising regulated market participants, and monitoring market activities. Collectively, these functions are performed by entities regulated by the Commission: broker-dealers, broker-dealers that operate an alternative trading system ("ATS"), clearing agencies, major security-based swap participants ("MSBSPs"), the Municipal Securities Rulemaking Board ("MSRB"), national securities associations, national securities exchanges, security-based swap data repositories ("SBSDRs"),

---

7 *See* SIFMA, Research Quarterly: Fixed Income – Outstanding (Mar. 14, 2022), *available at* https://www.sifma.org/resources/research/research-quarterly-fixed-income-outstanding/.

8 *See* SIFMA, US Fixed Income Securities Statistics (June 9, 2022), *available at* https://www.sifma.org/resources/research/us-fixed-income-securities-statistics/.

9 The Commission's tripartite mission is to: (1) protect investors; (2) maintain, fair, orderly, and efficient markets; and (3) facilitate capital formation. *See, e.g.*, Commission, *Our Goals*, *available at* https://www.sec.gov/our-goals.

security-based swap dealers ("SBSDs" or collectively with MSBSPs, "SBS Entities"), and transfer agents (collectively, "Market Entities").[10]

To perform their functions, Market Entities rely on an array of electronic information, communication, and computer systems (or similar systems) ("information systems") and networks of interconnected information systems. While Market Entities have long relied on information systems to perform their various functions, the acceleration of technical innovation in recent years has exponentially expanded the role these systems play in the U.S. securities markets.[11] This expansion has been driven by the greater efficiencies and lower costs that can be achieved through the use of information systems.[12] It also has been driven by newer entrants (financial technology (Fintech) firms) that have developed business models that rely heavily on information systems (*e.g.*, applications on mobile devices) to provide services to investors and other participants in the securities markets and more established Market Entities adopting the use

---

[10] Currently, there are no MSBSPs registered with the Commission.

[11] *See, e.g.*, Bank of International Settlements, Erik Feyen, Jon Frost, Leonardo Gambacorta, Harish Natarajan, and Mathew Saal, *Fintech and the digital transformation of financial services: implications for market structure and public policy*, BIS Papers No. 117 (July 2021), *available at* https://www.bis.org/publ/bppdf/bispap117.pdf ("BIS Papers 117") ("Significant technology advances have taken place in two key areas that have contributed to the current wave of technology-based finance:" Increased connectivity… [and] Low-cost computing and data storage…").

[12] *Id.* ("Technology has reduced the costs of, and need for, much of the traditional physical infrastructure that drove fixed costs for the direct financial services provider… Financial intermediaries can reduce marginal costs through technology-enabled automation and 'straight through' processing, which are accelerating with the expanded use of data and [artificial intelligence]-based processes. Digital innovation can also help to overcome spatial (geographical) barriers, and even to bridge differences across legal jurisdictions…"). *See also* United Nations, Office for Disaster Risk Reduction, Constantine Toregas and Joost Santos, *Cybersecurity and its cascading effect on societal systems* (2019), *available at* https://www.undrr.org/publication/cybersecurity-and-its-cascading-effect-societal-systems ("Cybersecurity and its Cascading Effect on Societal Systems") ("Modern society has benefited from the additional efficiency achieved by improving the coordination across interdependent systems using information technology (IT) solutions. IT systems have significantly contributed to enhancing the speed of communication and reducing geographic barriers across consumers and producers, leading to a more efficient and cost-effective exchange of products and services across an economy.").

of similar technologies.[13] The COVID-19 pandemic also has contributed to the greater reliance on information systems.[14]

This increased reliance on information systems by Market Entities has caused a corresponding increase in their cybersecurity risk.[15] This risk can be caused by the actions of external threat actors, including organized or individual threat actors seeking financial gain, nation states conducting espionage operations, or individuals engaging in protest, acting on

---

13 BIS Papers 117 ("Internet and mobile technology have rapidly increased the ability to transfer information and interact remotely, both between businesses and directly to the consumer. Through mobile and smartphones, which are near-ubiquitous, technology has increased access to, and the efficiency of, direct delivery channels and promises lower-cost, tailored financial services… Incumbents large and small are embracing digital transformation across the value chain to compete with fintechs and big techs. Competitive pressure on traditional financial institutions may force even those that are lagging to transform or risk erosion of their customer base, income, and margins.").

14 *Id.* ("The COVID-19 pandemic has accelerated the digital transformation. In particular, the need for digital connectivity to replace physical interactions between consumers and providers, and in the processes that produce financial services, will be even more important as economies, financial services providers, businesses and individuals navigate the pandemic and the eventual post-COVID-19 world."). *See also* McKinsey & Company, *How Covid-19 has pushed companies over the technology tipping point – and transformed business forever* (Oct. 5, 2020), *available at* https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever#/ (noting that due to the COVID-19 pandemic, "companies have accelerated the digitization of their customer and supply-chain interactions and of their internal operations by three to four years [and] the share of digital or digitally enhanced products in their portfolios has accelerated by a shocking seven years").

15 *See, e.g.*, Financial Services Information Sharing and Analysis Center ("FS-ISAC"), *Navigating Cyber 2022* (Mar. 2022), *available at*: www.fsisac.com/navigatingcyber2022-report (detailing cyber threats that emerged in 2021 and predictions for 2022); Danny Brando, Antonis Kotidis, Anna Kovner, Michael Lee, and Stacey L. Schreft, *Implications of Cyber Risk for Financial Stability*, FEDS Notes, Washington: Board of Governors of the Federal Reserve System (May 12, 2022), *available at* https://doi.org/10.17016/2380-7172.3077 ("Implications of Cyber Risk for Financial Stability") ("Cyber risk in the financial system has grown over time as the system has become more digitized, as evidenced by the increase in cyber incidents. That growth has brought to light unique features of cyber risk and the potentially greater scope for cyber events to affect financial stability."); United States Government Accountability Office ("GAO"), *Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts*, GAO-20-631 (Sept. 2020), *available at* https://www.gao.gov/assets/gao-20-631.pdf ("GAO Cybersecurity Report") ("The federal government has long identified the financial services sector as a critical component of the nation's infrastructure. The sector includes commercial banks, securities brokers and dealers, and providers of the key financial systems and services that support these functions. Altogether, the sector holds about $108 trillion in assets and faces a variety of cybersecurity-related risks. Key risks include (1) an increase in access to financial data through information technology service providers and supply chain partners; (2) a growth in sophistication of malware—software meant to do harm—and (3) an increase in interconnectivity via networks, the cloud, and mobile applications."); Cybersecurity and its Cascading Effect on Societal Systems ("Nonetheless, IT dependence has also exposed critical infrastructure and industry systems to a myriad of cyber security risks, ranging from accidental causes, technological glitches, to malevolent willful attacks.").

grudges or personal offenses, or seeking thrills.[16] Internal threat actors (*e.g.*, disgruntled employees or employees seeking financial gain) also can be sources of cybersecurity risk.[17] Threat actors may target Market Entities because they handle financial assets or proprietary information about financial assets and transactions.[18] In addition to threat actors, errors of employees, service providers, or business partners can create cybersecurity risk (*e.g.*, mistakenly exposing confidential or personal information by, for example, sending it through an unencrypted email to unintended recipients).[19]

Another factor increasing the cybersecurity risk to Market Entities is the growing sophistication of the tactics, techniques, and procedures employed by threat actors.[20] This trend

---

16 *See, e.g.*, Verizon, *Data Breach Investigations Report* (2022) *available at* https://www.verizon.com/business/resources/Tba/reports/dbir/2022-data-breach-investigations-report-dbir.pdf ("Verizon DBIR") (finding that 73% of the data breaches analyzed in the report were caused by external actors). The Verizon DBIR is an annual report that analyzes cyber security incidents (defined as a security event that compromises the integrity, confidentiality or availability of an information asset) and breaches (defined as an incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party). To perform the analysis, data about the cybersecurity incidents included in the report are catalogued using the Vocabulary for Event Recording and Incident Sharing (VERIS). VERIS is a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner. More information about VERIS is available at: http://veriscommunity.net/index.html. *See also* Microsoft, *Microsoft Digital Defense Report* (Oct. 2021), *available at* https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi ("Microsoft Report") ("The last year has been marked by significant historic geopolitical events and unforeseen challenges that have changed the way organizations approach daily operations. During this time, nation state actors have largely maintained their operations at a consistent pace while creating new tactics and techniques to evade detection and increase the scale of their attacks").

17 *See, e.g.*, Verizon DBIR (finding that 18% of the data breaches analyzed in the report were caused by internal actors). *But see id.* ("Internal sources accounted for the fewest number of incidents (18 percent), trailing those of external origin by a ratio of four to one. The relative infrequency of data breaches attributed to insiders may be surprising to some. It is widely believed and commonly reported that insider incidents outnumber those caused by other sources. While certainly true for the broad range of security incidents, our caseload showed otherwise for incidents resulting in data compromise. This finding, of course, should be considered in light of the fact that insiders are adept at keeping their activities secret.").

18 *See, e.g.*, GAO Cybersecurity Report ("The financial services sector faces significant risks due to its reliance on sophisticated technologies and information systems, as well as the potential monetary gain and economic disruption that can occur by attacking the sector"); IOSCO Cybersecurity Report ("[T]he financial sector is one of the prime targets of cyber attacks. It is easy to understand why: the sector is 'where the money is' and it can represent a nation or be a symbol of capitalism for some politically motivated activists.").

19 *See* Verizon DBIR (finding that error (defined as anything done (or left undone) incorrectly or inadvertently) as one of action types leading to cybersecurity incidents and breaches).

20 *See, e.g.*, Bank of England, *CBEST Intelligence-Led Testing: Understanding Cyber Threat Intelligence Operations (Version 2.0)*, *available at* https://www.bankofengland.co.uk/-/media/boe/files/financial-

is further exacerbated by the ability of threat actors to purchase tools to engage in cyber-crime.[21]

Threat actors employ a number of tactics to cause harmful cybersecurity incidents.[22] One tactic is the use of malicious software ("malware") that is uploaded into a computer system and used by threat actors to compromise the confidentiality of information stored or operations performed (*e.g.*, monitoring key strokes) on the system or the integrity or availability of the system (*e.g.*, command and control attacks where a threat actor is able to infiltrate a system to install malware to enable it to remotely send commands to infected devices).[23] There are a

---

stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf ("Bank of England CBEST Report") ("The threat actor community, once dominated by amateur hackers, has expanded to include a broad range of professional threat actors, all of whom are strongly motivated, organised and funded. They include: state-sponsored organisations stealing military, government and commercial intellectual property; organised criminal gangs committing theft, fraud and money laundering which they perceive as low risk and high return; non-profit hacktivists and for-profit mercenary organisations attempting to disrupt or destroy their own or their client's perceived enemies."); Microsoft Report ("Sophisticated cybercriminals are also still working for governments conducting espionage and training in the new battlefield").

21 *See, e.g.*, Microsoft Report ("Through our investigations of online organized crime networks, frontline investigations of customer attacks, security and attack research, nation state threat tracking, and security tool development, we continue to see the cybercrime supply chain consolidate and mature. It used to be that cybercriminals had to develop all the technology for their attacks. Today they rely on a mature supply chain, where specialists create cybercrime kits and services that other actors buy and incorporate into their campaigns. With the increased demand for these services, an economy of specialized services has surfaced, and threat actors are increasing automation to drive down their costs and increase scale.").

22 *See, e.g.*, Financial Industry Regulatory Authority ("FINRA"), Common Cybersecurity Threats, available at: www.finra.org/rules-guidance/guidance/common-cybersecurity-threats ("FINRA Common Cybersecurity Threats") (summarizing common cybersecurity threats faced by broker-dealers to include phishing, imposter websites, malware, ransomware, distributed denial-of-service attacks, and vendor breaches, among others).

23 *See* CISA, *Malware Tip Card*, *available at* https://www.cisa.gov/sites/default/files/publications/Malware_1.pdf ("CISA Malware Tip Card") ("Malware, short for "malicious software," includes any software (such as a virus, Trojan, or spyware) that is installed on your computer or mobile device. The software is then used, usually covertly, to compromise the integrity of your device. Most commonly, malware is designed to give attackers access to your infected computer. That access may allow others to monitor and control your online activity or steal your personal information or other sensitive data.").

number of different forms of malware, including adware, botnets, rootkit, spyware, Trojans, viruses, and worms.[24]

A second tactic is a variation of malware known as "ransomware."[25] In this scheme, the threat actor encrypts the victim's data making it unusable and then demands payment to decrypt it.[26] Ransomware schemes have become more prevalent with the widespread adoption and use of

---

[24] *See, e.g.*, CISA Malware Tip Card ("Adware [is] a type of software that downloads or displays unwanted ads when a user is online or redirects search requests to certain advertising websites. Botnets [are] networks of computers infected by malware and controlled remotely by cybercriminals, usually for financial gain or to launch attacks on websites or networks. Many botnets are designed to harvest data, such as passwords, Social Security numbers, credit card numbers, and other personal information…Rootkit [is] a type of malware that opens a permanent "back door" into a computer system. Once installed, a rootkit will allow additional viruses to infect a computer as various hackers find the vulnerable computer exposed and compromise it. Spyware [is] a type of malware that quietly gathers a user's sensitive information (including browsing and computing habits) and reports it to unauthorized third parties. Trojan [is] a type of malware that disguises itself as a normal file to trick a user into downloading it in order to gain unauthorized access to a computer. Virus [is] a program that spreads by first infecting files or the system areas of a computer or network router's hard drive and then making copies of itself. Some viruses are harmless, others may damage data files, and some may destroy files entirely. Worm [is] a type of malware that replicates itself over and over within a computer.").

[25] *See* CISA, Ransomware 101, *available at* https://www.cisa.gov/stopransomware/ransomware-101 ("Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. In recent years, ransomware incidents have become increasingly prevalent among the Nation's state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations.").

[26] *See, e.g.*, Federal Bureau of Investigation ("FBI"), *Internet Crime Report (2021)*, *available at* https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf ("FBI Internet Crime Report") ("Ransomware is a type of malicious software, or malware, that encrypts data on a computer, making it unusable. A malicious cyber criminal holds the data hostage until the ransom is paid. If the ransom is not paid, the victim's data remains unavailable. Cyber criminals may also pressure victims to pay the ransom by threatening to destroy the victim's data or to release it to the public.").

crypto assets.[27] It is a common tactic used against the financial sector.[28] Commission staff has observed that this tactic has increasingly been employed against certain Market Entities.[29]

Another group of tactics are various social engineering schemes. In a social engineering attack, the threat actor uses social skills to convince an individual to provide access or information that can be used to access an information system.[30] "Phishing" is a variation of a social engineering attack in which an email is used to convince an individual to provide information (*e.g.*, personal or account information or log-in credentials) that can be used to gain unauthorized access to an information system.[31] Threat actors also use websites to perform phishing attacks.[32] "Spear phishing" is a variation of phishing that targets a specific individual or

---

27 *See, e.g.*, Institute for Security and Technology, *Combating Ransomware: A Comprehensive Framework For Action: Key Recommendations from the Ransomware Task Force* (Apr. 2021), *available at* https://securityandtechnology.org/ransomwaretaskforce/report ("The explosion of ransomware as a lucrative criminal enterprise has been closely tied to the rise of Bitcoin and other cryptocurrencies, which use distributed ledgers, such as blockchain, to track transactions.").

28 *See, e.g.*, FBI Internet Crime Report (stating that it received 649 complaints that indicated organizations in the sixteen U.S. critical infrastructure sectors were victims of a ransomware attack, with the financial sector being the source of the second largest number of complaints).

29 *See,* Office of Compliance, Inspections and Examinations (now the Division of Examinations ("EXAMS")), Commission, Risk Alert, *Cybersecurity: Ransomware Alert* (July 10, 2020), *available at* https://www.sec.gov/files/Risk%20Alert%20-%20Ransomware.pdf ("EXAMS Ransomware Risk Alert") (observing an apparent increase in sophistication of ransomware attacks on Commission registrants, including broker-dealers). Any staff statements represent the views of the staff. They are not a rule, regulation, or statement of the Commission. Furthermore, the Commission has neither approved nor disapproved their content. These staff statements, like all staff statements, have no legal force or effect: they do not alter or amend applicable law; and they create no new or additional obligations for any person.

30 *See, e.g.*, *CISA, Security Tip (ST04-014) – Avoiding Social Engineering and Phishing Attacks*, *available at* https://www.cisa.gov/uscert/ncas/tips/ST04-014 ("CISA Security Tip (ST04-014)").

31 *See, e.g.*, CISA Security Tip (ST04-014); Microsoft Report ("Phishing is the most common type of malicious email observed in our threat signals. These emails are designed to trick an individual into sharing sensitive information, such as usernames and passwords, with an attacker. To do this, attackers will craft emails using a variety of themes, such as productivity tools, password resets, or other notifications with a sense of urgency to lure a user to click on a link.").

32 *See, e.g.*, Microsoft Report ("The phishing webpages used in these attacks may utilize malicious domains, such as those purchased and operated by the attacker, or compromised domains, where the attacker abuses a vulnerability in a legitimate website to host malicious content. The phishing sites frequently copy well-known, legitimate login pages, such as Office 365 or Google, to trick users into inputting their credentials. Once the user inputs their credentials, they will often be redirected to a legitimate final site—such as the real Office 365 login page—leaving the user unaware that actors have obtained their credentials. Meanwhile, the entered credentials are stored or sent to the attacker for later abuse or sale.").

group.[33] "Vishing" and "smishing" are variations of social engineering that use phone communications or text messages, respectively, for this purpose.[34] These social engineering tactics also are used to deceive the recipient of an electronic communication (*e.g.*, an email or text message) to open a link or attachment in the communication that uploads malware on to the recipient's information systems.[35]

In addition to malware and social engineering, threat actors may try to circumvent or thwart the information system's logical security mechanisms (*i.e.*, to "hack" the system).[36] There are many variations of hacking.[37] One tactic is a "brute force" attack in which the threat actor attempts to determine an unknown value (*e.g.*, log-in credentials) using an automated process that tries a large number of possible values.[38] The Commission staff has observed that a variation of this tactic has increasingly been employed by threat actors against certain Market

---

33 *See, e.g.*, U.S. Office of the Director of National Intelligence, *Spear Phishing and Common Cyber Attacks*, *available at* https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Spearphishing.pdf ("ODNI Spear Phishing Alert") ("A spear phishing attack is an attempt to acquire sensitive information or access to a computer system by sending counterfeit messages that appear to be legitimate. 'Spear phishing' is a type of phishing campaign that targets a specific person or group and often will include information known to be of interest to the target, such as current events or financial documents. Like other social engineering attacks, spear phishing takes advantage of our most basic human traits, such as a desire to be helpful, provide a positive response to those in authority, a desire to respond positively to someone who shares similar tastes or views, or simple curiosity about contemporary news and events.").

34 *See, e.g.*, CISA Security Tip (ST04-014).

35 *See, e.g.*, ODNI Spear Phishing Alert ("The goal of spear phishing is to acquire sensitive information such as usernames, passwords, and other personal information. When a link in a phishing e-mail is opened, it may open a malicious site, which could download unwanted information onto a user's computer. When the user opens an attachment, malicious software may run which could compromise the security posture of the host. Once a connection is established, the attacker is able to initiate actions that could compromise the integrity of your computer, the network it resides on, and data.").

36 *See* Verizon DBIR (definition of "hacking"); *see also* NIST Glossary (defining a "hacker" as an "unauthorized user who attempts to or gains access to an information system").

37 *See, e.g.*, Web Application Security Consortium, *WASC Threat Classification: Version 2.00* (1/1/2010), *available at* https://projects.webappsec.org/f/WASC-TC-v2_0.pdf ("WASC Classification Report").

38 *See, e.g.*, WASC Classification Report ("The most common type of a brute force attack in web applications is an attack against log-in credentials. Since users need to remember passwords, they often select easy to memorize words or phrases as passwords, making a brute force attack using a dictionary useful. Such an attack attempting to log-in to a system using a large list of words and phrases as potential passwords is often called a 'word list attack' or a 'dictionary attack.'").

Entities to access their customers' accounts.[39] The ability of threat actors to hack into information systems can be facilitated by vulnerabilities in information systems, including for example the software run on the systems.[40]

Threat actors also cause harmful cybersecurity incidents through denial-of-service ("DoS") attacks.[41] This type of attack may involve botnets or compromised servers sending "junk" data or messages to an information system that a Market Entity uses to provide services to

---

[39] *See* EXAMS, Commission, Risk Alert, *Cybersecurity: Safeguarding Client Accounts against Credential Compromise* (Sept. 15, 2020), *available at* https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf ("EXAMS Safeguarding Client Accounts Risk Alert") ("The Office of Compliance Inspections and Examinations ('OCIE') has observed in recent examinations an increase in the number of cyber-attacks against SEC-registered investment advisers ('advisers') and brokers and dealers ('broker-dealers,' and together with advisers, 'registrants' or 'firms') using credential stuffing. Credential stuffing is an automated attack on web-based user accounts as well as direct network login account credentials. Cyber attackers obtain lists of usernames, email addresses, and corresponding passwords from the dark web and then use automated scripts to try the compromised user names and passwords on other websites, such as a registrant's website, in an attempt to log in and gain unauthorized access to customer accounts.").

[40] *See, e.g.*, CISA, *Alert (AA22-117A): 2021 Top Routinely Exploited Vulnerabilities*, available at https://www.cisa.gov/uscert/ncas/alerts/aa22-117a ("CISA 2021 Vulnerability Report") ("Globally, in 2021, malicious cyber actors targeted internet-facing systems, such as email servers and virtual private network (VPN) servers, with exploits of newly disclosed vulnerabilities. For most of the top exploited vulnerabilities, researchers or other actors released proof of concept (POC) code within two weeks of the vulnerability's disclosure, likely facilitating exploitation by a broader range of malicious actors. To a lesser extent, malicious cyber actors continued to exploit publicly known, dated software vulnerabilities—some of which were also routinely exploited in 2020 or earlier. The exploitation of older vulnerabilities demonstrates the continued risk to organizations that fail to patch software in a timely manner or are using software that is no longer supported by a vendor."). To address this risk, CISA maintains a Known Exploited Vulnerability (KEV) catalogue that identifies known vulnerabilities. *See, e.g.*, CISA, *Reducing The Significant Risk of Known Exploited Vulnerabilities*, *available at* https://www.cisa.gov/known-exploited-vulnerabilities ("CISA strongly recommends all organizations review and monitor the KEV catalog and prioritize remediation of the listed vulnerabilities to reduce the likelihood of compromise by known threat actors.").

[41] *See* CISA, *Security Tip (ST04-015) – Understanding Denial-of-Service Attacks*, *available at* https://www.cisa.gov/uscert/ncas/tips/ST04-015 ("A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. DoS attacks can cost an organization both time and money while their resources and services are inaccessible.").

investors, market participants, or other Market Entities causing the system to fail or be unable to process operations in a timely manner. DoS attacks are a commonly used tactic.[42]

The tactics, techniques, and procedures employed by threat actors can impact the information systems a Market Entity operates directly (*e.g.*, a web application or email system).[43] They also can adversely impact the Market Entity and its information systems through its connection to information systems operated by third-parties such as service providers (*e.g.*, cloud service providers), business partners, customers, counterparties, members, registrants, or users.[44] Further, the tactics, techniques, and procedures employed by threat actors can adversely impact the Market Entity and its information systems through its connection to information systems operated by utilities or central platforms to which the Market Entity is connected (*e.g.*, a securities exchange, securities trading platform, securities clearing agency, or a payment processor).[45]

If cybersecurity risk materializes into a significant cybersecurity incident, a Market Entity may lose its ability to perform a key function causing harm to the Market Entity, investors, or other market participants. Moreover, given the interconnectedness of Market Entities' information systems, a significant cybersecurity incident at one Market Entity has the potential to spread to other Market Entities in a cascading process that could cause widespread disruptions

---

42 *See* Verizon DBIR (finding that DoS attacks represented 46% of the total cybersecurity incidents analyzed).

43 *See, e.g.*, Verizon DBIR (finding that the top assets breached in cyber security incidents are servers hosting web applications and emails, and stating that because they are "internet-facing" they "provide a useful venue for attackers to slip through the organization's 'perimeter'").

44 *See, e.g.*, Ponemon Institute LLC, *The Cost of Third-Party Cybersecurity Risk Management* (Mar. 2019), *available at* https://info.cybergrx.com/ponemon-report ("Third-party breaches remain a dominant security challenge for organizations, with over 63% of breaches linked to a third party.").

45 *See, e.g.*, Financial Markets Authority, New Zealand, *Market Operator Obligations Targeted Review – NZX* (January 2021), *available at* https://www.fma.govt.nz/assets/Reports/Market-Operator-Obligations-Targeted-Review-NZX.pdf ("New Zealand FMA Report") (describing an August 2020 cybersecurity incident at New Zealand's only regulated financial product market that caused a trading halt of approximately four days).

threatening the fair, orderly, and efficient operation of the U.S. securities markets.[46] Further, the disruption of a Market Entity that provides critical services to other Market Entities through connected information systems could cause cascading disruptions to those other Market Entities to the extent they cannot obtain those critical services from another source.[47]

A significant cybersecurity incident also can result in unauthorized access to and use of personal, confidential, or proprietary information.[48] In the case of personal information, this can cause harm to investors and others whose personal information was accessed or used (*e.g.*, identity theft).[49] This could lead to theft of investor assets. In the case of confidential or proprietary information, this can cause harm to the business of the person whose proprietary information was accessed or used (*e.g.*, public exposure of trading positions or business strategies) or provide the unauthorized user with an unfair advantage over other market participants (*e.g.*, trading based on confidential business information). Unauthorized access to proprietary information also can lead to theft of a Market Entity's valuable intellectual property.

Cybersecurity incidents affecting Market Entities can cause substantial harm to other market participants, including investors. For example, significant cybersecurity incidents caused

---

46 *See, e.g.*, Implications of Cyber Risk for Financial Stability ("Cyber shocks can lead to losses hitting many firms at the same time because of correlated risk exposures (sometimes called the popcorn effect), such as when firms load the same malware-infected third-party software update."); The Bank for International Settlements, Committee on Payments and Market Infrastructures ("CPMI") and IOSCO, *Guidance on cyber resilience for financial market infrastructures* (June 2016), *available at* https://www.bis.org/cpmi/publ/d146.pdf ("[T]here is a broad range of entry points through which a [financial market intermediary ("FMI")] could be compromised. As a result of their interconnectedness, cyber attacks could come through an FMI's participants, linked FMIs, service providers, vendors and vendor products . . . . Because an FMI's systems and processes are often interconnected with the systems and processes of other entities within its ecosystem, in the event of a large-scale cyber incident it is possible for an FMI to pose contagion risk (i.e., propagation of malware or corrupted data) to, or be exposed to contagion risk from, its ecosystem.").

47 *See, e.g.*, Implications of Cyber Risk for Financial Stability ("And the interconnectedness of the financial system means that an event at one or more firms may spread to others (the domino effect). For example, a cyber event at a single bank can disrupt the bank's ability to send payments and have cascading effects on other banks' liquidity and operations.").

48 *See, e.g.*, Bank of England CBEST Report ("One class of targeted attack is Computer Network Exploitation (CNE) where the goal is to steal (or exfiltrate) confidential information from the target. This is effectively espionage in cyberspace or, in information security terms, compromising confidentiality.").

49 The NIST Glossary defines "identity fraud or theft" as "all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain."

by malware can cause the loss of the Market Entity's data, or the data of other market participants.[50] These incidents also can lead to business disruptions that are not just costly to the Market Entity but also the other market participants that rely on the Market Entity's services.

A Market Entity also may incur substantial remediation costs due to a significant cybersecurity incident.[51] For example, the incident may result in reimbursement to other market participants for cybersecurity-related losses and payment for their use of identity protection services. A Market Entity's failure to protect itself adequately against a significant cybersecurity incident also may increase its insurance premiums. In addition, a significant cybersecurity incident may expose a Market Entity to litigation costs (*e.g.*, to defend lawsuits brought by individuals whose personal information was stolen), regulatory scrutiny, reputational damage, and, if a result of a compliance failure, penalties. Finally, a sufficiently severe significant cybersecurity incident could cause the failure of a Market Entity. Given the interconnectedness of Market Entities, a significant cybersecurity incident that degrades or disrupts the critical functions of one Market Entity could cause harm to other Market Entities (*e.g.*, by cutting off their access to a critical service such as securities clearance or by exposing them to the same malware that degraded or disrupted the critical functions of the first Market Entity). This could lead to market-wide outages that compromise the fair, orderly, and efficient functioning of the U.S. securities markets.

---

[50] CISA, *Cyber Essentials Starter Kit – The Basics for Building a Culture of Cyber Readiness* (Spring 2021), *available at* https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Starter%20Kit_03.12.2021_508_0.pdf ("CISA Cyber Essentials Starter Kit") ("Malware is designed to spread quickly. A lack of defense against it can completely corrupt, destroy or render your data inaccessible.").

[51] *See*, *e.g.*, IBM Security, *Cost of Data Breach Report 2022*, *available at* https://www.ibm.com/security/data-breach (noting the average cost of a data breach in the financial industry is $5.97 million); FBI Internet Crime Report (noting that cybercrime victims lost approximately $6.9 billion in 2021).

For these reasons, the Commission is proposing new rule requirements that are designed to protect the U.S. securities markets and investors in these markets from the threat posed by cybersecurity risks.[52]

2. Critical Operations of Market Entities are Exposed to Cybersecurity Risk

The fair, orderly, and efficient operation of the U.S. securities markets depends on Market Entities performing various functions without disruption. Market Entities rely on information systems and networks of interconnected information systems to perform their functions. This exposes them to the harms that can be caused by threat actors using the tactics, techniques, and procedures discussed above (among others) and by errors of employees or third-party service providers (among others). The GAO has stated that the primary cybersecurity risks

---

[52] The Commission has pending proposals to address cybersecurity risk with respect to investment advisers, investment companies, and public companies. *See Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies*, Release Nos. 33-11028, 34-94917, IA-5956, IC-34497 (Feb. 9, 2022) [87 FR 13524, (Mar. 9, 2022)] ("Investment Management Cybersecurity Release"); *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, Release Nos. 33-11038, 34-94382, IC-34529 (Mar. 9, 2022) [87 FR 16590 (Mar. 23, 2022)]. In addition, as discussed in more detail below in section II.F. of this release, the Commission is proposing to amend Regulation SCI (17 CFR 242.1000 through 1007) and Regulation S-P (17 CFR 248.1 through 248.30) concurrent with this release. *See Regulation Systems Compliance and Integrity*, Release No. 34-97143 (Mar. 15, 2023) (File No. S7-07-23) ("Regulation SCI 2023 Proposing Release"); *Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information*, Release Nos. 34-97141, IA-6262, IC-34854 (Mar. 15, 2023) (File No. S7-05-23) ("Regulation S-P 2023 Proposing Release"). The Commission encourages commenters to review the proposals with respect to Regulation SCI and Regulation S-P to determine whether they might affect their comments on this proposing release. *See also* section II.F. of this release (seeking specific comment on how the proposals in this release would interact with Regulation SCI and Regulation S-P as they currently exist and would be amended). Further, the Commission has reopened the comment period for the Investment Management Cybersecurity Release to allow interested persons additional time to analyze the issues and prepare their comments in light of other regulatory developments, including the proposed rules and amendments regarding this proposal, the Regulation SCI 2023 Proposing Release and the Regulation S-P 2023 Proposing Release that the Commission should consider in connection with the Investment Management Cybersecurity Release. *See Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies; Reopening of Comment Period*, Release Nos. 33-11167, 34-97144, IA-6263, IC-34855 (Mar. 15, 2023), [88 FR 16921 (Mar. 31, 2023)]. The Commission encourages commenters to review the Investment Management Cybersecurity Release and the comments on that proposal to determine whether they might affect their comments on this proposing release. The comments on the Investment Management Cybersecurity Release are available at: https://www.sec.gov/comments/s7-04-22/s70422.htm. Lastly, the Commission also proposed rules and amendments regarding an investment adviser's obligations with respect to outsourcing certain categories of "covered functions," including cybersecurity. *See Outsourcing by Investment Advisers*, Release No. IA-6176 (Oct. 26, 2022), [87 FR 68816 (Nov. 16, 2022)]. The Commission encourages commenters to review that proposal to determine whether it might affect comments on this proposing release.

identified by financial sector firms are: (1) internal actors;[53] (2) malware;[54] (3) social engineering;[55] and (4) interconnectivity.[56] As discussed below, a significant cybersecurity incident can cause serious harm to Market Entities and others who use their services or are connected to them through information systems and, if severe enough, negatively impact the fair, orderly, and efficient operations of the U.S. securities markets.

a. Common Uses of Information Systems by Market Entities

Market Entities need accurate and accessible books and records, among other things, to manage and conduct their operations, manage and mitigate their risks, monitor the progress of their business, track their financial condition, prepare financial statements, prepare regulatory filings, and prepare tax returns. Increasingly, these records are made and preserved on information systems.[57] These recordkeeping information systems also store personal, confidential, and proprietary business information about the Market Entity and its customers, counterparties, members, registrants, or users.

The complexity and scope of these books and records systems ranges from ones used by large Market Entities that comprise networks of systems that track thousands of different types of daily transactions (*e.g.*, securities trades and movements of assets) to ones used by small Market

---

53 *See* GAO Cybersecurity Report ("Risks due to insider threats involve careless, poorly trained, or disgruntled employees or contractors hired by an organization who may intentionally or inadvertently introduce vulnerabilities or malware into information systems. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. Results of insider threats can include data destruction and account compromise.").

54 *Id.* ("The risk of malware exploits impacting the [financial] sector has increased as malware exploits have grown in sophistication").

55 *Id.* ("The financial services sector is at risk due to social engineering attacks, which include a broad range of malicious activities accomplished through human interaction that enable attackers to gain access to sensitive data by convincing a legitimate, authorized user to give them their credentials and/or other personal information").

56 *Id.* ("Interconnectivity involves interdependencies throughout the financial services sector and the sharing of data and information via networks, the cloud, and mobile applications. Organizations in the financial services sector utilize data aggregation hubs and cloud service providers, and new financial technologies such as algorithms based on consumers' data and risk preferences to provide digital services for investment and financial advice.").

57 Some Market Entities may store certain or all of their records in paper format. This discussion pertains to recordkeeping systems that store records electronically on information systems.

Entities comprising off-the-shelf accounting software and computer files on a desktop computer. In either case, the impact on the confidentiality, integrity, or availability of the information system being compromised as a consequence of a significant cybersecurity incident can be devastating to the Market Entity and its customers, counterparties, members, registrants or users. For example, it could cause the Market Entity to cease operations or allow threat actors to use personal information about the customers of the Market Entity to steal their identities.

Market Entities also use information systems so that their employees can communicate with each other and with external persons. These include email, text messaging, and virtual meeting applications. The failure of these information systems as a result of a significant cybersecurity incident can seriously disrupt the Market Entity's ability to carry out its functions. Moreover, these outward facing information systems are vectors that threat actors use to cause harmful cybersecurity incidents by, for example, tricking an employee through social engineering into downloading malware in an attachment to an email.

b. Broker-Dealers

Broker-dealers perform a number of functions in the U.S. securities markets, including underwriting the issuance of securities for publicly and privately held companies, making markets in securities, brokering securities transactions, dealing securities, operating an ATS, executing securities transactions, clearing and settling securities transactions, and maintaining custody of securities for investors. Some broker-dealers may perform multiple functions; whereas others may perform a single function. Increasingly, these functions are performed through the use of information systems. For example, broker-dealers use information systems to connect to securities exchanges, ATSs, and other securities markets in order to transmit purchase and sell orders. Broker-dealers also use information systems to connect to clearing agencies or clearing broker-dealers to transmit securities settlement instructions and transfer funds. They use information systems to communicate and transact with other broker-dealers. In addition, they use information systems to provide securities services to investors, including information

systems that investors use to access their securities accounts and transmit orders to purchase or sell securities.

Depending on the functions undertaken by a broker-dealer, a significant cybersecurity incident could affect customers, including retail investors. For example, a significant cybersecurity incident could result in the broker-dealer experiencing a systems outage, which in turn could leave customers unable to purchase or sell securities held in their account and the broker-dealer unable to trade for itself. In addition, broker-dealers maintain records and information related to their customers that include personal information, such as names, addresses, phone numbers, employer information, tax identification information, bank information, and other detailed and individualized information related to broker-dealer obligations under applicable statutory and regulatory provisions.[58] If personal information held by a broker-dealer is accessed or stolen by unauthorized users, it could result in harm (*e.g.*, identity theft or conversion of financial assets) to many individuals, including retail investors.

Further, a significant cybersecurity incident at a broker-dealer could provide a gateway for threat actors to attack the self-regulatory organizations ("SROs")—such as national securities exchanges and registered clearing agencies—ATSs, and other broker-dealers to which the firm is connected through information systems and networks of interconnected information systems.[59] This could cause a cascading effect where a significant cybersecurity incident initially impacting one broker-dealer spreads to other Market Entities. Moreover, the information systems that link a broker-dealer to other Market Entities, its customers, and other service providers are vectors

---

[58] *See, e.g.*, 17 CFR 240.17a-3(a)(17) (requiring broker-dealers to make account records of the customer's or owner's name, tax identification number, address, telephone number, date of birth, employment status, annual income, net worth, and the account's investment objectives). Broker-dealers also must comply with relevant anti-money laundering (AML) laws, rules, orders, and guidance. *See, e.g.*, Commission, *Anti-Money Laundering (AML) Source Tool for Broker-Dealers*, (May 16, 2022), *available at* https://www.sec.gov/about/offices/ocie/amlsourcetool.

[59] Section 3(a)(26) of the Exchange Act defines a self-regulatory organization as any national securities exchange, registered securities association, registered clearing agency, or (with limitations) the MSRB. *See* 15 U.S.C. 78c(a)(26).

that expose the broker-dealer to cybersecurity risk arising from threats that originate in information systems outside the broker-dealer's control.

In addition, some broker-dealers operate ATSs. An ATS is a trading system for securities that meets the definition of "exchange" under federal securities laws but is not required to register with the Commission as a national securities exchange if it complies with the conditions to an exemption provided under Regulation ATS, which includes registering as a broker-dealer.[60] Registering as a broker-dealer requires becoming a member of an SRO, such as FINRA, and membership in FINRA subjects an ATS to FINRA's rules and oversight. Since Regulation ATS was adopted in 1998, ATSs' operations have increasingly relied on complex automated systems to bring together buyers and sellers for various securities, which include—for example—electronic limit order books and auction mechanisms. These developments have made ATSs significant sources of orders and trading interest for securities. ATSs employ information systems to accept, store, and match orders pursuant to pre-programmed methods and to communicate the execution of these orders for trade reporting purposes and for clearance and settlement of the transactions. ATSs, in particular ATSs that are "NMS Stock ATSs,"[61] use information systems to connect to various trading centers in order to receive market data that ATSs use to price and execute orders that are entered on the ATS. A significant cyber security incident could disrupt the ATS's critical infrastructure and significantly impede the ability of the ATS to (among other things): (1) receive market data; (2) accept, price, and match orders; or (3)

---

60 17 CFR 242.300 through 242.304. Exchange Act Rule 3a1-1(a)(2) exempts from the definition of "exchange" under Section 3(a)(1) of the Exchange Act an organization, association, or group of persons that complies with Regulation ATS. *See* 17 CFR 240.3a1-1(a)(2). Regulation ATS requires an ATS to, among other things, register as a broker-dealer, file a Form ATS with the Commission to notice its operations, and establish written safeguards and procedures to protect subscribers' confidential trading information. *See* 17 CFR 242.301(b)(1), (2), and (10), respectively. The broker-dealer operator of the ATS controls all aspects of the ATS's operations and is legally responsible for its operations and for ensuring that the ATS complies with applicable federal securities laws and the rules and regulations thereunder, including Regulation ATS. *See Regulation of NMS Stock Alternative Trading Systems*, Exchange Act Release No. 83663 (July 18, 2018) [83 FR 38768, 38819-20 (Aug. 7, 2018)] ("Regulation of NMS Stock Alternative Trading Systems Release").

61 *See* 17 CFR 242.300(k) (defining the term "NMS Stock ATS").

report transactions. This, in turn, could negatively impact the ability of ATS subscribers to trade and execute the orders of their investors or purchase certain securities at favorable or predictable prices or in a timely manner to the extent the ATS provides liquidity to the market for those securities.

c. Clearing Agencies

Clearing agencies are broadly defined in the Exchange Act and undertake a variety of functions.[62] An entity that meets the definition of a "clearing agency" is required to register with the Commission or obtain from the Commission an exemption from registration prior to performing the functions of a clearing agency.[63]

Two common functions of registered clearing agencies are operating as a central counterparty ("CCP") or a central securities depository ("CSD"). Registered clearing agencies that provide these services are "covered clearing agencies" under Commission regulations.[64] A CCP acts as the buyer to every seller and the seller to every buyer, providing a trade guaranty with respect to transactions submitted for clearing by the clearing agency's participants.[65] A CSD acts as a depository for handling securities, whereby all securities of a particular class or series of any issuer deposited within the system are treated as fungible. Market Entities may use a CSD to transfer, loan, or pledge securities by bookkeeping entry without the physical delivery of certificates. A CSD also may permit or facilitate the settlement of securities transactions more

---

62 *See* 15 U.S.C. 78c(a)(23)(A).

63 *See* 15 U.S.C. 78q-1(b); 17 CFR 240.17Ab2–1.

64 *See* 17 CFR 240.17Ad-22. *See also Standards for Covered Clearing Agencies*, Exchange Act Release No. 78961 (Sept. 28, 2016) [81 FR 70786, 70793 (Oct. 13, 2016)] ("CCA Standards Adopting Release"). As discussed below, some clearing agencies operate pursuant to Commission exemptions from registration.

65 *See* 17 CFR 240.17Ad-22 ("Rule 17Ad-22"); *Definition of "Covered Clearing Agency"*, Exchange Act Release No. 88616 (Apr. 9, 2020) [85 FR 28853, 28855-56 (May 14, 2020)] ("CCA Definition Adopting Release").

generally.[66] Currently, all clearing agencies registered with the Commission that are actively providing clearance and settlement services are covered clearing agencies.[67]

Registered clearing agencies also are SROs under section 19 of the Exchange Act, and their proposed rules are subject to Commission review and published for notice and comment. While certain types of proposed rules are effective upon filing, others are subject to Commission approval before they can go into effect.

Additionally, section 17A(b)(1) of the Exchange Act provides the Commission with authority to exempt a clearing agency or any class of clearing agencies ("exempt clearing agencies") from any provision of section 17A or the rules or regulations thereunder.[68] An exemption may be effected by rule or order, upon the Commission's own motion or upon application, and conditionally or unconditionally.[69] The Commission has provided exemptions from registration as a clearing agency for clearing agencies that provide matching services.[70]

---

66 *See* 15 U.S.C. 78c(a)(23)(A); 17 CFR 240.17Ad-22; CCA Definition Adopting Release, 81 FR at 28856.

67 The active covered clearing agencies are: (1) The Depository Trust Company ("DTC"); (2) Fixed Income Clearing Corporation ("FICC"); (3) National Securities Clearing Corporation ("NSCC"); (4) Intercontinental Exchange, Inc. ("ICE") Clear Credit LLC ("ICC"); (5) ICE Clear Europe Limited ("ICEEU"); (6) The Options Clearing Corporation ("Options Clearing Corp."); and (7) LCH SA. Certain clearing agencies are registered with the Commission but are not covered clearing agencies. *See* CCA Standards Adopting Release, 81 FR at 70793. In particular, although subject to paragraph (d) of Rule 17Ad-22, the Boston Stock Exchange Clearing Corporation ("BSECC") and Stock Clearing Corporation of Philadelphia ("SCCP") are currently registered with the Commission as clearing agencies but conduct no clearance or settlement operations. *See Self-Regulatory Organizations; The Boston Stock Clearing Corporation; Notice of Filing and Immediate Effectiveness of Proposed Rule Change To Amend the Articles of Organization and By-Laws*, Exchange Act Release No. 63629 (Jan. 3, 2011) [76 FR 1473, 1474 (Jan. 10, 2011)] ("BSECC Notice"); *Self-Regulatory Organizations; Stock Clearing Corporation of Philadelphia; Notice of Filing and Immediate Effectiveness of Proposed Rule Change Relating to the Suspension of Certain Provisions Due to Inactivity*, Exchange Act Release No. 63268 (Nov. 8, 2010) [75 FR 69730, 69731 (Nov. 15, 2010)] ("SCCP Notice").

68 15 U.S.C. 78q-1(b)(1). *See also* 15 U.S.C. 78mm (providing the Commission with general exemptive authority).

69 *See* 15 U.S.C. 78q-1(b)(1). The Commission's exercise of authority to grant exemptive relief must be consistent with the public interest, the protection of investors, and the purposes of Section 17A of the Exchange Act, including the prompt and accurate clearance and settlement of securities transactions and the safeguarding of securities and funds.

70 *See Global Joint Venture Matching Services - US, LLC; Order Granting Exemption from Registration as a Clearing Agency*, Exchange Act Release No. 44188 (Apr. 17, 2001) [66 FR 20494 (Apr. 23, 2001)] (granting an exemption to provide matching services to Global Joint Venture Matching Services US LLC, now known as DTCC ITP Matching U.S. LLC) ("DTCC ITP Matching Order"); *Bloomberg STP LLC;*

Matching services centrally match trade information between a broker-dealer and its institutional customer. The Commission also has provided exemptions for non-U.S. clearing agencies to perform the functions of a clearing agency with respect to transactions of U.S. participants involving U.S. government and agency securities.[71]

Registered and exempt clearing agencies rely on information systems to perform the functions described above. Given their central role, the information systems operated by clearing agencies are critical to the operations of the U.S. securities markets. For registered clearing agencies, in particular, these information systems include those that set and calculate margin obligations and other charges, perform netting and calculate payment obligations,

---

SS&C Technologies, Inc.; Order of the Commission Approving Applications for an Exemption From Registration as a Clearing Agency, Exchange Act Release No. 76514 (Nov. 25, 2015) [80 FR 75388 (Dec. 1, 2015)] (granting an exemption to provide matching services to each of Bloomberg STP LLC and SS&C Technologies, Inc.) ("BSTP SS&C Order"). In addition, on July 1, 2011, the Commission published a conditional, temporary exemption from clearing agency registration for entities that perform certain post-trade processing services for security-based swap transactions. *See Order Pursuant to Section 36 of the Securities Exchange Act of 1934 Granting Temporary Exemptions From Clearing Agency Registration Requirements Under Section 17A(b) of the Exchange Act for Entities Providing Certain Clearing Services for Security-Based Swaps*, Exchange Act Release No. 34–64796 (July 1, 2011) [76 FR 39963 (July 7, 2011)]. The order facilitated the Commission's identification of entities that operate in that area and that accordingly may fall within the clearing agency definition. Recently, the Commission indicated that the 2011 Temporary Exemption may no longer be necessary. *See Rules Relating to Security-Based Swap Execution and Registration and Regulation of Security-Based Swap Execution Facilities*, Release No. 34–94615 (Apr. 6, 2022) [87 FR 28872, 28934 (May 11, 2022)] (stating that the "Commission preliminarily believes that, if it adopts a framework for the registration of [security-based swap execution facilities ("SBSEFs")], the 2011 Temporary Exemption would no longer be necessary because entities carrying out the functions of SBSEFs would be able to register with the Commission as such, thereby falling within the exemption from the definition of 'clearing agency' in existing Rule 17Ad–24.").

71 *See Euroclear Bank SA/NV; Order of the Commission Approving an Application To Modify an Existing Exemption From Clearing Agency Registration*, Exchange Act Release No. 79577 (Dec. 16, 2016) [81 FR 93994 (Dec. 22, 2016)] (providing an exemption to Euroclear Bank SA/NV (successor in name to Morgan Guaranty Trust Company of NY)) ("Euroclear Bank Order"); *Self-Regulatory Organizations; Cedel Bank; Order Approving Application for Exemption From Registration as a Clearing Agency*, Exchange Act Release No. Release No. 38328 (Feb. 24, 1997) [62 FR 9225 (Feb. 28, 1997)] (providing an exemption to Clearstream Banking, S.A. (successor in name to Cedel Bank, societe anonyme, Luxembourg)) ("Clearstream Banking Order"). Furthermore, pursuant to the Commission's statement on CCPs in the European Union ("EU") authorized under the European Markets Infrastructure Regulation ("EMIR"), an EU CCP may request an exemption from the Commission where it has determined that the application of Commission requirements would impose unnecessary, duplicative, or inconsistent requirements in light of EMIR requirements to which it is subject. *See Statement on Central Counterparties Authorized under the European Markets Infrastructure Regulation Seeking to Register as a Clearing Agency or to Request Exemptions from Certain Requirements Under the Securities Exchange Act of 1934*, Exchange Act Release No. 34-90492 (Nov. 23, 2020) [85 FR 76635, 76639 (Nov. 30, 2020)], https://www.govinfo.gov/content/pkg/FR-2020-11-30/pdf/FR-2020-11-30.pdf (stating that in seeking an exemption, an EU CCP could provide "a self-assessment. . . [to] explain how the EU CCP's compliance with EMIR corresponds to the requirements in the Exchange Act and applicable SEC rules thereunder, such as Rule 17Ad-22 and Regulation SCI.").

facilitate the movement of funds and securities, or effectuate end-of-day settlement. Certain exempt clearing agencies (*e.g.,* Euroclear and Clearstream) may provide CSD functions like covered clearing agencies while other exempt clearing agencies (*e.g.*, DTCC ITP) may not provide such functions. Nonetheless, any entity that falls within the definition of a clearing agency centralizes technology functions in a manner that increases its potential to become a single point of failure in the case of a significant cybersecurity incident.[72]

The technology behind clearing agency information systems is subject to growing innovation and interconnectedness, with multiple clearing agencies sharing links among their systems and with the systems of other Market Entities. This growing interconnectivity means that a significant cybersecurity incident at a registered clearing agency could, for example, prevent it from acting timely to carry out its functions, which, in turn, could negatively impact other Market Entities that utilize the clearing agency's services.[73] Further, a significant cybersecurity incident at a registered or exempt clearing agency could provide a gateway for threat actors to attack the members of the clearing agency and other financial institutions that connect to it through information systems. Moreover, the information systems that link the clearing agency to its members are vectors that expose the clearing agency to cybersecurity risk.

The records stored by clearing agencies on their information systems include proprietary information about their members, including confidential business information (*e.g.*, information

---

72 *See generally* Board of Governors of the Federal Reserve System ("Federal Reserve Board"), Commission, Commodity Futures Trading Commission ("CFTC"), *Risk Management of Designated Clearing Entities* (July 2011), *available at* https://www.federalreserve.gov/publications/other-reports/files/risk-management-supervision-report-201107.pdf (report to the Senate Committees on Banking, Housing, and Urban Affairs and Agriculture, Nutrition, and Forestry and the House Committees on Financial Services and Agriculture stating that a designated clearing entity ("DCE") "faces two types of non-financial risks – operational and legal – that may disrupt the functioning of the DCE. . . . DCEs face operational risk from both internal and external sources, including human error, system failures, security breaches, and natural or man-made disasters.").

73 *See also* EXAMS, Commission, *Staff Report on the Regulation of Clearing Agencies* (Oct. 1, 2020), *available at* https://www.sec.gov/files/regulation-clearing-agencies-100120.pdf (staff stating that "consolidation among providers of clearance and settlement services concentrates clearing activity in fewer providers and has increased the potential for providers to become single points of failure.").

about the financial condition of the members used by the clearing agency to manage credit risk). Each clearing agency also is required to keep all records made or received by it in the course of its business and in the conduct of its self-regulatory activity. A significant cybersecurity incident at a clearing agency could lead to the improper use of this information to harm the members (*e.g.*, public exposure of confidential financial information) or provide the unauthorized user with an unfair advantage over other market participants (*e.g.*, trading based on confidential business information). Moreover, a disruption to a registered clearing agency's operations as a result of a significant cybersecurity incident could interfere with its ability to perform its responsibilities as an SRO (*e.g.*, interrupting its oversight of clearing member activities for compliance with its rules and the federal securities laws), and, therefore, materially impact the fair, orderly, and efficient functioning of the U.S. securities markets.

d. The Municipal Securities Rulemaking Board

The MSRB is an SRO that serves as a regulator of the U.S. municipal securities market with a mandate to protect municipal securities investors, municipal entities, obligated persons, and the public interest.[74] Pursuant to the Exchange Act, the MSRB shall propose and adopt rules with respect to transactions in municipal securities effected by broker-dealers and municipal securities dealers and with respect to advice provided to or on behalf of municipal entities or obligated persons by broker-dealers, municipal securities dealers, and municipal advisors with respect to municipal financial products, the issuance of municipal securities, and solicitations of municipal entities or obligated persons undertaken by broker-dealers, municipal securities dealers, and municipal advisors.[75] Pursuant to the Exchange Act, the MSRB's rules shall be designed to prevent fraudulent and manipulative acts and practices, to promote just and equitable principles of trade, to foster cooperation and coordination with persons engaged in regulating,

---

[74] *See* 15 U.S.C. 78o-4. Information about the MSRB and its functions is available at: www.msrb.org.

[75] *See* 15.U.S.C. 78o-4(b)(2).

clearing, settling, processing, information with respect to, and facilitating transactions in municipal securities and municipal financial products, to remove impediments to and perfect the mechanism of a free and open market in municipal securities and municipal products, and in general, to protect investors, municipal entities, obligated persons, and the public interest.[76] As an SRO, the MSRB's proposed rules are subject to Commission review and published for notice and comment. While certain types of proposed rules are effective upon filing, others are subject to Commission approval before they can go into effect.

The MSRB relies on information systems to carry out its mission regulating broker-dealers, municipal securities dealers, and municipal advisors. For example, the MSRB operates the Electronic Municipal Market Access website ("EMMA"). EMMA provides transparency to the U.S. municipal bond market by disclosing free information on virtually all municipal bond offerings, including real-time trade prices, bond disclosure documents, and certain market statistics.[77] The MSRB also provides data to the Commission, broker-dealer examining authorities, and banking supervisors to assist in their examination and enforcement efforts involving participants in the municipal securities markets. The MSRB also maintains other data on the U.S. municipal securities markets. This data can be used by the public and others to understand better these markets. The MSRB is also required to keep all records made or received by it in the course of its business and in the conduct of its self-regulatory activity.

A significant cybersecurity incident could disrupt the operation of EMMA and could negatively impact the fair, orderly, and efficient operation of the U.S. municipal securities

---

[76] *See* 15.U.S.C. 78o-4(b)(2)(C).

[77] Broker- dealers, and municipal securities dealers that trade municipal securities are subject to transaction reporting obligations under MSRB Rule G–14. EMMA, established by the MSRB in 2009, is currently designated by the Commission as the official repository of municipal securities disclosure providing the public with free access to relevant municipal securities data, and is the central database for information about municipal securities offerings, issuers, and obligors. Additionally, the MSRB's Real-Time Transaction Reporting System ("RTRS"), with limited exceptions, requires broker-dealers and municipal securities dealers to submit transaction data to the MSRB within 15 minutes of trade execution, and such near real-time post-trade transaction data can be accessed through the MSRB's EMMA website.

market. For example, the loss or corruption of transparent price information could cause investors to stop purchasing or selling municipal securities or negatively impact the ability of investors to liquidate or purchase municipal securities at favorable or predictable prices or in a timely manner. In addition, the unauthorized access or use of personal or proprietary information of the persons who are registered with the MSRB could cause them harm through identity theft or the disclosure of confidential business information.

Further, a significant cybersecurity incident impacting the MSRB could provide a gateway for threat actors to attack registrants that connect to the MRSB through information systems and networks of interconnected information systems. Moreover, the information systems that link the MSRB to its registrants are vectors that expose the MSRB to cybersecurity risk.

e. National Securities Associations

A national securities association is an SRO created to regulate broker-dealers and the off-exchange broker-dealer market.[78] Currently, FINRA is the only national securities association registered under section 15A of the Exchange Act. As a national securities association, FINRA must have rules for its members that, among other things, are designed to prevent fraudulent and manipulative acts and practices, to promote just and equitable principles of trade, to foster cooperation and coordination with persons engaged in regulating, clearing, settling, or processing information with respect to (and facilitating transactions in) securities, to remove impediments to and perfect the mechanism of a free and open market and a national market system, and, in general, to protect investors and the public interest.[79] FINRA's rules also must provide for discipline of its members for violations of any provision of the Exchange Act, Exchange Act

---

[78] *See* 15 U.S.C. 78o-3(a); *Exemption for Certain Exchange Members*, Exchange Act Release No. 95388 (July 29, 2022) [87 FR 49930 (Aug. 12, 2022)] (proposing amendments to national securities association membership exemption for certain exchange members).

[79] *See* 15 U.S.C. 78o-3(b)(6).

rules, the rules of the MSRB, or its own rules.[80] A national securities association is an SRO under section 19 of the Exchange Act, and its proposed rules are subject to Commission review and are published for notice and comment. While certain types of proposed FINRA rules are effective upon filing, others are subject to Commission approval before they can go into effect.

FINRA also performs other functions of vital importance to the U.S. securities markets. It developed and operates the Trade Reporting and Compliance Engine ("TRACE"), which facilitates the mandatory reporting of over-the-counter transactions in eligible fixed-income securities.[81] In addition, FINRA operates the Trade Reporting Facility ("TRF"). FINRA members report over-the-counter transactions in national market system ("NMS") stocks to the TRF, which are then included in publicly disseminated consolidated equity market data pursuant to an NMS plan.[82] Further, pursuant to plans declared effective by the Commission under Exchange Act Rule 17d-2 ("Rule 17d-2"),[83] FINRA frequently acts as the sole SRO with regulatory responsibility with respect to certain applicable laws, rules, and regulations for its members that are also members of other SROs (*e.g.*, national securities exchanges).[84] Some of these Rule 17d-2 plans facilitate the conduct of market-wide surveillance, including for insider

---

80 *See* 15 U.S.C. 78o-3(b)(7).

81 FINRA members are subject to transaction reporting obligations under FINRA Rule 6730. This rule requires FINRA members to report transactions in TRACE-Eligible Securities, which the rule defines to include a range of fixed-income securities.

82 In addition, FINRA operates the Alternative Display Facility ("ADF"), which allows members to display quotations and report trades in NMS stocks. Although there are currently no users of the ADF, FINRA has issued a pre-quotation notice advising that a new participant intends to begin using the ADF, subject to regulatory approval. *See Self-Regulatory Organizations; Financial Industry Regulatory Authority, Inc.; Notice of Filing of a Proposed Rule Change Relating to Alternative Display Facility New Entrant*, Exchange Act Release No. 96550 (Dec. 20, 2022) [87 FR 79401 (Dec. 27, 2022)].

83 17 CFR 240.17d-2. Pursuant to a plan declared effective by the Commission under Rule 17d-2, the Commission relieves an SRO of those regulatory responsibilities allocated by the plan to another SRO.

84 *See, e.g., Program for Allocation of Regulatory Responsibilities Pursuant to Rule 17d-2; Notice of Filing and Order Approving and Declaring Effective an Amended Plan for the Allocation of Regulatory Responsibilities Between the Financial Industry Regulatory Authority, Inc. and MEMX LLC*, Exchange Act Release No. 96101 (Oct. 18, 2022) [87 FR 64280 (Oct. 24, 2022)].

trading.[85] The disruption of these FINRA activities by a significant cybersecurity incident could interfere with its ability to carry out its regulatory responsibilities (*e.g.*, disclosing confidential information pertaining to its surveillance of trading activity), and, therefore, materially impact the fair, orderly, and efficient functioning of the U.S. securities markets.

FINRA uses other information systems to perform its responsibilities as an SRO. For example, it operates a number of information systems that its members use to make regulatory filings.[86] These systems include the FINRA's eFOCUS system through which its broker-dealer members file periodic (monthly or quarterly) confidential financial and operational reports.[87] FINRA Gateway is another information system that it uses as a compliance portal for its members to file and access information. A disruption of FINRA's business operations caused by a significant cybersecurity incident could disrupt its ability to carry out its responsibilities as an SRO (*e.g.*, by disrupting its oversight of broker-dealer activities for compliance with its rules and the federal securities laws or its review of broker-dealers' financial condition), and could therefore materially impact the fair, orderly, and efficient functioning of the U.S. securities markets.

---

85 *See, e.g., Program for Allocation of Regulatory Responsibilities Pursuant to Rule 17d-2; Notice of Filing and Order Approving and Declaring Effective an Amendment to the Plan for the Allocation of Regulatory Responsibilities Among Cboe BZX Exchange, Inc., Cboe BYX Exchange, Inc., NYSE Chicago, Inc., Cboe EDGA Exchange, Inc., Cboe EDGX Exchange, Inc., Financial Industry Regulatory Authority, Inc., MEMX LLC, MIAX PEARL, LLC, Nasdaq BX, Inc., Nasdaq PHLX LLC, The Nasdaq Stock Market LLC, NYSE National, Inc., New York Stock Exchange LLC, NYSE American LLC, NYSE Arca, Inc., Investors' Exchange LLC, and Long-Term Stock Exchange, Inc. Relating to the Surveillance, Investigation, and Enforcement of Insider Trading Rules*, Exchange Act Release No. 89972 (Sept. 23, 2020) [85 FR 61062 (Sept. 29, 2020)].

86 Further information about these filing systems is available at: https://www.finra.org/filing-reporting/regulatory-filing-systems.

87 The eFOCUS system provides firms with the capability to electronically submit their Financial and Operational Combined Uniform Single (FOCUS) Reports to FINRA. FINRA member broker-dealers are required to prepare and submit FOCUS reports pursuant to Exchange Rule 17a-5 (17 CFR 240.17a-5) ("Rule 17a-5") and FINRA's FOCUS Report filing plan. *See, e.g.*, *Self-Regulatory Organizations; Notice of Filing and Order Granting Accelerated Approval of Proposed Rule Change by the National Association of Securities Dealers, Inc. Relating to the Association's FOCUS Filing Plan*, Exchange Act Release No. 36780, (Jan. 26, 1996) [61 FR 3743 (Feb. 1, 1996)].

Further, a significant cybersecurity incident at FINRA could provide a gateway for threat actors to attack members that connect to it through information systems and networks of interconnected information systems. Moreover, the information systems that link FINRA to its members are vectors that expose FINRA to cybersecurity risk.

Additionally, the records stored by FINRA on its information systems include proprietary information about its members, including confidential business information (*e.g.*, information about the operational and financial condition of its broker-dealer members) and confidential personal information about registered persons affiliated with member firms. FINRA also is required to keep all records made or received by it in the course of its business and in the conduct of its self-regulatory activity. A significant cybersecurity incident at FINRA could lead to the improper use of this information to harm the members (*e.g.*, public exposure of confidential financial information) or their registered persons (*e.g.*, public exposure of personal information). Further, it could provide the unauthorized user with an unfair advantage over other market participants (*e.g.*, trading based on confidential financial information about its members).

f. National Securities Exchanges

Under the Exchange Act, an "exchange" is any organization, association, or group of persons, whether incorporated or unincorporated, that constitutes, maintains, or provides a market place or facilities for bringing together purchasers and sellers of securities or for otherwise performing with respect to securities the functions commonly performed by a stock exchange (as that term is generally understood), and includes the market place and the market

facilities maintained by that exchange.[88] Section 5 of the Exchange Act[89] requires an organization, association, or group of persons that meets the definition of "exchange" under section 3(a)(1) of the Exchange Act, unless otherwise exempt, to register with the Commission as a national securities exchange pursuant to section 6 of the Exchange Act. Registered national securities exchanges also are SROs, and must comply with regulatory requirements applicable to both national securities exchanges and SROs.[90] Section 6 of the Exchange Act requires, among other things, that the rules of a national securities exchange be designed to prevent fraudulent and manipulative acts and practices; to promote just and equitable principles of trade; to foster cooperation and coordination with persons engaged in facilitating transactions in securities; to remove impediments to, and perfect the mechanism of, a free and open market and a national market system; and, in general, to protect investors and the public interest; and that the rules of a national securities exchange not be designed to permit unfair discrimination between customers, issuers, brokers, or dealers.[91] As SROs under section 19 of the Exchange Act, the proposed rules of national securities exchanges are subject to Commission review and are published for notice

---

88 *See* 15 U.S.C. 78c(a)(1). Exchange Act Rule 3b-16 ("Rule 3b-16") defines terms used in the statutory definition of "exchange" under section 3(a)(1) of the Exchange Act. Under paragraph (a) of Rule 3b-16, an organization, association, or group of persons is considered to constitute, maintain, or provide such a marketplace or facilities if they "[b]ring[] together the orders for securities of multiple buyers and sellers" and use "established non-discretionary methods (whether by providing a trading facility or by setting rules) under which such orders interact with each other, and the buyers and sellers entering such orders agree to the terms of a trade." *See* 17 CFR 240.3b-16(a). In January 2022, the Commission: (1) proposed amendments to Rule 3b-16 to include systems that offer the use of non-firm trading interest and provide communication protocols to bring together buyers and sellers of securities; (2) re-proposed amendments to Regulation ATS for ATSs that trade government securities or repurchase and reverse repurchase agreements on government securities; (3) re-proposed amendments to Regulation SCI to apply to ATSs that meet certain volume thresholds in U.S. Treasury securities or in a debt security issued or guaranteed by a U.S. executive agency or government-sponsored enterprise; and (4) proposed amendments to, among other things, Form ATS-N, Form ATS-R, Form ATS, and the fair access rule under Regulation ATS. *See Amendments Regarding the Definition of ''Exchange'' and Alternative Trading Systems (ATSs) That Trade U.S. Treasury and Agency Securities, National Market System (NMS) Stocks, and Other Securities*, Exchange Act Release No. 94062 (Jan. 26, 2022) [87 FR 15496 (Mar. 18, 2022)] ("Amendments Regarding the Definition of 'Exchange' and ATSs Release"). The Commission encourages commenters to review that proposal with respect to ATSs and the comments on that proposal to determine whether they might affect comments on this proposing release.

89 15 U.S.C. 78e.

90 *See, e.g.*, 15 U.S.C. 78f and 78s.

91 *See* 15 U.S.C. 78f(b)(5).

and comment.[92] While certain types of proposed exchange rules are effective upon filing, others are subject to Commission approval before they can go into effect.

National securities exchanges use information systems to operate their marketplaces and facilities for bringing together purchasers and sellers of securities. In particular, national securities exchanges rely on automated, complex, and interconnected information systems for trading, routing, market data, regulatory, and surveillance purposes. They also use information systems to connect to members, other national securities exchanges, plan processors, and clearing agencies to facilitate order routing, trading, trade reporting, and the clearing of securities transactions. They also provide quotation, trade reporting, and regulatory information to the securities information processors to ensure that current market data information is available to market participants.[93] A significant cyber security incident at a national securities exchange could disrupt or disable its ability to provide these market functions, causing broader disruptions

---

92 *See* 15 U.S.C. 78s.

93 The national securities exchanges will provide quotation, trade reporting, and regulatory information to competing consolidators and self-aggregators after the market data infrastructure rules have been implemented. *See Market Data Infrastructure*, Exchange Act Release No. 90610 (Dec. 9, 2020) [86 FR 18596 (Apr. 9, 2021)] ("MDI Adopting Release"). In July 2012, the Commission adopted Rule 613 of Regulation NMS, which required national securities exchanges and national securities associations (the "Participants") to jointly develop and submit to the Commission a national market system plan to create, implement, and maintain a consolidated audit trail (the "CAT"). *See Consolidated Audit Trail*, Exchange Act Release No. 67457 (July 18, 2012) [77 FR 45722 (Aug. 1, 2012)]; 17 CFR 242.613. In November 2016, the Commission approved the national market system plan required by Rule 613 (the "CAT NMS Plan"). *See Joint Industry Plan; Order Approving the National Market System Plan Governing the Consolidated Audit Trail*, Exchange Act Release No. 78318 (Nov. 15, 2016) [81 FR 84696 (Nov. 23, 2016)] (the "CAT NMS Plan Approval Order"). The Participants conduct the activities related to the CAT in a Delaware limited liability company, Consolidated Audit Trail, LLC (the "Company"). The Participants jointly own on an equal basis the Company. As such, the CAT's Central Repository is a facility of each of the Participants. *See* CAT NMS Plan Approval Order, 81 FR at 84758. It would also qualify as an "information system" of each national securities exchange and each national securities association under proposed Rule 10. FINRA CAT, LLC—a wholly-owned subsidiary of FINRA—has entered into an agreement with the Company to act as the plan processor for the CAT. However, because the CAT System is operated by FINRA CAT, LLC on behalf of the national securities exchanges and FINRA, the Participants remain ultimately responsible for the performance of the CAT and its compliance with any statutes, rules, and regulations. The goal of the CAT NMS Plan is to create a modernized audit trail system that provides regulators with more timely access to a more comprehensive set of trading data, thus enabling regulators to more efficiently and effectively analyze and reconstruct broad-based market events, conduct market analysis in support of regulatory decisions, and to conduct market surveillance, investigations, and other enforcement activities. The CAT accepts data that are submitted by the Participants and broker-dealers, as well as data from certain market data feeds like SIP and OPRA.

to the securities markets.[94] For example, a significant cyber security incident could severely impede the ability to trade securities, or could disrupt the public dissemination of consolidated market data, impacting investors and the maintenance of fair, orderly, and efficient markets. In addition, the information systems that link national securities exchanges to their members are vectors that expose the exchange to cybersecurity risk.

Similarly, proprietary market data systems of exchanges are widely used and relied upon by a wide swath of market participants for detailed information about quoting and trading activity on an exchange. A significant cybersecurity incident that disrupts the availability or integrity of these feeds could have a significant impact on the trading of securities because market participants may withdraw from trading without access to current quotation and trade information. This could interfere with the maintenance of fair, orderly, and efficient markets.

National securities exchanges also use information systems to perform their responsibilities as SROs. In particular, exchanges employ market-regulation systems to assist with obligations such as enforcing their rules and the federal securities laws with respect to their members. A disruption of a national securities exchange's business operations caused by a significant cybersecurity incident could disrupt its ability to carry out its regulatory responsibilities as an SRO and, therefore, materially impact the fair, orderly, and efficient functioning of the U.S. securities markets.

Each exchange also is required to keep all records made or received by it in the course of its business and in the conduct of its self-regulatory activity. The records stored by national securities exchanges on their information systems include proprietary information about their members, including confidential business information (*e.g.*, information about the financial condition of their members). The records also include information relating to trading, routing,

---

[94] *See, e.g.*, New Zealand FMA Report (describing an August 2020 cybersecurity incident at New Zealand's only regulated financial product market that caused a trading halt of approximately four days).

market data, and market surveillance, among other areas.[95] A significant cybersecurity incident at a national securities exchange could lead to the improper use of this information to harm exchange members (*e.g.*, public exposure of confidential financial information) or provide the unauthorized user with an unfair advantage over other market participants (*e.g.*, trading based on confidential business information).

g. Security-Based Swap Data Repositories

Title VII of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Title VII of the Dodd-Frank Act"), enacted in 2010, provided for a comprehensive, new regulatory framework for swaps and security-based swaps, including regulatory reporting and public dissemination of transactions in security-based swaps.[96] In 2015, the Commission established a regulatory framework for SBSDRs to provide improved transparency to regulators and help facilitate price discovery and efficiency in the SBS market.[97] Under this framework, SBSDRs are registered securities information processors and disseminators of market data in the security-based swap market,[98] thereby supporting the Dodd-Frank Act's goal of public dissemination for all security-based swaps to enhance price discovery to market participants.[99] The collection and dissemination of security-based swap data by SBSDRs provide transparency in the security-based swap market for regulators and market participants.

---

95 For example, as discussed above, the national securities exchanges and FINRA jointly operate the CAT System, which collects and stores information relating market participants, and their order and trading activities.

96 Public Law 111-203, 124 Stat. 1376 (2010), section 761(a) (adding Exchange Act section 3(a)(75) (defining SBSDR)) and section 763(i) (adding Exchange Act section 13(n) (establishing a regulatory regime for SBSDRs)).

97 *See Security-Based Swap Data Repository Registration, Duties, and Core Principles*, Exchange Act Release No. 74246 (Feb. 11, 2015) [80 FR 14438 (Mar. 19, 2015)] ("SBSDR Adopting Release"); *Regulation SBSR—Reporting and Dissemination of Security-Based Swap Information*, Exchange Act Release No. 74244 (Feb. 11, 2015) [80 FR 14563 (Mar. 19, 2015)] ("SBSR Adopting Release").

98 *See* 17 CFR 242.909 ("A registered security-based swap data repository shall also register with the Commission as a securities information processor on Form SDR"); *see also* Form SDR ("With respect to an applicant for registration as a security-based swap data repository, Form SDR also constitutes an application for registration as a securities information processor.").

99 *See, e.g.*, SBSDR Adopting Release, 80 FR at 14604.

In addition, as centralized repositories for security-based swap transaction data that is used by regulators, SBSDRs provide an important infrastructure assisting relevant authorities in performing their market oversight.[100] Data maintained by SBSDRs can assist regulators in addressing market abuses, performing supervision, and resolving issues and positions if an institution fails.[101] SBSDRs are required to collect and maintain accurate security-based swap transaction data so that relevant authorities can access and analyze the data from secure, central locations, thereby putting the regulators in a better position to monitor for potential market abuse and risks to financial stability.[102] SBSDRs also have the potential to reduce operational risk and enhance operational efficiency, such as by maintaining transaction records that would help counterparties to ensure that their records reconcile on all of the key economic details.

SBSDRs use information systems to perform these functions, including to disseminate market data and provide price transparency in the security-based swap market. They also use information systems to operate centralized repositories for security-based swap data for use by regulators. These information systems provide an important market infrastructure that assists relevant authorities in performing their market oversight.[103] As discussed above, data maintained

---

100 *See Security-Based Swap Data Repository Registration, Duties, and Core Principles*, Exchange Act Release No. 63347 (Nov. 19, 2010) [75 FR 77306, 77307 (Dec. 10, 2010)], corrected at 75 FR 79320 (Dec. 20, 2010) and 76 FR 2287 (Jan. 13, 2011) ("SBSDR Proposing Release") ("The data maintained by an [SBSDR] may also assist regulators in (i) preventing market manipulation, fraud, and other market abuses; (ii) performing market surveillance, prudential supervision, and macroprudential (systemic risk) supervision; and (iii) resolving issues and positions after an institution fails.").

101 *See* SBSDR Proposing Release at 77307.

102 *See* SBSDR Adopting Release, 80 FR at 14440 (stating that "[SBSDRs] are required to collect and maintain accurate [security-based swap] transaction data so that relevant authorities can access and analyze the data from secure, central locations, thereby putting them in a better position to monitor for potential market abuse and risks to financial stability.").

103 *See* Committee on Payments and Settlement Systems ("CPSS"), Technical Committee of IOSCO, *Principles for financial markets intermediaries* (Apr. 2012), *available a*t https://www.bis.org/cpmi/publ/d101a.pdf ("FMI Principles") (Principle for financial markets intermediaries ("PFMI") 1.14 stating that "[b]y centralising the collection, storage, and dissemination of data, a well-designed [trade repository ("TR")] that operates with effective risk controls can serve an important role in enhancing the transparency of transaction information to relevant authorities and the public, promoting financial stability, and supporting the detection and prevention of market abuse."). In 2014, the CPSS became the Committee on Payments and Market Infrastructures ("CPMI").

by SBSDRs may, for example, assist regulators in addressing market abuses, performing supervision, and resolving issues and positions if an institution fails.

SBSDRs are subject to certain cybersecurity risks that if realized could impede their ability to meet the goals set out in Title VII of the Dodd-Frank Act and the Commission's rules.[104] For example, SBSDRs process and disseminate trade data using information systems. If these information systems suffer from a significant cybersecurity incident, public access to timely and reliable trade data for the derivatives markets could potentially be compromised.[105] Also, if the data stored at an SBSDR is corrupted by a threat actor through a cybersecurity attack, the SBSDR would not be able to provide accurate data to relevant regulatory authorities, which could hinder the oversight of the derivatives markets. Moreover, SBSDRs use information systems to receive and maintain personal, confidential, and proprietary information and data. The unauthorized use or access of this information could be used to create unfair business or trading advantages and, in the case of personal information, to steal identities.

Further, a significant cybersecurity incident at an SBSDR could provide a gateway for threat actors to attack Market Entities and others that connect to it through information systems. Moreover, the links established between an SBSDR and other entities, including unaffiliated clearing agencies and other SBSDRs, are vectors that expose the SBSDR to cybersecurity risk arising from threats that originate in information systems outside the SBSDR's control.[106]

---

104 *See* SBSDR Adopting Release, 80 FR at 14450 ("[SBSDRs] themselves are subject to certain operational risks that may impede the ability of [SBSDRs] to meet these goals, and the Title VII regulatory framework is intended to address these risks.").

105 *See* FMI Principles (PFMI 1.14, Box 1 stating that "[t]he primary public policy benefits of a TR, which stem from the centralisation and quality of the data that a TR maintains, are improved market transparency and the provision of this data to relevant authorities and the public in line with their respective information needs. Timely and reliable access to data stored in a TR has the potential to improve significantly the ability of relevant authorities and the public to identify and evaluate the potential risks posed to the broader financial system.").

106 *See* FMI Principles (PFMI at 3.20.20 stating that "[a] TR should carefully assess the additional operational risks related to its links to ensure the scalability and reliability of IT and related resources. A TR can establish links with another TR or with another type of FMI. Such links may expose the linked [financial market infrastructures ("FMIs")] to additional risks if not properly designed. Besides legal risks, a link to

h. SBS Entities

The SBS Entities covered by the proposed rulemaking are SBSDs and MSBSPs. An SBSD generally refers to any person who: (1) holds itself out as a dealer in security-based swaps; (2) makes a market in security-based swaps; (3) regularly enters into security-based swaps with counterparties as an ordinary course of business for its own account; or (4) engages in any activity causing it to be commonly known in the trade as a dealer or market maker in security-based swaps.[107] An SBSD does not, however, include a person that enters into security-based swaps for such person's own account, either individually or in a fiduciary capacity, but not as a part of regular business.[108]

An MSBSP generally includes any person that is not a security-based swap dealer and that satisfies one of the following three alternative statutory tests: (1) it maintains a "substantial position" in security-based swaps, excluding positions held for hedging or mitigating commercial risk and positions maintained by any employee benefit plan (or any contract held by such a plan) for the primary purpose of hedging or mitigating any risk directly associated with the operation of the plan, for any of the major security-based swap categories determined by the Commission; (2) its outstanding security-based swaps create substantial counterparty exposure that could have serious adverse effects on the financial stability of the U.S. banking system or financial markets; or (3) it is a "financial entity" that is "highly leveraged" relative to the amount of capital it holds

---

either another TR or to another type of FMI may involve the potential spillover of operational risk. The mitigation of operational risk is particularly important because the information maintained by a TR can support bilateral netting and be used to provide services directly to market participants, service providers (for example, portfolio compression service providers), and other linked FMIs."). The CPMI and IOSCO issued guidance for cyber resilience for FMIs, including CSDs, securities settlement systems ("SSSs"), CCPs, and trade repositories. *See* CPMI-IOSCO, *Guidance on cyber resilience for financial market infrastructures* (June 2016), *available at* https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf; *see also* CPMI-IOSCO*, Implementation monitoring of the PFMI: Level 3 assessment on Financial Market Infrastructures' Cyber Resilience* (Nov. 2022), *available at* https://www.iosco.org/library/pubdocs/pdf/IOSCOPD723.pdf (presenting the results of an assessment of the state of cyber resilience (as of February 2021) of FMIs from 29 jurisdictions that participated in the exercise in 2020 to 2022).

107 *See* 15 U.S.C. 78c(a)(71); 17 CFR 240.3a71-1 *et seq*.

108 *See* 15 U.S.C. 78c(a)(71)(C); 17 CFR 240.3a71-1(b).

(and that is not subject to capital requirements by an appropriate federal banking agency) and maintains a "substantial position" in outstanding security-based swaps in any major category as determined by the Commission.[109] Currently, there are no MSBSPs registered with the Commission.

SBS Entities play (or, in the case of MSBSPs, could play) a critical role in the U.S. security-based swap market.[110] SBS Entities rely on information systems to transact in security-based swaps with other market participants, to receive and deliver collateral, to create and maintain books and records, and to obtain market information to update books and records, and manage risk.

A disruption to an SBS Entity's operations caused by a significant cybersecurity incident could have a large negative impact on the U.S. security-based swap market given the concentration of dealers in this market. Further, a disruption in the security-based swap market could negatively impact the broader securities markets by, for example, causing participants to liquidate positions related to, or referenced by, the impacted security-based swaps to mitigate losses to participants' positions or portfolios or due to loss of trading confidence. A disruption in the security-based swap market also could negatively impact the broader securities markets by causing participants to liquidate the collateral margining the security-based swaps for similar reasons or to cover margin calls. The consequences of a business disruption to an SBS Entity's functions—such as those that may be caused by a significant cybersecurity incident—may be amplified because, unlike many other securities transactions, securities-based swap transactions give rise to an ongoing obligation between transaction counterparties during the life of the

---

109 *See* 15 U.S.C. 78c(a)(67); 17 CFR 240.3a67-1 *et seq*.

110 Currently, this role is fulfilled by SBSDs, given there are no MSBSPs registered with the Commission.

transaction.[111] This means that each counterparty bears the risk of its counterparty's ability to perform under the terms of a security-based swap until the transaction is terminated. A disruption of an SBS Entity's normal business activities because of a significant cybersecurity incident could produce spillover or contagion by negatively affecting the willingness or the ability of market participants to extend credit to each other, and could substantially reduce liquidity and valuations for particular types of financial instruments.[112] The security-based swap market is large[113] and thus a disruption of an SBS Entity's operations due to a significant cybersecurity incident could negatively impact sectors of the U.S. economy.[114]

Further, a significant cybersecurity incident at an SBS Entity could provide a gateway for threat actors to attack the exchanges, SBSDRs, clearing agencies, counterparties, and other SBS Entities to which the firm is connected through information systems and networks of interconnected information systems. Moreover, the information systems that link SBS Entities to other Market Entities are vectors that expose the SBS Entity to cybersecurity risk arising from threats that originate in information systems outside the SBS Entity's control. SBS Entities also store proprietary and confidential information about their counterparties on their information systems, including financial information they use to perform credit analysis. A significant

---

111 *See Further Definition of "Swap Dealer," "Security-Based Swap Dealer," "Major Swap Participant," "Major Security-Based Swap Participant" and "Eligible Contract Participant"*, Exchange Act Release No. 66868 (Apr. 27, 2012) [77 FR 30596, 30616-17 (May 23, 2012)] ("Further Definition Release") (noting that "[i]n contrast to a secondary market transaction involving equity or debt securities, in which the completion of a purchase or sale transaction can be expected to terminate the mutual obligations of the parties to the transaction, the parties to a security-based swap often will have an ongoing obligation to exchange cash flows over the life of the agreement").

112 *See Cross-Border Security-Based Swap Activities; Re-Proposal of Regulation SBSR and Certain Rules and Forms Relating to the Registration of Security-Based Swap Dealers and Major Security-Based Swap Participants*, Exchange Act Release No. 69490 (May 1, 2013) [78 FR 30967, 30980-81 (May 23, 2013)] ("Cross-Border Proposing Release").

113 *See, e.g.,* Commission, *Report on Security-Based Swaps Pursuant to Section 13(m)(2) of the Securities Exchange Act of 1934* (July 15, 2022) *available at* https://www.sec.gov/files/report-on-security-based-swaps-071522.pdf.

114 *See* Cross-Border Proposing Release, 78 FR at 30972 ("The Dodd-Frank Act was enacted, among other reasons, to promote the financial stability of the United States by improving accountability and transparency in the financial system. The 2008 financial crisis highlighted significant issues in the over-the-counter ('OTC') derivatives markets, which . . . are capable of affecting significant sectors of the U.S. economy.") (footnotes omitted).

cybersecurity incident at an SBS Entity could lead to the improper use of this information to harm the counterparties (*e.g.*, public exposure of confidential financial information) or provide the unauthorized user with an unfair advantage over other market participants (*e.g.*, trading based on confidential business information).

i. Transfer Agents

A transfer agent is any person who engages on behalf of an issuer of securities or on behalf of itself as an issuer of securities in (among other functions): (1) tracking, recording, and maintaining the official record of ownership of each issuer's securities; (2) canceling old certificates, issuing new ones, and performing other processing and recordkeeping functions that facilitate the issuance, cancellation, and transfer of those securities; (3) facilitating communications between issuers and registered securityholders; and (4) making dividend, principal, interest, and other distributions to securityholders.[115] To perform these functions, transfer agents maintain records and information related to securityholders that may include names, addresses, phone numbers, email addresses, employers, employment history, bank and specific account information, credit card information, transaction histories, securities holdings, and other detailed and individualized information related to the transfer agents' recordkeeping and transaction processing on behalf of issuers. With advances in technology and the expansion of book-entry ownership of securities, transfer agents today increasingly rely on technology and automation to perform the core recordkeeping, processing, and transfer services described above, including the use of computer systems to store, access, and process the information related to securityholders they maintain on behalf of issuers. A significant cybersecurity incident that impacts these systems could cause harm to investors by, for example, preventing the transfer agent from transferring ownership of securities or preventing investors from receiving dividend, interest, or principal payments.

---

[115] *See Transfer Agent Regulations*, Exchange Act Release No. 76743 (Dec. 22, 2015) [80 FR 81948, 81949 (Dec. 31, 2015)].

Further, a significant cybersecurity incident at a transfer agent could provide a gateway for threat actors to attack other Market Entities that connect to it through information systems and networks of interconnected information systems. Moreover, the information systems that link transfer agents to other Market Entities expose the transfer agent to cybersecurity risk arising from threats that originate in information systems outside the transfer agent's control. The records stored by transfer agents on their information systems include proprietary information about securities ownership and corporate actions. A significant cybersecurity incident at a transfer agent could lead to the improper use of this information to harm securities holders (*e.g.*, public exposure of their confidential financial information or the use of that information to steal their identities) or provide the unauthorized user with an unfair advantage over other market participants (*e.g.*, trading based on confidential business information).

B. Overview of the Proposed Cybersecurity Requirements

As discussed above, the U.S. securities markets are part of the critical infrastructure of the United States.[116] In this regard, they play a central role in the U.S. economy in terms of facilitating the flow of capital, including the savings of individual investors. The fair, orderly, and efficient operation of the U.S. securities markets depends on Market Entities being able to perform their critical functions, and Market Entities are increasingly relying on information systems and interconnected networks of information systems to perform these functions. These information systems are targets of threat actors. Moreover, Market Entities—as financial institutions—are choice targets for threat actors seeking financial gain or to inflict economic harm. Further, threat actors are using increasingly sophisticated and constantly evolving tactics, techniques, and procedures to attack information systems. In addition to threat actors, cybersecurity risk also can be caused by the errors of employees, service providers, or business

---

[116] *See* section I.A. of this release (discussing cybersecurity risk and how critical operations of Market Entities are exposed to cybersecurity risk).

partners. The interconnectedness of Market Entities increases the risk that a significant cybersecurity incident can simultaneously impact multiple Market Entities causing harm to the U.S. securities markets.

For these reasons, it is critically important that Market Entities take steps to protect their information systems and the information residing on those systems from cybersecurity risk. A Market Entity that fails to do so is more vulnerable to succumbing to a significant cybersecurity incident. As discussed above, a significant cybersecurity incident can cause serious harm not only to the Market Entity but also to its customers, counterparties, members, registrants, or users, or to any other market participants (including other Market Entities) that interact with the Market Entity. Therefore, it is vital to the U.S. securities markets and the participants in those markets that *all* Market Entities address cybersecurity risk, which, as discussed above, is increasingly threatening the financial sector.

Consequently, the Commission is proposing new Rule 10 and new Form SCIR to require that Market Entities address cybersecurity risks, to improve the Commission's ability to obtain information about significant cybersecurity incidents impacting Market Entities, and to improve transparency about the cybersecurity risks that can cause adverse impacts to the U.S. securities markets.[117] Under proposed Rule 10, certain broker-dealers, the MSRB, and all clearing agencies, national securities associations, national securities exchanges, SBSDRs, SBS Entities, and transfer agents would be defined as a "covered entity" (collectively, "Covered Entities").[118]

---

[117] In designing the requirements of proposed Rule 10, the Commission considered several cybersecurity sources (which are cited in the relevant sections below), including the NIST Framework, the NIST Glossary, and CISA's *Cyber Essentials Starter Kit* (information about CISA's Cyber Essentials Starter Kit is available at: https://www.cisa.gov/publication/cisa-cyber-essentials). The Commission also considered definitions in relevant federal statutes including the Federal Information Security Modernization Act of 2014, Pub. L. 113–283 (Dec. 18, 2014); 44 U.S.C. 3551 *et seq.* ("FISMA") and the Cyber Incident Reporting for Critical Infrastructure Act of 2022, H.R. 2471, 117th Cong. (2021-2022); 6 U.S.C. 681 *et seq*. ("CIRCIA").

[118] The following broker-dealers would be Covered Entities: (1) broker-dealers that maintain custody of securities and cash for customers or other broker-dealers ("carrying broker-dealers"); (2) broker-dealers that introduce their customer accounts to a carrying broker-dealer on a fully disclosed basis ("introducing

Proposed Rule 10 would require all Market Entities (Covered Entities and Non-Covered Entities) to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks.[119] All Market Entities also, at least annually, would be required to review and assess the design and effectiveness of their cybersecurity policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review.[120] They also would be required to prepare a report (in the case of Covered Entities) and a record (in the case of Non-Covered Entities) with respect to the annual review. CISA states that organizations should "approach cyber as business risk."[121] Like other business risks (*e.g.*, market, credit, or liquidity risk), cybersecurity risk can be addressed through policies and procedures that are reasonably designed to manage the risk. Finally, all Market Entities would need to give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring.[122]

---

broker-dealers"); (3) broker-dealers with regulatory capital equal to or exceeding $50 million; (4) broker-dealers with total assets equal to or exceeding $1 billion; (5) broker-dealers that operate as market makers; and (6) broker-dealers that operate an ATS (sometimes collectively referred to as "Covered Broker-Dealers"). Broker-dealers that do not fall into one of these six categories (sometimes collectively referred to as "Non-Covered Entities" or "Non-Covered Broker-Dealers") would not be Covered Entities for the purposes of proposed Rule 10. *See also* section II.A.1.b. of this release (discussing the categories of broker-dealers that would be "Covered Entities" in greater detail).

119 *See* paragraphs (b) through (d) of proposed Rule 10 (setting forth the requirements for Market Entities that meet the definition of "covered entity"); paragraph (e)(1) of proposed Rule 10 (setting forth the requirements for Market Entities that are not Covered Entities (*i.e.*, Non-Covered Broker-Dealers)). *See also* sections II.B.1. and II.C. of this release (discussing these proposed requirements in more detail). As discussed in sections II.F. and IV.C.1.b. of this release, certain categories of Market Entities are subject to existing requirements to address aspects of cybersecurity risk or that may relate to cybersecurity. These other requirements, however, do not address cybersecurity risk as directly, broadly, or comprehensively as the requirements of proposed Rule 10.

120 *See* paragraph (b)(2) of proposed Rule 10; paragraph (e)(1) of proposed Rule 10. *See also* sections II.B.1.f. and II.C. of this release (discussing these proposed requirements in more detail).

121 *See* CISA Cyber Essentials Starter Kit ("Ask yourself what type of impact would be catastrophic to your operations? What information if compromised or breached would cause damage to employees, customers, or business partners? What is your level of risk appetite and risk tolerance? Raising the level of awareness helps reinforce the culture of making informed decisions and understanding the level of risk to the organization.").

122 *See* paragraph (c)(1) of proposed Rule 10; paragraph (e)(2) of proposed Rule 10. *See also* sections II.B.2.a. and II.C. of this release (discussing these proposed requirements in more detail).

Market Entities that meet the definition of "covered entity" would be subject to certain additional requirements under proposed Rule 10.[123] First, as discussed in more detail below, the written policies and procedures that Covered Entities would need to establish, maintain, and enforce would need to include the following elements:

- Periodic assessments of cybersecurity risks associated with the Covered Entity's information systems and written documentation of the risk assessments;
- Controls designed to minimize user-related risks and prevent unauthorized access to the Covered Entity's information systems;
- Measures designed to monitor the Covered Entity's information systems and protect the Covered Entity's information from unauthorized access or use, and oversee service providers that receive, maintain, or process information, or are otherwise permitted to access the Covered Entity's information systems;
- Measures to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the Covered Entity's information systems; and
- Measures to detect, respond to, and recover from a cybersecurity incident and written documentation of any cybersecurity incident and the response to and recovery from the incident.[124]

Second, Covered Entities—in addition to providing the Commission with immediate written electronic notice of a significant cybersecurity incident—would need to report and update information about the significant cybersecurity incident by filing Part I of proposed Form SCIR with the Commission.[125] The form would elicit information about the significant cybersecurity incident and the Covered Entity's efforts to respond to, and recover from, the incident.

Third, Covered Entities would need to disclose publicly summary descriptions of their cybersecurity risks and the significant cybersecurity incidents they experienced during the

---

123 *Compare* paragraphs (b) through (d) of proposed Rule 10 (setting forth the requirements for Covered Entities), *with* paragraph (e) of proposed Rule 10 (setting forth the requirements for Non-Covered Entities).

124 *See* sections II.B.1.a. through II.B.1.e. of this release (discussing these proposed requirements in more detail). In the case of Non-Covered Entities, as discussed in more detail below in section II.C. of this release, the design of the cybersecurity risk management policies and procedures would need to take into account the size, business, and operations of the broker-dealer. *See* paragraph (e) of proposed Rule 10.

125 *See* sections II.B.2. and II.B.4. of this release (discussing these proposed requirements in more detail).

current or previous calendar year on Part II of proposed Form SCIR.[126] The form would need to be filed with the Commission and posted on the Covered Entity's business Internet website. Covered Entities that are carrying or introducing broker-dealers also would need to provide the form to customers at account opening, when information on the form is updated, and annually.

Covered Entities and Non-Covered Entities would need to preserve certain records relating to the requirements of proposed Rule 10 in accordance with amended or existing recordkeeping requirements applicable to them or, in the case of exempt clearing agencies, pursuant to conditions in relevant exemption orders.[127]

Finally, the Commission is proposing amendments to address the potential availability of substituted compliance to non-U.S. SBS Entities with respect to the proposed cybersecurity requirements.[128]

In developing the proposed requirements summarized above with regard to SBSDRs and SBS Entities, the Commission consulted and coordinated with the CFTC and the prudential regulators in accordance with section 712(a)(2) of Title VII of the Dodd-Frank Act. In accordance with section 752 of Title VII of the Dodd-Frank Act, the Commission has consulted and coordinated with foreign regulatory authorities through Commission staff participation in numerous bilateral and multilateral discussions with foreign regulatory authorities addressing the regulation of OTC derivatives markets.

---

126 *See* sections II.B.3. and II.B.4.of this release (discussing these proposed requirements in more detail).

127 *See* sections II.B.5. and II.C. of this release (discussing these proposed requirements in more detail).

128 *See* sections II.D. of this release (discussing these proposed amendments in more detail).

II. DISCUSSION OF PROPOSED CYBERSECURITY RULE

A. Definitions

Proposed Rule 10 would define a number of terms for the purposes of its requirements.[129] These definitions also would be used for the purposes of Parts I and II of proposed Form SCIR.[130] The defined terms are intended to tailor the risk management, notification, reporting, and disclosure requirements of proposed Rule 10 to the distinctive aspects of cybersecurity risk as compared with other risks Market Entities face (*e.g.*, market, credit, or liquidity risk).[131]

1. "Covered Entity"

a. Market Entities that Meet the Definition of "Covered Entity" Would be Subject to Additional Requirements

Proposed Rule 10 would define the term "covered entity" to identify the types of Market Entities that would be subject to certain additional requirements under the rule.[132] As discussed above, proposed Rule 10 would require all Market Entities to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks.[133] All Market Entities also, at least annually, would be required to review and assess the design and effectiveness of their cybersecurity risk management policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time

---

129 *See* paragraph (a) of proposed Rule 10.

130 *See* sections II.B.2. and II.B.3. of this release (discussing Parts I and II of proposed Form SCIR in more detail).

131 *See* paragraphs (a)(2) through (9) of proposed Rule 10 (defining, respectively, the terms "cybersecurity incident," "cybersecurity risk," "cybersecurity threat," "cybersecurity vulnerability," "information," "information systems," "personal information," and "significant cybersecurity incident").

132 *See* paragraphs (a)(1)(i) through (ix) of proposed Rule 10 (defining these Market Entities as "covered entities"). A Market Entity that falls within the definition of "covered entity" for purposes of proposed Rule 10 may not necessarily meet the definition of a "covered entity" for purposes of certain federal statutes, such as, but not limited to, CIRCIA and any regulations promulgated thereunder. CIRCIA, among other things, requires the Director of CISA to issue and implement regulations defining the term "covered entity" and requiring covered entities to report covered cyber incidents and ransom payments as the result of ransomware attacks to CISA in certain instances.

133 *See* paragraph (b)(1) of proposed Rule 10 (setting forth the requirement for Market Entities that meet the definition of "covered entity"); paragraph (e)(1) of proposed Rule 10 (setting forth the requirement for Market Entities that do not meet the definition of "covered entity," which, as discussed above, would be certain smaller broker-dealers).

period covered by the review.[134] They also would be required to prepare a report (in the case of Covered Entities) or a record (in the case of Non-Covered Entities) with respect to the annual review. Further, all Market Entities would need to give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring.[135] As discussed above, Market Entities use information systems that expose them to cybersecurity risk and that risk is increasing due to the interconnectedness of the information systems and the sophistication of the tactics used by threat actors. Therefore, regardless of their function, interconnectedness, or size, all Market Entities would be subject to these requirements designed to address cybersecurity risks.

Market Entities that are Covered Entities would be subject to certain additional requirements under proposed Rule 10.[136] In particular, they would be required to: (1) include certain elements in their cybersecurity risk management policies and procedures;[137] (2) file Part I of proposed Form SCIR with the Commission and, for some Covered Entities, other regulators to report information about a significant cybersecurity incident;[138] and (3) make public disclosures on Part II of proposed Form SCIR about their cybersecurity risks and the significant cybersecurity incidents they experienced during the current or previous calendar year.[139]

---

134 *See* paragraph (b)(2) of proposed Rule 10; paragraph (e)(1) of proposed Rule 10.

135 *See* paragraph (c)(1) of proposed Rule 10 (setting forth the requirement for Market Entities that meet the definition of "covered entity"); paragraph (e)(2) of proposed Rule 10 (setting forth the requirement for Market Entities that do not meet the definition of "covered entity").

136 *See* paragraphs (b) through (d) of proposed Rule 10 (setting forth the requirements for Covered Entities); paragraph (e) of proposed Rule 10 (setting forth the requirements for Non-Covered Entities). As discussed above, Covered Entities would need to prepare a report with respect to their review and assessment of the policies and procedures. *See* paragraph (b)(2) of proposed Rule 10. Non-Covered Entities would need to make a record with the respect to the annual review and assessment of their policies and procedures. *See* paragraph (e) of proposed Rule 10.

137 *See* paragraphs (b)(1)(i) through (v) of proposed Rule 10.

138 *See* paragraph (c)(2) of proposed Rule 10. *See also* paragraph (a)(10) of proposed Rule 10 (defining the term "significant cybersecurity risk").

139 *See* paragraph (d) of proposed Rule 10.

In determining which Market Entities would be Covered Entities subject to the additional requirements, the Commission considered: (1) how the type of Market Entity supports the fair, orderly, and efficient operation of the U.S. securities markets and the consequences if that type of Market Entity's critical functions were disrupted or degraded by a significant cybersecurity incident; (2) the harm that could befall investors, including retail investors, if that type of Market Entity's functions were disrupted or degraded by a significant cybersecurity incident; (3) the extent to which that type of Market Entity poses cybersecurity risk to other Market Entities through information system connections, including the number of connections; (4) the extent to which the that type of Market Entity would be an attractive target for threat actors; and (5) the personal, confidential, and proprietary business information about the type of Market Entity and other persons (*e.g.*, investors) stored on the Market Entity's information systems and the harm that could be caused if that information was accessed or used by threat actors.

b. Broker-Dealers

The following broker-dealers registered with the Commission would be Covered Entities: (1) broker-dealers that maintain custody of securities and cash for customers or other broker-dealers (*i.e.*, carrying broker-dealers); (2) broker-dealers that introduce their customers' accounts to a carrying broker-dealer on a fully disclosed basis (*i.e.*, introducing broker-dealers);[140] (3) broker-dealers with regulatory capital equal to or exceeding $50 million; (4) broker-dealers with total assets equal to or exceeding $1 billion; (5) broker-dealers that operate as market makers; and (6) broker-dealers that operate an ATS. Thus, under proposed Rule 10, these six categories

---

[140] When a broker-dealer introduces a customer to a carrying broker-dealer on a fully disclosed basis, the carrying broker-dealer knows the identity of the customer and holds cash and securities in an account for the customer that identifies the customer as the accountholder. This is distinguishable from a broker-dealer that introduces its customers to another carrying broker-dealer on an omnibus basis. In this scenario, the carrying broker-dealer does not know the identities of the customers and holds their cash and securities in an account that identifies the broker-dealer introducing the customers on an omnibus basis as the accountholder. A broker-dealer that introduces customers to another broker-dealer on an omnibus basis is, itself, a carrying broker-dealer for purposes of the Commission's financial responsibility rules, including, the broker-dealer net capital and customer protection rules. *See, e.g.*, 17 CFR 240.15c3-1 and 17 CFR 240.15c3-3. This category of broker-dealer would be a carrying broker-dealer for purposes of proposed Rule 10 and therefore subject to the rule's requirements for Covered Entities.

of broker-dealers would be subject to the additional requirements.[141] All other types of broker-dealers would not meet the definition of Covered Entity.[142]

The first category of broker-dealers included as Covered Entities would be carrying broker-dealers. Specifically, proposed Rule 10 would define "covered entity" to include any broker-dealer that maintains custody of cash and securities for customers or other broker-dealers and is not exempt from the requirements of Exchange Act Rule 15c3-3 (*i.e.*, a carrying broker-dealer).[143] Some carrying broker-dealers are large in terms of their assets and dealing activities or the number of their accountholders. For example, they may engage in a variety of order handling, trading, and/or clearing activities, and thereby play a significant role in U.S. securities markets, often through multiple business lines and/or in multiple asset classes. Consequently, if their critical functions were disrupted or degraded by a significant cybersecurity incident it could have a potential negative impact on the U.S. securities markets by, for example, reducing liquidity in the markets or sectors of the markets due to the firm's inability to continue dealing and trading activities. A broker-dealer in this situation could lose its ability to provide liquidity to other market participants for an indeterminate length of time, which could lead to unfavorable

---

141 *See* paragraphs (a)(1)(i)(A) through (F) of proposed Rule 10. Certain of the definitions in proposed Rule 10 would be used for the purposes of the requirements in the rule for broker-dealers that are not Covered Entities. Specifically, paragraph (e)(1) of proposed Rule 10 would require broker-dealers that are not Covered Entities to establish, maintain, and enforce written policies and procedures that are reasonably designed to address the *cybersecurity risks* of the broker-dealer taking into account the size, business, and operations of the broker-dealer. The term "cybersecurity risk" is defined in paragraph (a)(3) of proposed Rule 10 and that definition incorporates the terms "cybersecurity incident," "cybersecurity threat," and "cybersecurity vulnerability," which are defined, respectively, in paragraphs (a)(2), (a)(4), and (a)(5) of proposed Rule 10. In addition, paragraph (e)(2) of proposed Rule 10 would require broker-dealers that are not Covered Entities to provide immediate written electronic notice to the Commission and their examining authority if they experience a "significant cybersecurity incident" as that term is defined in the rule. Therefore, paragraph (a)(8) of proposed Rule 10 would define the term "market entity" to mean a Covered Entity *and* a broker-dealer registered with the Commission that is not a Covered Entity. Further, the definitions in proposed Rule 10 would refer to "market entities" (rather than "covered entities") in order to not limit the application of these definitions to paragraphs (b) through (d) of proposed Rule 10, which set forth the requirements for Covered Entities (but not for Non-Covered Entities).

142 As discussed below in section IV.C.2. of this release, of the 3,510 broker-dealers registered with the Commission as of the third quarter of 2022, 1,541 would meet the definition of "covered entity" under proposed Rule 10, leaving 1,969 broker-dealers as Non-Covered Entities.

143 *See* paragraph (a)(1)(i)(A) of proposed Rule 10. *See also* 17 CFR 240.15c3-3 ("Rule 15c3-3"). Rule 15c3-3 sets forth requirements for broker-dealers that maintain custody of customer securities and cash that are designed to protect those assets and ensure their prompt return to the customers.

market conditions for investors, such as higher buy prices and lower sell prices or even the inability to execute a trade within a reasonable amount of time. Further, some carrying broker-dealers hold millions of accounts for investors. If a significant cybersecurity incident prevented this investor-base from accessing the securities markets, it could impact liquidity as well.

Also, the dealing activities of carrying broker-dealers may make them attractive targets for threat actors seeking to access proprietary and confidential information about the broker-dealer's trading positions and strategies to use for financial advantage. In addition, the size and financial resources of carrying broker-dealers may make them attractive targets for threat actors employing ransomware schemes.

Because carrying broker-dealers hold cash and securities for customers and other broker-dealers, a significant cybersecurity incident could put these assets in peril or make them unavailable. For example, a significant cybersecurity incident could cause harm to the investors that own these assets—including retail investors—if it causes the investors to lose access to their securities accounts (and, therefore, the ability to purchase or sell securities), causes the failure of the carrying broker-dealer (which could tie up the assets in a liquidation proceeding under the Securities Investor Protection Act), or, in the worst case, results in the assets being stolen. The fact that carrying broker-dealers hold cash and securities for investors also may make them attractive targets for threat actors seeking to steal those assets through hacking the accounts or using stolen credentials and log-in information. In addition, carrying broker-dealers with large numbers of customers might be attractive targets for threat actors because of the volume of personal information they maintain. Threat actors may seek to access and download this information in order to sell it to other threat actors. If this information is accessed or stolen by threat actors, it could result in harm (*e.g.*, identity theft or conversion of financial assets) to many individuals, including retail investors. Carrying broker-dealers typically are connected to a number of different Market Entities through information systems, including national securities exchanges, clearing agencies, and other broker-dealers (including introducing broker-dealers).

The second category of broker-dealers included as Covered Entities would be introducing broker-dealers.[144] These broker-dealers introduce customer accounts on a fully disclosed basis to a carrying broker-dealer. In this arrangement, the carrying broker-dealer knows the identities of the fully disclosed customers and maintains custody of their securities and cash. The introducing broker-dealer typically interacts directly with the customers by, for example, making securities recommendations and accepting their orders to purchase or sell securities. An introducing broker-dealer must enter into an agreement with a carrying broker-dealer to which it introduces customer accounts on a fully disclosed basis.[145]

These broker-dealers would be included as Covered Entities because they are a conduit to their customers' accounts at the carrying broker-dealer and have access to information and trading systems of the carrying broker-dealer. Consequently, a significant cybersecurity incident could harm their customers to the extent it causes the customers to lose access to their securities accounts at the carrying broker-dealer. Further, a significant cybersecurity incident at an introducing broker-dealer could spread to the carrying broker-dealer given the information systems that connect the two firms. These connections also may make introducing broker-dealers attractive targets for threat actors seeking to access the information systems of the carrying broker-dealer to which the introducing broker-dealer is connected.

In addition, introducing broker-dealers may store personal information about their customers on their information systems or be able to access this information on the carrying broker-dealer's information systems. The fact that they store this information also may make

---

144 *See* paragraph (a)(1)(i)(B) of proposed Rule 10.

145 *See* FINRA Rule 4311. Pursuant to FINRA requirements, the carrying agreement must specify the responsibilities of the carrying broker-dealer and the introducing broker-dealer, including, at a minimum, the responsibilities for: (1) opening and approving accounts; (2) accepting of orders; (3) transmitting of orders for execution; (4) executing of orders; (5) extending credit; (6) receiving and delivering of funds and securities; (7) preparing and transmitting confirmations; (8) maintaining books and records; and (9) monitoring of accounts. *See* FINRA Rule 4311(c)(1).

them attractive targets for threat actors seeking to use the information to steal identities or assets, or to sell the personal information to other bad actors who will seek to use it for these purposes.

The third category of broker-dealers included as Covered Entities would be broker-dealers that have regulatory capital equal to or exceeding $50 million.[146] Regulatory capital is the total capital of the broker-dealer plus allowable subordinated liabilities of the broker-dealer and is reported on the FOCUS reports broker-dealers file pursuant to Rule 17a-5.[147] The fourth category would be a broker-dealer with total assets equal to or exceeding $1 billion.[148] The $50 million and $1 billion thresholds are modeled on the thresholds that trigger enhanced recordkeeping and reporting requirements for certain broker-dealers pursuant to Exchange Act Rules 17h-1T and 17h-2T.[149]

These thresholds are designed to include as Covered Entities broker-dealers that are large in terms of their assets and dealing activities (and that would not otherwise be Covered Broker-Dealers under the definitions in proposed Rule 10).[150] For example, larger broker-dealers that exceed these thresholds often engage in proprietary trading (including high frequency trading) and are sources of liquidity in certain securities. Consequently, if their critical functions were disrupted or degraded by a significant cybersecurity incident it could have a potential negative impact on those securities markets if it reduces liquidity in the markets through the inability to

---

146 *See* paragraph (a)(1)(i)(C) of proposed Rule 10.

147 *See* 17 CFR 240.17a-5; Form X-17A-5, Line Item 3550.

148 *See* paragraph (a)(1)(i)(D) of proposed Rule 10.

149 *See* 17 CFR 240.17h-1T and 17h-1T. *See also Order Under Section 17(h)(4) of the Securities Exchange Act of 1934 Granting Exemption from Rule 17h–1T and Rule 17h–2T for Certain Broker-Dealers Maintaining Capital, Including Subordinated Debt of Greater Than $20 Million But Less Than $50 Million*, Exchange Act Release No. 89184 (June 29, 2020) [85 FR 40356 (July 6, 2020)] ("17h Release") (setting forth the $50 million and $1 billion thresholds).

150 Size has been recognized as a proxy for substantial market activity relative to other registrants of the same type and therefore a firm's relative risk to the financial markets. *See* 17h Release (noting that broker-dealers that have less than $50 million in regulatory capital and less than $1 billion in total assets are "relatively small in size," and "because of their relative size" and to the extent they are not carrying firms, these entities "present less risk to the financial markets," while stating that with respect to broker-dealers with at least $50 million in regulatory capital or at least $1 billion in total assets "the Commission believes . . . those broker-dealers . . . pose greater risk to the financial markets, investors, and other market participants").

continue dealing and trading activities. For example, a broker-dealer in this situation could lose its ability to provide liquidity to other market participants for an indeterminate length of time, which could lead to unfavorable market conditions for investors, such as higher buy prices and lower sell prices or even the ability to execute a trade within a reasonable amount of time.

In addition, the size and dealing activities of these broker-dealers could make them attractive targets for threat actors seeking to access proprietary and confidential information about the broker-dealer's trading positions and strategies to use for financial advantage. This also may make them attractive targets for threat actors employing ransomware schemes. Further, given their size and trading activities, these broker-dealers may be connected to a number of different Market Entities through information systems, including national securities exchanges, clearing agencies, other broker-dealers, and ATSs.

The fifth category of broker-dealers included as Covered Entities would be broker-dealers that operate as market makers. Specifically, proposed Rule 10 would define "covered entity" to include a broker-dealer that operates as a market maker under the Exchange Act or the rules thereunder (which includes a broker-dealer that operates pursuant to Exchange Act Rule 15c3-1(a)(6)) or is a market maker under the rules of an SRO of which the broker-dealer is a member.[151] The proposed rule's definition of "market maker" is tied to securities laws that confer benefits or impose requirements on market makers and, consequently, covers broker-dealers that take advantage of those benefits or are subject to those requirements. The objective is to rely on these other securities laws to define a market maker rather than set forth a new definition of "market maker" in proposed Rule 10, which could conflict with these other laws.

---

[151] *See* paragraph (a)(1)(i)(E) of proposed Rule 10. *See also* 17 CFR 240.15c3-1 ("Rule 15c3-1"). Paragraph (a)(6) of Rule 15c3-1 permits a market maker to avoid taking capital charges for its proprietary positions provided, among other things, its carrying firm takes the capital charges instead. *See also, e.g.*, Rule 103 of the New York Stock Exchange (setting forth requirements for Designated Market Makers and Designated Market Maker Units).

Market makers would be included as Covered Entities because disruptions to their operations caused by a significant cybersecurity incident could have a material impact on the fair, orderly, and efficient functioning of the U.S. securities markets. For example, a significant cybersecurity incident could imperil a market maker's operations and ability to facilitate transactions in particular securities between buyers and sellers. In addition, market makers typically are connected to a number of different Market Entities through information systems, including national securities exchanges and other broker-dealers.

The sixth category of broker-dealers included as Covered Entities would be broker-dealers that operate an ATS.[152] Since Regulation ATS was adopted in 1998, ATSs have become increasingly important venues for trading securities in a fast and automated manner. ATSs perform exchange-like functions such as offering limit order books and other order types. These developments have made ATSs significant sources of orders and trading interest for securities. ATSs use data feeds, algorithms, and connectivity to perform these functions. ATSs rely heavily on information systems to perform these functions, including to connect to other Market Entities such as broker-dealers and principal trading firms.

A significant cybersecurity incident that disrupts an ATS could negatively impact the ability of investors to liquidate or purchase certain securities at favorable or predictable prices or in a timely manner to the extent it provides liquidity to the market for those securities. Further, a significant cybersecurity incident at an ATS could provide a gateway for threat actors to attack other Market Entities that connect to it through information systems and networks of interconnected information systems. In addition, ATSs are connected to a number of different Market Entities through information systems, including national securities exchanges and other broker-dealers. Finally, the records stored by ATSs on their information systems include

---

[152] *See* paragraph (a)(1)(i)(F) of proposed Rule 10.

proprietary information about the Market Entities that use their services, including confidential business information (*e.g.*, information about their trading activities).

For the foregoing reasons, the categories of broker-dealers discussed above would be Covered Entities under proposed Rule 10. All other categories of broker-dealers would be Non-Covered Entities.

Generally, the types of broker-dealers that would be Non-Covered Entities under proposed Rule 10 are smaller firms whose functions do not play as significant a role in promoting the fair, orderly, and efficient operation of the U.S. securities markets, as compared to broker-dealers that would be Covered Entities.[153] For example, they tend to offer a more focused and limited set of services such as facilitating private placements of securities, selling mutual funds and variable contracts, underwriting securities, and participating in direct investment offerings.[154] Further, they do not act as custodians for customer securities and cash or serve as a conduit (*i.e.*, an introducing broker-dealer) for customers to access their accounts at a carrying broker-dealer that does maintain custody of securities and cash. Therefore, they do not pose the risk that a significant cybersecurity incident could lead to investors losing access to their securities or cash or having those assets stolen. In addition, Non-Covered Broker-Dealers likely are less connected to other Market Participants through information systems than Covered Broker-Dealers. For these reasons, the additional policies and procedures, reporting, and disclosure requirements would not apply to Non-Covered Broker-Dealers.

At the same time, Non-Covered Broker-Dealers are part of the financial sector and exposed to cybersecurity risk. Further, certain Non-Covered Broker-Dealers maintain personal

---

153 For example, as discussed below in section IV.C.2. of this release, the 1,541 broker-dealers that would be Covered Entities had average total assets of $3.5 billion and average regulatory equity of $325 million; whereas the 1,969 that would be Non-Covered Entities had average total assets of $4.7 million and average regulatory equity of $3 million. This means that Non-Covered Broker-Dealers under proposed Rule 10 accounted for about 0.2% of the total assets of all broker-dealers and 0.1% of total capital for all broker-dealers.

154 *See* section IV.C.2. of this release (discussing the activities of broker-dealers that would not meet the definition of "covered entity" in proposed Rule 10).

information about their customers that if accessed by threat actors or mistakenly exposed to unauthorized users could result in harm to the customers. For these reasons, Non-Covered Broker-Dealers—among other things—would be required under proposed Rule 10 to: (1) establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks taking into account their size, business, and operations; (2) review and assess the design and effectiveness of their cybersecurity policies and procedures annually, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review; (3) make a written record that documents the steps taken in performing the annual review and the conclusions of the annual review; and (4) give the Commission and their examining authority immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring.[155] The Commission's objective in proposing Rule 10 is to address the cybersecurity risks faced by all Market Entities but apply a more limited set of requirements to Non-Covered Broker-Dealers commensurate with the level of risk they pose to investors, the U.S. securities markets, and the U.S. financial sector more generally.

c. Market Entities Other Than Broker-Dealers

The MSRB and all clearing agencies, national securities associations, national securities exchanges, SBSDRs, SBS Entities,[156] and transfer agents would be Covered Entities and, therefore, subject to the additional requirements regarding the minimum elements that must be included in their cybersecurity risk management policies and procedures, reporting, and public

---

155 *See* section II.C. of this release (discussing the requirements for these broker-dealers in more detail).

156 In addition to the requirements proposed in Rule 10 itself, the scope of certain existing regulations applicable to SBS Entities would include proposed Rule 10 if adopted; *see, e.g.*, 17 CFR 240.15Fk-1(b)(2)(i) (which establishes the scope of specified chief compliance officer duties by reference to Section 15F of the Exchange Act (15 U.S.C. 78*o*-10) and the rules and regulations thereunder); 17 CFR 240.15Fh-3(h)(2)(iii)(I) (which establishes the scope of specified supervisory requirements by reference to Section 15F(j) of the Exchange Act (15 U.S.C. 78*o*-10(j)).

disclosure.[157] In particular, proposed Rule 10 would define Covered Entity to include: (1) a clearing agency (registered or exempt) under section 3(a)(23)(A) of the Exchange Act;[158] (2) an MSBSP that is registered pursuant to section 15F(b) of the Exchange Act;[159] (3) the Municipal Securities Rulemaking Board;[160] (4) a national securities association under section 15A of the Exchange Act;[161] (5) a national securities exchange under section 6 of the Exchange Act;[162] (6) a security-based swap data repository under section 3(a)(75) of the Exchange Act;[163] (7) a security-based swap dealer that is registered pursuant to section 15F(b) of the Exchange Act;[164] and (8) a transfer agent as defined in section 3(a)(25) of the Exchange Act that is registered or required to be registered with an appropriate regulatory agency ("ARA") as defined in section 3(a)(34)(B) of the Exchange Act.[165]

SROs play a critical role in setting and enforcing rules for their members or registrants that govern trading, fair access, transparency, operations, and business conduct, among other things. SROs and SBSDRs also play a critical role in ensuring fairness in the securities markets through the transparency they provide about securities transactions and pricing, and the information about securities transactions they can provide to regulators. National securities

---

157 *See* paragraphs (a)(1)(ii) through (ix) of proposed Rule 10 (defining these Market Entities as "covered entities").

158 *See* paragraph (a)(1)(ii) of proposed Rule 10. *See also* 15 U.S.C. 78c(a)(23)(A) (defining the term "clearing agency").

159 *See* paragraph (a)(1)(iii) of proposed Rule 10. *See also* 15 U.S.C. 78o-10(b). Registered MSBSPs include both MSBSPs that are conditionally registered pursuant to paragraph (d) of Exchange Act Rule 15Fb2-1 ("Rule 15Fb2-1") (17 CFR 240.15Fb2-1) and MSBSPs that have been granted ongoing registration pursuant to paragraph (e) of Rule 15Fb2-1.

160 *See* paragraph (a)(1)(iv) of proposed Rule 10.

161 *See* paragraph (a)(1)(v) of proposed Rule 10. *See also* 15 U.S.C. 78o-3.

162 *See* paragraph (a)(1)(vi) of proposed Rule 10. *See also* 15 U.S.C. 78f.

163 *See* paragraph (a)(1)(vii) of proposed Rule 10.

164 *See* paragraph (a)(1)(viii) of proposed Rule 10. *See* also 15 U.S.C. 78o-10(b). Registered SBSDs include both SBSDs that are conditionally registered pursuant to paragraph (d) of Rule 15Fb2-1 and SBSDs that have been granted ongoing registration pursuant to paragraph (e) of Rule 15Fb2-1.

165 *See* paragraph (a)(1)(ix) of proposed Rule 10. *See also* 15 U.S.C. 78q-1(c)(1) (registration requirements for transfer agents); 15 U.S.C. 78c(a)(25) (definition of transfer agent) and (a)(34)(B) (definition of appropriate regulatory agency).

exchanges play a critical role in ensuring the orderly and efficient operation of the U.S. securities markets through the marketplaces they operate. Clearing agencies are critical to the orderly and efficient operation of the U.S. securities markets through the centralized clearing and settlement services they provide as well as their role as securities depositories, with exempt clearing agencies serving an important role as part of this process. Market liquidity is critical to the orderly and efficient operation of the U.S. securities markets. In this regard, SBS Entities play a critical role in providing liquidity to the security-based swap market.

The disruption or degradation of the functions of an SRO (including functions that support securities marketplaces and the oversight of market participants) could cause harm to investors to the extent it negatively impacted the fair, orderly, and efficient operations of the U.S. securities markets. For example, it could prevent investors from purchasing or selling securities or doing so at fair or reasonable prices. Investors also would face harm if a transfer agent's functions were disrupted or degraded by a significant cybersecurity incident. Transfer agents provide services such as stockholder recordkeeping, processing of securities transactions and corporate actions, and paying agent activities. Their core recordkeeping systems provide a direct conduit to their issuer clients' master records that document and, in many instances provide the legal underpinning for, registered securityholders' ownership of the issuer's securities. If these functions were disrupted, investors might not be able to transfer ownership of their securities or receive dividends and interest due on their securities positions.

SROs, exempt clearing agencies, and SBSDRs connect to multiple members, registrants, users, or others though networks of information systems. The interconnectedness of these Market Entities with other Market Entities through information systems creates the potential that a significant cybersecurity incident at one Market Entity (*e.g.*, one caused by malware) could spread to other Market Entities in a cascading process that could cause widespread disruptions

threatening the fair, orderly, and efficient operation of the U.S. securities markets.[166] Additionally, the disruption of a Market Entity that provides critical services to other Market Entities through information system connections could disrupt the activities of these other Market Entities if they cannot obtain the services from another source.

SROs, exempt clearing agencies, SBSDRs, SBS Entities, and transfer agents could be prime targets of threat actors because of the central roles they play in the securities markets. For example, threat actors could seek to disrupt their functions for geopolitical purposes. Threat actors also could seek to gain unauthorized access to their information systems to conduct espionage operations on their internal non-public activities. Moreover, because they hold financial assets (*e.g.*, clearing deposits in the case of clearing agencies) and/or store substantial confidential and proprietary information about other Market Entities or financial transactions, they may be choice targets for threat actors seeking to steal the assets or use the financial information to their advantage.

SROs, exempt clearing agencies, and SBSDRs store confidential and proprietary information about their members, registrants, and users, including confidential business information, and personal information. A significant cybersecurity incident at any of these types of Market Entities could lead to the improper use of this information to harm the members, registrants, and users or provide the unauthorized user with an unfair advantage over other market participants and, in the case of personal information, to steal identities. Moreover, given the volume of information stored by these Market Entities about different persons, the harm caused by a cybersecurity incident could be widespread, negatively impacting many victims.

SBS Entities also store proprietary and confidential information about their counterparties on their information systems, including financial information they use to perform credit analysis.

---

166 *See, e.g.*, Implications of Cyber Risk for Financial Stability ("[T]he interconnectedness of the financial system means that an event at one or more firms may spread to others (the domino effect).").

A significant cybersecurity incident at an SBS Entity could lead to the improper use of this information to harm the counterparties or provide the unauthorized user with an unfair advantage over other market participants. Transfer agents store proprietary information about securities ownership and corporate actions. A significant cybersecurity incident at a transfer agent could lead to the improper use of this information to harm securities holders. Transfer agents also may store personal information including names, addresses, phone numbers, email addresses, employers, employment history, bank and specific account information, credit card information, transaction histories, securities holdings, and other detailed and individualized information related to the transfer agents' recordkeeping and transaction processing on behalf of issuers. Threat actors breaching the transfer agent's information systems could use this information to steal identities or financial assets of the persons to whom this information pertains. They also could sell it to other threat actors.

In light of these considerations, the MSRB and all clearing agencies, national securities associations, national securities exchanges, SBSDRs, SBS Entities, and transfer agents would be Covered Entities under proposed Rule 10 and, therefore, subject to the additional requirements regarding the minimum elements that must be included in their cybersecurity risk management policies and procedures, reporting, and public disclosure.[167]

2. "Cybersecurity Incident"

Proposed Rule 10 would define the term "cybersecurity incident" to mean an unauthorized occurrence on or conducted through a Market Entity's information systems that jeopardizes the confidentiality, integrity, or availability of the information systems or any information residing on those systems.[168] The objective is to use a term that is broad enough to

---

[167] *See* paragraphs (a)(1)(ii) through (ix) of proposed Rule 10 (defining these Market Entities as "covered entities").

[168] *See* paragraph (a)(2) of proposed Rule 10. *See generally*, NIST Glossary (defining "cybersecurity risk" as "an effect of uncertainty on or within information and technology" and defining "incident" as "an

encompass within the definition of "cybersecurity incident" the various categories of unauthorized occurrences that can impact an information system (*e.g.*, unauthorized access, use, disclosure, downloading, disruption, modification, or destruction). As discussed earlier, the sources of cybersecurity risk are myriad as are the tactics, techniques, and procedures employed by threat actors.[169]

The definition of "cybersecurity incident" in proposed Rule 10 is designed to include any unauthorized incident impacting an information system or the information residing on the system. An information system can experience an unauthorized occurrence without a threat actor itself directly obtaining unauthorized access to the system. For example, a social engineering tactic could cause an employee to upload ransomware unintentionally that encrypts the information residing on the system or a DoS attack could cause the information system to shut down. In either case, the threat actor did not need to access the information system to cause harm.

While the definition is intended to be broad, the occurrence must be one that *jeopardizes* (*i.e.*, places at risk) the confidentiality, integrity, or availability of the information systems or any information residing on those systems. Confidentiality would be jeopardized if the unauthorized occurrence resulted in or could result in persons accessing an information system or the information residing on the system who are not permitted or entitled to do so or resulted in or could result in the disclosure of the information residing on the information system to the public

---

occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies"); FISMA (defining "incident" as an "occurrence" that: (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. 44 U.S.C. 3552(b)(2).

169 *See* section I.A.1. of this release (discussing the sources of the cybersecurity risk).

or to any person not permitted or entitled to view it.[170] Integrity would be jeopardized if the unauthorized occurrence resulted in or could result in: (1) an unpermitted or unintended modification or destruction of the information system or the information residing on the system; or (2) otherwise resulted in or could result in a compromise of the authenticity of the information system (including its operations and output) and the information residing on the system.[171] Availability would be jeopardized if the unauthorized occurrence resulted in or could result in the Market Entity or other authorized users being unable to access or use the information system or information residing on the system or being unable access or use the information system or information residing on the system in a timely or reliable manner.[172]

3. "Significant Cybersecurity Incident"

Proposed Rule 10 would have a two-pronged definition of "significant cybersecurity incident."[173] The first prong of the definition would be a cybersecurity incident, or a group of related cybersecurity incidents, that significantly disrupts or degrades the ability of the Market Entity to maintain critical operations.[174] As discussed earlier, significant cybersecurity incidents can negatively impact information systems and the information residing on information systems in two fundamental ways. First, they can disrupt or degrade the information system or the information residing on the information system in a manner that prevents the Market Entity from performing functions that rely on the system operating as designed (*e.g.*, an order routing system of an national securities exchange or a margin calculation and collection system of a clearing agency) or that rely on the Market Entity being able to process or access information on the

---

170 *See generally* NIST Glossary (defining "confidentiality" as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information").

171 *See generally* NIST Glossary (defining "integrity" as "guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity").

172 *See generally* NIST Glossary (defining "availability" as "ensuring timely and reliable access to and use of information").

173 *See* paragraphs (a)(10)(i) and (ii) of proposed Rule 10.

174 *See* paragraph (a)(10)(i) of proposed Rule 10.

system (*e.g.*, a general ledger of a broker-dealer or SBS Entity that tracks and records securities transactions).[175] This type of harm can be caused by, for example, a ransomware attack that encrypts the information stored on the system, a DoS attack that overwhelms the information system, or hackers taking control of a the system or shutting it down. Generally, critical operations would be activities, processes, and services that if disrupted could prevent the Market Entity from continuing to operate or prevent it from performing a service that supports the fair, orderly, and efficient functioning of the U.S. securities markets.[176]

The second fundamental way that a significant cybersecurity incident can negatively impact an information system or the information residing on the information system is when unauthorized persons are able to access and use the information stored on the information system (*e.g.*, proprietary business information or personal information).[177] Therefore, the second prong of the definition would be a cybersecurity incident, or a group of related cybersecurity incidents, that leads to the unauthorized access or use of the information or information systems of the Market Entity, where the unauthorized access or use of such information or information systems results in or is reasonably likely to result in: (1) substantial harm to the Market Entity; or (2) substantial harm to a customer, counterparty, member, registrant, or user of the Market Entity, or

---

175 *See* sections I.A.1. and I.A.2. of this release (discussing the consequences of these types of information system degradations and disruptions). This type of impact would compromise the integrity or availability of the information system. *See generally* NIST Glossary (defining "integrity" as "guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity" and "availability" as "ensuring timely and reliable access to and use of information").

176 *See, e.g.*, Basel Committee on Banking Supervision, Principles for Operational Resilience (Mar. 2021) ("The term critical operations is based on the Joint Forum's 2006 high-level principles for business continuity. It encompasses critical functions as defined by the FSB and is expanded to include activities, processes, services and their relevant supporting assets the disruption of which would be material to the continued operation of the bank or its role in the financial system.") (footnotes omitted).

177 *See* sections I.A.1. and I.A.2. of this release (discussing the consequences of this type of compromise of an information system). This type of impact would compromise the confidentiality of the information system. *See generally* NIST Glossary (defining "confidentiality" as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information").

to any other person that interacts with the Market Entity.[178] As discussed earlier, this kind of significant cybersecurity incident could lead to the improper use of this information to harm persons to whom it pertains (*e.g.*, public exposure of their confidential financial information or the use of that information to steal their identities) or provide the unauthorized user with an unfair advantage over other market participants (*e.g.*, trading based on confidential business information).[179]

4. "Cybersecurity Threat"

Proposed Rule 10 would define the term "cybersecurity threat" to mean any potential occurrence that may result in an unauthorized effort to affect adversely the confidentiality, integrity, or availability of a Market Entity's information systems or any information residing on those systems.[180] As discussed earlier, threat actors use a number of different tactics, techniques, and procedures (*e.g.*, malware, social engineering, hacking, DoS attacks) to commit cyber-related crime.[181] These threat actors may be nation states, individuals (acting alone or as part of organized syndicates) seeking financial gain, or individuals seeking to cause harm for a variety of reasons. Further, the threat actors may be external or internal actors. Also, as discussed earlier, errors can pose a cybersecurity threat (*e.g.*, accidentally providing access to confidential information to individuals that are not authorized to view or use it). The definition of "cybersecurity threat" in proposed Rule 10 is designed to include the potential actions of threat

---

178 *See* paragraph (a)(10)(ii) of proposed Rule 10. There could be instances where a significant cybersecurity incident meets both prongs. For example, an unauthorized user that is able to access the Market Entity's internal computer systems could shut down critical operations of the Market Entity and use information on the systems to steal assets of the Market Entity or assets or identities of the Market Entity's customers.

179 *See* sections I.A.1. and I.A.2. of this release (discussing the consequences of this type of compromise of an information system).

180 *See* paragraph (a)(4) of proposed Rule 10. *See generally* NIST Glossary (defining "threat" as any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service and also the potential for a threat-source to successfully exploit a particular information system vulnerability).

181 *See* section I.A.1. of this release (discussing the various tactics, techniques, and procedures used by threat actors).

actors (*e.g.*, seeking to install malware on or hack into an information system or engaging in social engineering tactics) and potential errors (*e.g.*, an employee failing to secure confidential, proprietary, and personal information) that may result in an unauthorized effort to affect adversely the confidentiality, integrity, or availability of a Market Entity's information systems or any information residing on those systems.

5. "Cybersecurity Vulnerability"

Proposed Rule 10 would define the term "cybersecurity vulnerability" to mean a vulnerability in a Market Entity's information systems, information system security procedures, or internal controls, including, for example, vulnerabilities in their design, configuration, maintenance, or implementation that, if exploited, could result in a cybersecurity incident.[182] Cybersecurity vulnerabilities are weaknesses in the Covered Entity's information systems that threat actors could exploit, for example, to hack into the system or install malware.[183] One example would be an information system that uses outdated software that is no longer updated to address known flaws that could be exploited by threat actors to access the system. Cybersecurity vulnerabilities also are weaknesses in the procedures and controls the Market Entity uses to protect its information systems and the information residing on them such as procedures and controls that do not require outdated software to be replaced or that do not adequately restrict access to the system. Cybersecurity vulnerabilities can also include lack of training opportunities for employees to increase their cybersecurity awareness, such as how to properly secure sensitive data and recognize harmful files. The definition of "cybersecurity vulnerability" in proposed Rule 10 is designed to include weaknesses in the information systems themselves and

---

[182] *See* paragraph (a)(5) of proposed Rule 10. *See generally* NIST Glossary (defining "vulnerability" as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source").

[183] *See* section I.A.1. of this release (discussing information system vulnerabilities). *See generally* CISA 2021 Vulnerability Report ("Globally, in 2021, malicious cyber actors targeted internet-facing systems, such as email servers and virtual private network (VPN) servers, with exploits of newly disclosed vulnerabilities.").

weaknesses in the measures the Covered Entity takes to protect the systems and the information residing on the systems.

6. "Cybersecurity Risk"

Proposed Rule 10 would define the term "cybersecurity risk" to mean financial, operational, legal, reputational, and other adverse consequences that could stem from cybersecurity incidents, cybersecurity threats, and cybersecurity vulnerabilities.[184] As discussed earlier, cybersecurity incidents have the potential to cause harm to Market Entities and others who use their services or are connected to them through information systems and, if severe enough, negatively impact the fair, orderly, and efficient operations of the U.S. securities markets.[185] The definition of "cybersecurity risk" in proposed Rule 10 is designed to encompass the types of harm and damage that can befall a Market Entity that experiences a cybersecurity incident.

7. "Information"

As discussed in more detail below, a Market Entity would be required under proposed Rule 10 to establish, maintain, and enforce written policies and procedures that are reasonably designed to address the Market Entity's cybersecurity risks.[186] Cybersecurity risks—as discussed above—would be financial, operational, legal, reputational, and other adverse consequences that could result from cybersecurity incidents, cybersecurity threats, and cybersecurity

---

[184] *See* paragraph (a)(3) of proposed Rule 10. *See also* paragraphs (a)(4) and (5) of proposed Rule 10 (defining, respectively, "cybersecurity threat" to mean "any potential occurrence that may result in an unauthorized effort to affect adversely the confidentiality, integrity, or availability of a Market Entity's information systems or any information residing on those systems" and "cybersecurity vulnerability" to mean "a vulnerability in a Market Entity's information systems, information system security procedures, or internal controls, including, for example, vulnerabilities in their design, configuration, maintenance, or implementation that, if exploited, could result in a cybersecurity incident").

[185] *See* sections I.A.1. and I.A.2. of this release (discussing, respectively, the harms that can be caused by significant cybersecurity incidents generally and with respect to each category of Market Entity).

[186] *See* paragraphs (b)(1) and (e) of proposed Rule 10 (requiring Covered Entities and Non-Covered Entities, respectively, to have policies and procedures to address their cybersecurity risks); sections II.B.1. and II.C. of this release (discussing the requirements of paragraphs (b)(1) and (e) of proposed Rule 10, respectively, in more detail).

vulnerabilities.[187] Cybersecurity incidents would be unauthorized occurrences on or conducted through a market entity's *information systems* that jeopardize the confidentiality, integrity, or availability of the *information systems* or any *information* residing on those systems.[188] Cybersecurity threats would be any potential occurrences that may result in an unauthorized effort to affect adversely the confidentiality, integrity, or availability of a market entity's *information systems* or any *information* residing on those systems.[189] Finally, cybersecurity vulnerabilities would be a vulnerability in a Market Entity's *information systems*, *information system* security procedures, or internal controls, including, for example, vulnerabilities in their design, configuration, maintenance, or implementation that, if exploited, could result in a cybersecurity incident.[190] Consequently, the policies and procedures required under proposed Rule 10 would need to cover all of the Market Entity's *information systems* and *information* residing on those systems in order to address the Market Entity's cybersecurity risks.

Proposed Rule 10 would define the term "information" to mean any records or data related to the Market Entity's business residing on the Market Entity's information systems, including, for example, personal information received, maintained, created, or processed by the Market Entity.[191] The definition is designed to cover the full range of information stored by Market Entities on their information systems regardless of the digital format in which the information is stored.[192] As discussed earlier, Market Entities create and maintain a wide range

---

187 *See* paragraph (a)(3) of proposed Rule 10 (defining "cybersecurity risk").

188 *See* paragraph (a)(2) of proposed Rule 10 (defining "cybersecurity incident").

189 *See* paragraph (a)(4) of proposed Rule 10 (defining "cybersecurity threat").

190 *See* paragraph (a)(5) of proposed Rule 10 (defining "cybersecurity vulnerability").

191 *See* paragraph (a)(6) of proposed Rule 10.

192 *See generally* NIST Glossary (defining "information" as any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. *Id*. (defining "data" (among other things) as: (1) pieces of information from which "understandable information" is derived; (2) distinct pieces of digital information that have been formatted in a specific way; and (3) a subset of information in an electronic format that allows it to be retrieved or transmitted. *Id.* (defining "records" (among other things) as units of related data fields (*i.e.*, groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).

of information on their information systems.[193] This includes information used to manage and conduct their operations, manage and mitigate their risks, monitor the progress of their business, track their financial condition, prepare financial statements, prepare regulatory filings, and prepare tax returns. They also store personal, confidential, and proprietary business information about their customers, counterparties, members, registrants or users. This includes information maintained by clearing agencies, the MSRB, the national securities exchanges, and SBSDRs about market activity and about their members, registrants, and users.

The information maintained by Market Entities on their information systems is an attractive target for threat actors, particularly confidential, proprietary, and personal information.[194] Also, it also can be critical to performing their various functions, and the inability to access and use their information could disrupt or degrade their ability to operate in support of the fair, orderly, and efficient operation of the U.S. securities markets.[195] Consequently, protecting the confidentiality, integrity, and availability of information residing on a Market Entity's information systems is critical to avoiding the harms that can be caused by cybersecurity risk. The definition of "information" in proposed Rule 10 is designed to encompass this information and, therefore, to extend the proposed protections of the rule to it.

8. "Information Systems"

The policies and procedures required under proposed Rule 10 also would need to cover the Market Entity's *information systems* in order to address the Market Entity's cybersecurity risks. Proposed Rule 10 would define the term "information systems" to mean the information resources owned or used by the Market Entity, including, for example, physical or virtual

---

193 *See* section I.A.2. of this release.

194 *See* sections I.A.1. and I.A.2 of this release (discussing how threat actors seek unauthorized access to and use of confidential, proprietary, and personal information to, among other reasons, conduct espionage operations, steal identities, use it for business advantage, hold it hostage (in effect) through a ransomware attack, or sell it to other threat actors).

195 *Id.*

infrastructure controlled by the information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the Market Entity's information to maintain or support the Market Entity's operations.[196]

As discussed earlier, Market Entities use information systems to perform a wide range of functions.[197] For example, they use information systems to maintain books and records to manage and conduct their operations, manage and mitigate their risks, monitor the progress of their business, track their financial condition, prepare financial statements, prepare regulatory filings, and prepare tax returns. Market Entities also use information systems so that their employees can communicate with each other and with external persons. These include email, text messaging, and virtual meeting applications. They also use internet websites to communicate information to their customers, counterparties, members, registrants, or users. They use information systems to perform the functions associated with their status and obligations as a broker-dealer, registered or exempt clearing agency, national securities association, national securities exchange, SBSDR, SBS Entity, SRO, or transfer agent.

Information systems are targets that threat actors attack to access and use information maintained by Market Entities related to their business (particularly confidential, proprietary, and personal information).[198] In addition, the interconnectedness of Market Entities through information systems creates channels through which malware, viruses, and other destructive cybersecurity threats can spread throughout the financial system. Moreover, the disruption or degradation of a Market Entity's information systems could negatively impact the entity's ability to operate in support of the U.S. securities markets.[199] Consequently, protecting the confidentiality, integrity, and availability of a Market Entity's information systems is critical to

---

196 *See* paragraph (a)(7) of proposed Rule 10.

197 *See* section I.A.2. of this release.

198 *See* sections I.A.1. and I.A.2. of this release.

199 *Id.*

avoiding the harms that can be caused by cybersecurity risk. The definition of the term "information systems" in proposed Rule 10 is designed to be broad enough to encompass all the electronic information resources owned or used by a Market Entity to carry out its various operations. Accordingly, the definition of "information systems" would require a Market Entity's policies and procedures to address cybersecurity risks to cover all of its information systems.

9. "Personal Information"

Proposed Rule 10 would define the term "personal information" to mean any information that can be used, alone or in conjunction with any other information, to identify a person, including, but not limited to, name, date of birth, place of birth, telephone number, street address, mother's maiden name, Social Security number, government passport number, driver's license number, electronic mail address, account number, account password, biometric records, or other non-public authentication information.[200] The definition of "personal information" was guided by a number of established sources and aims to capture a broad array of information that can reside on a Market Entity's information systems that may be used alone, or with other information, to identify an individual. The definition is designed to encompass information that if compromised could cause harm to the individuals to whom the information pertains (*e.g.*, identity theft or theft of assets).

---

[200] *See* paragraph (a)(9) of proposed Rule 10. *See generally* NIST Glossary (defining "personal information" as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual and defining "personally identifying information" (among other things) as information that can be used to distinguish or trace an individual's identity—such as name, social security number, biometric data records—either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual (*e.g.*, date and place of birth, mother's maiden name, etc.)); 17 CFR 248.201(b)(8) ((defining "identifying information" as any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any: (1) name, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number; (2) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; (3) unique electronic identification number, address, or routing code; or (4) telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e))).

Personal information is an attractive target for threat actors because they can use it to steal a person's identity and then use the stolen identity to appropriate the person's assets through unauthorized transactions or to make unlawful purchases on credit or to effect other unlawful transactions in the name of the person.[201] They also can sell personal information they obtain through unauthorized access to an information system to criminals who will seek to use the information for these purposes. Moreover, the victims of identity theft can be the more vulnerable members of society (*e.g.*, individuals on fixed-incomes, including retirees). Consequently, proposed Rule 10 would have a provision that specifically addresses protecting personal information.[202]

10. Request for Comment

The Commission requests comment on all aspects of the proposed definitions. In addition, the Commission is requesting comment on the following specific aspects of the proposals:

1. In designing the definitions of proposed Rule 10, the Commission considered a number of sources cited in the sections above, including, in particular, the NIST Glossary and certain Federal statutes and regulations. Are these appropriate sources to consider? If so, explain why. If not, explain why not. Are there other sources the Commission should use? If so, identify them and explain why they should be considered and how they could inform potential modifications to the definitions.
2. In determining which categories of Market Entities would be Covered Entities subject to the additional requirements of proposed Rule 10, the Commission considered: (1) how the category of Market Entity supports the fair, orderly, and

---

201 *See* sections I.A.1. and I.A.2. of this release.

202 *See* paragraph (b)(1)(iii)(A)*(2)* of proposed Rule 10. *See also* proposed Form SCIR, which would elicit information about whether personal information was compromised in a significant cybersecurity incident.

efficient operation of the U.S. securities markets and the consequences if that type of broker-dealer's critical functions were disrupted or degraded by a significant cybersecurity incident; (2) the harm that could befall investors, including retail investors, if that category of Market Entity's functions were disrupted or degraded by a significant cybersecurity incident; (3) the extent to which the category of Market Entity poses cybersecurity risk to other Market Entities though information system connections, including the number of connections; (4) the extent to which the category of Market Entity would be an attractive target for threat actors; and (5) the personal, confidential, and proprietary business information about the category of Market Entity and other persons (*e.g.*, investors) stored on the Market Entity's information systems and the harm that could be caused if that information was accessed or used by threat actors through a cybersecurity breach. Are these appropriate factors to consider? If so, explain why. If not, explain why not. Are there other factors the Commission should take into account? If so, identify them and explain why they should be considered.

3. Should proposed Rule 10 be modified to include other categories of broker-dealers as Covered Entities? If so, identify the category of broker-dealers and explain how to define broker-dealers within that category and why it would be appropriate to apply the additional policies and procedures, reporting, and disclosure requirements of the proposed rule to that category of broker-dealers. For example, should the $50 million regulatory capital threshold be lowered (*e.g.*, to $25 million or some other amount) or should the $1 billion total assets threshold be lowered (*e.g.*, to $500 million or some other amount) to include more broker-dealers as Covered Entities? If so, identify the threshold and explain why it would be appropriate to apply the additional requirements to broker-dealers that fall within that threshold.

4. Should proposed Rule 10 be modified to include as a Covered Entity any broker-dealer that is an SCI entity for the purposes of Regulation SCI? Currently, under Regulation SCI, an ATS that trades certain stocks exceeding specific volume thresholds is an SCI entity?[203] As discussed above, a broker-dealer that operates an ATS would be a Covered Entity under proposed Rule 10 and, therefore, subject to the additional policies and procedures, reporting, and disclosure requirements of the proposed rule. However, the Commission is proposing to amend Regulation SCI to broaden the definition of "SCI entity" to include, among other Commission registrants, a broker-dealer that exceeds an asset-based size threshold or a volume-based trading threshold in NMS stocks, exchange-listed options, agency securities, or U.S. treasury securities.[204] A broker-dealer that exceeds the asset-based size threshold under the proposed amendments to Regulation SCI (which would be several hundred billion dollars) would be subject to the requirements of proposed Rule 10 applicable to Covered Entities, as it would exceed the $1 billion total assets threshold in the broker-dealer definition of "covered entity."[205] Further, a broker-dealer that exceeds one or more of the volume-based trading thresholds under the proposed amendments to Regulation SCI likely would meet one of the broker-dealer definitions of "covered entity" in proposed Rule 10 given its size and activities. For example, it may be carrying broker-dealer, have regulatory capital equal to or exceeding $50 million, have

---

203 *See* 17 CFR 242.1000 (defining the term "SCI alternative trading system" and including that defined term in the definition of "SCI Entity").

204 Regulation SCI 2023 Proposing Release.

205 *See* paragraph (a)(1)(i)(D) of proposed Rule 10. *See also* section II.F.1.c. of this release (discussing why this type of broker-dealer would be a Covered Entity).

total assets equal to or exceeding $1 billion, or operate as a market maker.[206] Nonetheless, should the definition of "covered entity" in proposed Rule 10 be modified to include any broker-dealer that is an SCI entity under Regulation SCI? If so, explain why. If not, explain why not.

5. Should proposed Rule 10 be modified to narrow the categories of broker-dealers that would be Covered Entities? If so, explain how the category should be narrowed and why it would be appropriate not to apply the additional requirements to broker-dealers that would no longer be included as Covered Entities. For example, are there certain types of carrying broker-dealers, introducing broker-dealers, market makers, or ATSs that should not be included as Covered Entities? If so, identify the type of broker-dealer and explain why it would be appropriate not to impose the additional policies and procedures, reporting, and disclosure requirements of the proposed rule on that type of broker-dealer. Similarly, should the proposed $50 million regulatory capital threshold be increased (*e.g.*, to $100 million or some other amount) or should the $1 billion total assets threshold be increased (*e.g.*, to $5 billion or some other amount) to exclude more broker-dealers from the definition of "covered entity"? If so, identify the threshold and explain why it would be appropriate not to apply the additional requirements on the broker-dealers that would not be Covered Entities under the narrower definition.

6. Should proposed Rule 10 be modified to divide other categories of Market Entities into Covered Entities and Non-Covered Entities? If so, identify the category of Market Entity and explain how to define Covered Entity and Non-

---

206 *See* paragraphs (a)(1)(i)(A), (C), (D), and (E) of proposed Rule 10 (defining these categories of broker-dealers as "covered entities"). *See also* section II.F.1.c. of this release (discussing why this type of broker-dealer likely would be a Covered Entity).

Covered Entity within that category and explain why it would be appropriate not to impose the additional policies and procedures, reporting, and disclosure requirements on the Market Entities that would be Non-Covered Entities. For example, are there types of clearing agencies (registered or exempt), MSBSPs, national securities exchanges, SBSDRs, SBSDs, or transfer agents that pose a level of cybersecurity risk to the U.S. securities markets and the participants in those markets that is no greater than the cybersecurity risk posed by the categories of broker-dealers that would be Non-Covered Entities? If so, explain why it would be appropriate not to apply the additional requirements of proposed Rule 10 to these types of Market Entities.

7. Should proposed Rule 10 be modified so that it applies to other participants in the U.S. securities markets that are registered with the Commission? If so, identify the registrant type and explain why it should be subject to the requirements of proposed Rule 10. For example, should competing consolidators or plan processors be subject to the requirements of proposed Rule 10?[207] If so, explain why. If not, explain why not. If competing consolidators or plan processors should be subject to proposed Rule 10, should they be treated as Covered Entities or Non-Covered Entities? If Covered Entities, explain why. If Non-Covered Entities, explain why. Should certain competing consolidators or plan processors be treated as Covered Entities and others be treated as Non-Covered Entities? If so, explain how to define Covered Entity and Non-Covered Entity within that category and explain why it would be appropriate not to apply the additional policies and procedures, reporting, and disclosure requirements of the proposed

---

[207] *See* 17 CFR 242.600(16) and (67) (defining the terms "competing consolidator" and "plan processor," respectively). *See also* 17 CFR 242.1000 (defining "SCI competing consolidator" and defining "SCI entity" to include SCI competing consolidator).

rule to the competing consolidators or plan processors in that category that would not be Covered Entities.

8. Should proposed Rule 10 be modified to revise the broker-dealer definitions of "covered entity"? For example, in order to include carrying broker-dealers as Covered Entities, paragraph (a)(1)(i)(A) of proposed Rule 10 would define the term "covered entity" to include a broker-dealer that maintains custody of cash and securities for customers or other brokers-dealers and is not exempt from the requirements of Rule 15c3-3. In addition, in order to include introducing broker-dealers as Covered Entities, paragraph (a)(1)(i)(B) of proposed Rule 10 would define the term "covered entity" to include a broker-dealer that introduces customer accounts on a fully disclosed basis to another broker-dealer that is a carrying broker-dealer under paragraph (a)(1)(i)(A) of the proposed rule. Would these broker-dealer definitions of "covered entity" work as designed? If not, explain why and suggest modifications to improve their design.

9. In order to include market makers as Covered Entities, paragraph (a)(1)(i)(E) of proposed Rule 10 would define the term "covered entity" to include a broker-dealer that is a market maker under the Exchange Act or the rules thereunder (which includes a broker-dealer that operates pursuant to paragraph (a)(6) of Rule 15c3-1) or is a market maker under the rules of an SRO of which the broker-dealer is a member. Would the definition work as designed? If not, explain why and suggest modifications to improve its design. For example, should the definition be based on a list of the functions and activities of a market maker as distinct from the functions and activities of other categories of broker-dealers? If so, identify the relevant functions and activities and explain how they could be incorporated into a definition.

10. Should paragraph (a)(2) of proposed Rule 10 be modified to revise the definition of "cybersecurity incident"? For example, as discussed above, the definition is designed to include any unauthorized occurrence that impacts an information system or the information residing on the system. Would the definition work as designed? If not, explain why and suggest modifications to improve its design. Is this design objective appropriate? If not, explain why and suggest an alternative design objective for the definition. Is the definition of "cybersecurity incident" overly broad in that it refers to an incident that jeopardizes the confidentiality, integrity, or availability of the information systems or any information residing on those systems? If so, explain why and suggest modifications to appropriately narrow its scope without undermining the objective of the rule to address cybersecurity risks facing Market Entities. Is the definition of "cybersecurity incident" too narrow? If so, how should it be broadened?

11. Should paragraph (a)(3) of proposed Rule 10 be modified to revise definition of "cybersecurity risk"? For example, the NIST definition of "cybersecurity risk" focuses on how this risk can cause harm: it can adversely impact organizational operations (*i.e.*, mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation. The definition of "cybersecurity risk" in proposed Rule 10 was guided by this aspect of cybersecurity risk. Does the definition appropriately incorporate this aspect of cybersecurity risk? If not, explain why and suggest modifications to improve its design. Is this design objective appropriate? If not, explain why and suggest an alternative design objective for the definition.

12. Should paragraph (a)(4) of proposed Rule 10 be modified to revise the definition of "cybersecurity threat"? For example, as discussed above, the definition is designed to include the potential actions of threat actors and errors that may result

in an unauthorized effort to affect adversely the confidentiality, integrity, or availability of a Market Entity's information systems or any information residing on those systems. Would the definition work as designed? If not, explain why and suggest modifications to improve its design. Is the definition of "cybersecurity threat" overly broad in that it includes any "potential occurrence"? If so, explain why and suggest modifications to appropriately narrow its scope without undermining the objective of the rule to address cybersecurity risks facing Market Entities. Is the definition of "cybersecurity threat" too narrow? If so, how should it be broadened?

13. Should paragraph (a)(5) of proposed Rule 10 be modified to revise the definition of "cybersecurity vulnerability"? For example, as discussed above, the definition is designed to include weaknesses in the information systems themselves and weaknesses in the measures the Covered Entity takes to protect the systems and the information residing on the systems. Would the definition work as designed? If not, explain why and suggest modifications to improve its design. Is this design objective appropriate? If not, explain why and suggest an alternative design objective for the definition. Is the definition of "cybersecurity vulnerability" overly broad? If so, explain why and suggest modifications to appropriately narrow its scope without undermining the objective of the rule to address cybersecurity risks facing Market Entities. Is the definition of "cybersecurity vulnerability" too narrow? If so, how should it be broadened?

14. Should paragraph (a)(6) of proposed Rule 10 be modified to revise the definition of "information"? For example, as discussed above, the definition is designed to be broad enough to encompass the wide range of information that resides on the information systems of Market Entities. Would the definition work as designed? If not, explain why and suggest modifications to improve its design. Is this design

objective appropriate? If not, explain why and suggest an alternative design objective for the definition. For example, should the definition focus on information that, if compromised, could cause harm to the Market Entity or others and exclude information that, if compromised, would not cause harm? If so, explain why and suggest rule text to implement this modification.

15. Should paragraph (a)(7) of proposed Rule 10 be modified to revise the definition of "information systems"? For example, as discussed above, the definition is designed to be broad enough to encompass all the electronic information resources owned or used by a Market Entity to carry out its various operations. Would the definition work as designed? If not, explain why and suggest modifications to improve its design. Is this design objective appropriate? If not, explain why and suggest an alternative design objective for the definition. Is the definition of "information systems" overly broad in that it includes any information resource "used by" the Market Entity, which may include information resources developed and maintained by a third party (other than a service provider that that receives, maintains, or processes information, or is otherwise permitted to access the Market Entity's information systems and any of the Market Entity's information residing on those systems)? If so, explain why and suggest modifications to improve its design. Is this design objective appropriate? If not, explain why and suggest an alternative design objective for the definition. Is the definition of "information system" overly narrow? If so, how should it be broadened?

16. Should paragraph (a)(9) of proposed Rule 10 be modified to revise the definition of "personal information"? For example, as discussed above, the definition is designed to encompass information that if compromised could cause harm to the individuals to whom the information pertains (e.g., identity theft or theft of

assets). Would the definition work as designed? If not, explain why and suggest modifications to improve its design. Is this design objective appropriate? If not, explain why and suggest an alternative design objective for the definition.

17. Should paragraph (a)(10) of proposed Rule 10 be modified to revise the definition of "significant cybersecurity incident"? For example, as discussed above, the definition would have two prongs: the first relating to incidents that significantly disrupt or degrade the ability of the Market Entity to maintain critical operations and the second relating to the unauthorized access or use of the information or information systems of the Market Entity. Are these the fundamental ways that significant cybersecurity incidents can negatively impact information systems and the information residing on information systems? If not, explain why and identify other fundamental ways that information and information systems can be negatively impacted by significant cybersecurity incidents that should be incorporated into the definition of "significant cybersecurity incident." Should the term "significant" be defined separately? If so, explain why and suggest potential definitions for this term. Instead, of "significant" should the definition use the word "material." If so, explain why and how that would change the meaning of the definition.

18. Should paragraph (a)(10)(i) of proposed Rule 10 be modified to revise the first prong of the definition of "significant cybersecurity incident"? For example, as explained above, the first prong is designed to address how a "significant cybersecurity incident" can disrupt or degrade the information system or the information residing on the system in a manner that prevents the Market Entity from performing functions that rely on the system operating as designed or that rely on the Market Entity being able to process or access information on the system. Would the first prong of the definition work as designed? If not, explain

why and suggest modifications to improve its design. Is this design objective appropriate? If not, explain why and suggest an alternative design objective for the first prong of the definition. For example, should the first prong of the definition be limited to cybersecurity incidents that "disrupt" the ability of the Market Entity to maintain critical operations (*i.e.*, not include incidents that "degrade" that ability)? If so, explain why and also explain how to distinguish between an incident that degrades the ability of the Market Entity to maintain critical operations and an incident that disrupts that ability. Also, explain why reporting to the Commission and other regulators (as applicable) and publicly disclosing incidents that degrade the ability of the Market Entity to maintain critical operations would not be necessary because they would no longer be significant cybersecurity incidents.[208]

19. Should paragraph (a)(10)(ii) of proposed Rule 10 be modified be to revise the second prong of the definition of "significant cybersecurity incident"? For example, as explained above, the second prong is designed to address how a "significant cybersecurity incident" can cause harm if unauthorized persons are able to access and use the information system or the information residing on the system. Would the definition work as designed? If not, explain why and suggest modifications to improve its design. Is this design objective appropriate? If not, explain why and suggest an alternative design objective for the second prong of the definition. For example, should the second prong of the definition be limited to cybersecurity incidents that "result" in substantial harm to the Market Entity or substantial harm to a customer, counterparty, member, registrant, or user of the

---

208 *See* paragraphs (c) and (d) of proposed Rule 10 (requiring, respectively, immediate notification and subsequent reporting of significant cybersecurity incidents and public disclosure of significant cybersecurity incidents).

Market entity, or to any other person that interacts with the Market Entity (*i.e.*, not include incidents that are "reasonably likely" to result in these consequences)? If so, explain why and also explain why reporting to the Commission and other regulators (as applicable) and publicly disclosing incidents that are reasonably likely to result in these consequences would not be necessary because they would no longer be significant cybersecurity incidents.[209] Alternatively, should the second prong of the definition be limited to an incident of unauthorized access or use that leads to "substantial harm" to a customer, counterparty, member, registrant or user of the Covered Entity, or should "inconvenience" to a customer, counterparty, member, registrant or user be enough? If yes, explain why. Should the second prong of the definition be modified so that it is limited to cybersecurity incidents that result in or are reasonably likely to result in substantial harm to more than one customer, counterparty, member, registrant, or user of the Market Entity, or to any other market participant that interacts with the Market Entity? If so, explain why.

20. Should proposed Rule 10 be modified to define additional terms for the purposes of the rule and Parts I and II of proposed Form SCIR? If so, identify the term, suggest a definition, and explain why including the definition would be appropriate. For example, would including additional defined terms improve the clarity of the requirements of proposed Rule 10 and Parts I and II of proposed Form SCIR? If so, explain why. Should proposed Rule 10 be modified to define the terms "confidentiality," "integrity", and "availability"? If so, explain why and suggest definitions.

---

[209] *See* paragraphs (c) and (d) of proposed Rule 10 (requiring, respectively, immediate notification and subsequent reporting of significant cybersecurity incidents and public disclosure of significant cybersecurity incidents).

B. Proposed Requirements for Covered Entities

1. Cybersecurity Risk Management Policies and Procedures

Risk management is the ongoing process of identifying, assessing, and responding to risk.[210] To manage risk generally, Market Entities should understand the likelihood that an event will occur and the potential resulting impacts.[211] Cybersecurity risk—like other business risks (*e.g.*, market, credit, or liquidity risk)—can be addressed through policies and procedures that are reasonably designed to manage the risk.[212]

Accordingly, proposed Rule 10 would require Covered Entities to establish, maintain, and enforce written policies and procedures that are reasonably designed to address the Covered Entity's cybersecurity risks.[213] Further, proposed Rule 10 would set forth minimum elements that would need to be included in the policies and procedures.[214] In particular, the policies and procedures would need to address: (1) risk assessment; (2) user security and access; (3) information protection; (4) cybersecurity threat and vulnerability management; and (5) cybersecurity incident response and recovery. As discussed in more detail below, the inclusion of these elements is designed to enumerate the core areas that Covered Entities would need to address when designing, implementing, and assessing their policies and procedures. Proposed Rule 10 also would require Covered Entities to review annually and assess their policies and procedures and prepare a written report describing the review and other related matters. Taken together, these requirements are designed to position Covered Entities to be better prepared to protect themselves against cybersecurity risks, to mitigate cybersecurity threats and

---

210 *See generally* NIST Framework.

211 *Id.*

212 *See generally* CISA Cyber Essentials Starter Kit (stating that organizations should "approach cyber as business risk").

213 *See* paragraph (b)(1) of proposed Rule 10.

214 *See* paragraphs (b)(1)(i) through (v) of proposed Rule 10. Covered Entities may wish to consult a number of resources in connection with these elements. *See generally* NIST Framework; CISA Cyber Essentials Starter Kit.

vulnerabilities, and to recover from cybersecurity incidents. They are also designed to help ensure that Covered Entities focus their efforts and resources on the cybersecurity risks associated with their operations and business practices.

The policies and procedures that would be required by proposed Rule 10—because they would need to address the *Covered Entity's cybersecurity risks*—generally should be tailored to the nature and scope of the Covered Entity's business and address the Covered Entity's specific cybersecurity risks. Thus, proposed Rule 10 is not intended to impose a one-size-fits-all approach to addressing cybersecurity risks. In addition, cybersecurity threats are constantly evolving and measures to address those threats continue to evolve. Therefore, proposed Rule 10 is designed to provide Covered Entities with the flexibility to update and modify their policies and procedures as needed so that that they continue to be reasonably designed to address the Covered Entity's cybersecurity risks over time.

a. Risk Assessment

Proposed Rule 10 would specify that the Covered Entity's cybersecurity risk management policies and procedures must include policies and procedures that require periodic assessments of cybersecurity risks associated with the Covered Entity's information systems and information residing on those systems.[215] Further, with respect to the periodic assessments, the policies and procedures would need to include two components.

First, the policies and procedures would need to provide that the Covered Entity will categorize and prioritize cybersecurity risks based on an inventory of the components of the

---

[215] *See* paragraph (b)(1)(i)(A) of proposed Rule 10. *See generally* NIST Framework (providing that the first core element of the framework is "identify"—meaning develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities); IOSCO Cybersecurity Report ("A key component of the risk management program is the identification of critical assets, information and systems, including order routing systems, risk management systems, execution systems, data dissemination systems, and surveillance systems. Practices supporting the identification function include the establishment and maintenance of an inventory of all hardware and software. This risk management program should also typically include third-party and technology providers' security assessments. Finally, accessing information about the evolving threat landscape is important in identifying the changing nature of cyber risk.").

Covered Entity's information systems and information residing on those systems and the potential effect of a cybersecurity incident on the Covered Entity.[216] As discussed earlier, proposed Rule 10 would define the term "cybersecurity risk" to mean financial, operational, legal, reputational, and other adverse consequences that could result from cybersecurity incidents, cybersecurity threats, and cybersecurity vulnerabilities.[217] For example, Covered Entities may be subject to different cybersecurity risks as a result of, among other things: (1) the functions they perform and the extent to which they use information systems to perform those functions; (2) the criticality of the functions they perform that rely on information systems; (3) the interconnectedness of their information systems with third-party information systems; (4) the software that operates on their information systems, including whether it is proprietary or vender-supplied software; (5) the nature and volume of the information they store on information systems (*e.g.*, personal, confidential, and/or proprietary information); (6) the complexity and scale of their information systems (*i.e.*, the size of their IT footprint); (7) the location of their information systems; (8) the number of users authorized to access their information systems; (9) the types of devices permitted to access their information systems (*e.g.*, company-owned or personal desktop computers, laptop computers, or smart phones); (10) the extent to which they conduct international operations and allow access to their information systems from international locations; and (11) the extent to which employees access their information systems from remote locations, including international locations. In categorizing and prioritizing cybersecurity risks, the Covered Entity generally should consider consulting with, among others, personnel familiar

---

216 *See* paragraph (b)(1)(i)(A)(*1*) of proposed Rule 10. *See generally* CISA Cyber Essentials Starter Kit ("Consider how much your organization relies on information technology to conduct business and make it a part of your culture to plan for contingencies in the event of a cyber incident. Identify and prioritize your organization's critical assets and the associated impacts to operations if an incident were to occur. Ask the questions that are necessary to understanding your security planning, operations, and security-related goals. Develop an understanding of how long it would take to restore normal operations. Resist the "it can't happen here" pattern of thinking. Instead, focus cyber risk discussions on "what-if" scenarios and develop an incident response plan to prepare for various cyber events and scenarios.").

217 *See* paragraph (a)(3) of proposed Rule 10; *see also* paragraphs (a)(2), (a)(4), and (a)(5) of proposed Rule 10 (defining, respectively, the terms "cybersecurity incident," cybersecurity threat," and "cybersecurity vulnerability," which are used in the definition of "cybersecurity risk").

with the Covered Entity's operations, its business partners, and third-party cybersecurity experts.[218] In addition, a Covered Entity could consider an escalation protocol in its risk assessment plan to ensure that its senior officers, including appropriate legal and compliance personnel, receive necessary information regarding cybersecurity risks on a timely basis.[219] Only after assessing, categorizing, and prioritizing its cybersecurity risks can a Covered Entity establish, maintain, and enforce reasonably designed cybersecurity policies and procedures under proposed Rule 10 to address those risks.

A Covered Entity also would need to reassess and re-prioritize its cybersecurity risks periodically. The Covered Entity would need to determine the frequency of these assessments and the types of developments in cybersecurity risk that would trigger an assessment based on its particular circumstances. Consequently, the Covered Entity generally should consider whether to reassess its cybersecurity risks to reflect internal changes as they arise, such as changes to its business, online presence, or customer website access, or external changes, such as changes in the evolving technology and cybersecurity threat landscape.[220] The Covered Entity generally should also consider raising any material changes in its risk assessment plan to senior officers, as appropriate. In assessing ongoing and emerging cybersecurity threats, a Covered Entity could

---

218 *See generally* CISA Cyber Essentials Starter Kit ("[H]ave conversations with your staff, business partners, vendors, managed service providers, and others within your supply chain . . . . Maintain situational awareness of cybersecurity threats and explore available communities of interest. These may include sector-specific Information Sharing and Analysis Centers, government agencies, law enforcement, associations, vendors, etc.").

219 *See generally id*. (stating that organizational leaders drive cybersecurity strategy, investment, and culture, and that leaders should, among other things: (1) use risk assessments to identify and prioritize allocation of resources and cyber investments; (2) perform a review of all current cybersecurity and risk policies and identify gaps or weaknesses; and (3) develop a policy roadmap, prioritize policy creation and updates based on the risk to the organization as determined by business leaders and technical staff).

220 *See generally id*. ("Maintain awareness of current events related to cybersecurity. Be proactive; alert staff to hazards that the organization may encounter. Maintain vigilance by asking yourself: what types of cyber attack[s] are hitting my peers or others in my industry? What tactics were successful in helping my peers limit damage? What does my staff need to know to help protect the organization and each other? On a national-level, are there any urgent cyber threats my staff need to know about?").

monitor and consider updates and guidance from private sector and governmental resources, such as the FS-ISAC and CISA.[221]

Second, the policies and procedures would need to require the Covered Entity to identify its service providers that receive, maintain, or process information, or are otherwise permitted to access its information systems and the information residing on those systems, and assess the cybersecurity risks associated with its use of these service providers.[222] Covered Entities are exposed to cybersecurity risks through the technology of their service providers.[223] Having identified the relevant service providers, the Covered Entity would need to assess how they expose it to cybersecurity risks. In identifying these cybersecurity risks, the service provider's cybersecurity practices would be relevant, including: (1) how the service provider protects itself against cybersecurity risk; and (2) its ability to respond to and recover from cybersecurity incidents.

A Covered Entity generally should take into account whether a cybersecurity incident at a service provider could lead to process failures or the unauthorized access to or use of information or information systems. For example, a Covered Entity may use a cloud service provider to

---

221 The FS-ISAC is a global private industry cyber intelligence sharing community solely focused on financial services. Additional information about FS-ISAC is available at https://www.fsisac.com. Often, private industry groups maintain relationships and information sharing agreements with government cybersecurity organizations, such as CISA. Private sector companies, such as information technology and cybersecurity consulting companies, may have insights on cybersecurity (given the access their contractual status gives them to customer networks) that the government initially does not. *See, e.g.*, Verizon DBIR; Microsoft Report. For example, private-sector cybersecurity firms may often be in the position to spot new malicious cybersecurity trends before they become more widespread and common.

222 *See* paragraph (b)(1)(i)(A)(*2*) of proposed Rule 10; paragraphs (a)(6) and (7) of proposed Rule 10 (defining, respectively, the terms "information" and "information systems"). Oversight of third-party service provider or vendor risk is a component of many cybersecurity frameworks. *See, e.g.*, NIST Framework (discussing supply chain risks associated with products and services an organization uses).

223 *See* GAO Cyber Security Report ("Increased connectivity with third-party providers and the potential for increased cyber risk is a concern in the financial industry as core systems and critical data are moved offsite to third parties."). For purposes of proposed Rule 10, the Covered Entity's assessment of service providers should not be limited to only certain service providers, such as those that provide core functions or services for the Covered Entity. Rather, the cybersecurity risk of any service provider that receives, maintains, or processes information, or is otherwise permitted to access the information systems of the Covered Entity and the information residing on those systems should be evaluated. Furthermore, it is possible that a service provider for a Covered Entity may itself be a Covered Entity under proposed Rule 10. For example, a carrying broker-dealer may be a service provider for a number of introducing broker-dealers.

maintain required books and records. If all of the Covered Entity's books and records were concentrated at this cloud service provider and a cybersecurity incident disrupts or degrades the cloud service provider's information systems, there could potentially be detrimental data loss affecting the ability of the Covered Entity to provide services and comply with regulatory obligations. Accordingly, as part of identifying the cybersecurity risks associated with using a cloud service provider, a Covered Entity should consider how the service provider will secure and maintain data and whether the service provider has response and recovery procedures in place such that any compromised or lost data in the event of a cybersecurity incident can be recovered and restored.

Finally, the Covered Entity's risk assessment policies and procedures would need to require written documentation of these risk assessments.[224] This documentation would be relevant to the reviews performed by the Covered Entity to analyze whether the policies and procedures need to be updated, to inform the Covered Entity of risks specific to it, and to support responses to cybersecurity risks by identifying cybersecurity threats to information systems that, if compromised, could result in significant cybersecurity incidents.[225] It also could be used by Commission and SRO staff and possibly internal auditors of the Covered Entity to examine for adherence to the risk assessment policies and procedures.

b. User Security and Access

Proposed Rule 10 would specify that the Covered Entity's cybersecurity risk management policies and procedures must include controls designed to minimize user-related risks and prevent unauthorized access to the Covered Entity's information systems and the

---

224 *See* paragraph (b)(1)(i)(B) of proposed Rule 10.

225 *See* paragraph (b)(2) of proposed Rule 10 (which would require a Covered Entity to review and assess the design and effectiveness of the cybersecurity policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review). *See also* section II.B.1.f. of this release (discussing the review proposal in more detail).

information residing on those systems.[226] Further, the rule would require that these policies and procedures include controls addressing five specific aspects relating to user security and access.

First, there would need to be controls requiring standards of behavior for individuals authorized to access the Covered Entity's information systems and the information residing on those systems, such as an acceptable use policy.[227] Second, there would need to be controls for identifying and authenticating individual users, including but not limited to implementing authentication measures that require users to present a combination of two or more credentials for access verification.[228] Third, there would need to be controls for establishing procedures for the timely distribution, replacement, and revocation of passwords or methods of authentication.[229] Fourth, there would need to be controls for restricting access to specific information systems of the Covered Entity or components thereof and the information residing on those systems solely to individuals requiring access to the systems and information as is necessary for them to perform their responsibilities and functions on behalf of the Covered Entity.[230] Fifth, there would need to be controls for securing remote access technologies.[231]

The objective of these policies, procedures, and controls would be to protect the Covered Entity's information systems from unauthorized access and improper use. There are a variety of controls that a Covered Entity, based on its particular circumstances, could include in these

---

226 *See* paragraph (b)(1)(ii) of proposed Rule 10; paragraphs (a)(6) and (7) of proposed Rule 10 (defining, respectively, the terms "information" and "information systems"). *See generally* NIST Framework (providing that the second core element of the framework is "protect"—meaning develop and implement appropriate safeguards to ensure delivery of critical services); CISA Cyber Essentials Starter Kit (stating with respect to user security and access that (among other things): (1) the authority and access granted employees, managers, and customers into an organization's digital environment needs limits; (2) setting approved access privileges requires knowing who operates on an organization's systems and with what level of authorization and accountability; and (3) organizations should ensure only those who belong on their "digital workplace have access"); IOSCO Cybersecurity Report (stating that network access controls are one of the types of controls trading venues use as the protection function).

227 *See* paragraph (b)(1)(ii)(A) of proposed Rule 10.

228 *See* paragraph (b)(1)(ii)(B) of proposed Rule 10.

229 *See* paragraph (b)(1)(ii)(C) of proposed Rule 10.

230 *See* paragraph (b)(1)(ii)(D) of proposed Rule 10.

231 *See* paragraph (b)(1)(ii)(E) of proposed Rule 10; paragraphs (a)(6) and (7) of proposed Rule 10 (defining, respectively, the terms "information" and "information systems").

policies and procedures to make them reasonably designed to achieve this objective. For example, access to information systems could be controlled through the issuance of user credentials, digital rights management with respect to proprietary hardware and copyrighted software, authentication and authorization methods (*e.g.,* multi-factor authentication and geolocation), and tiered access to personal, confidential, and proprietary information and data and network resources.[232] Covered Entities may wish to consider multi-factor authentication methods that are not based solely on SMS-delivery (*e.g.,* text message delivery) of authentication codes, because SMS-delivery methods may provide less security than other non-SMS based multi-factor authentication methods. Furthermore, Covered Entities could require employees to attend cybersecurity training on how to secure sensitive data and recognize harmful files prior to obtaining access to certain information systems. The training generally could address best practices in creating new passwords, filtering through suspicious emails, or browsing the internet.[233]

Further, a Covered Entity could use controls to monitor user access regularly in order to remove users that are no longer authorized. These controls generally should address the Covered Entity's employees (*e.g.*, removing access for employees that leave the firm) and external users of the Covered Entity's information systems (*e.g.*, customers that no longer use the firm's services or external service providers that no longer are under contract with the firm to provide it with any services). In addition, controls to monitor for unauthorized login attempts and account lockouts, and the handling of customer requests, including for user name and password changes,

---

232 *See generally* CISA Cyber Essentials Starter Kit (stating that organizations should (among other things): (1) learn who is on their networks and maintain inventories of network connections (*e.g.*, user accounts, vendors, and business partners); (2) leverage multi-factor authentication for all users, starting with privileged, administrative and remote access users; (3) grant access and administrative permissions based on need-to-know basis; (4) leverage unique passwords for all user accounts; and (5) develop IT policies and procedures addressing changes in user status (*e.g.*, transfers and terminations).

233 *See generally* CISA Cyber Essentials Starter Kit (stating that organizations should (among other things) leverage basic cybersecurity training to improve exposure to cybersecurity concepts, terminology, and activates associated with implementing cybersecurity best practices).

could be a part of reasonably designed policies and procedures. Similarly, controls to assess the need to authenticate or investigate any unusual customer, member, or user requests (*e.g.*, wire transfer or withdrawal requests) could be a part of reasonably designed policies and procedures.

A Covered Entity also generally should take into account the types of technology through which its users access the Covered Entity's information systems. For example, mobile devices (whether firm-issued or personal devices) that allow employees to access information systems and personal, confidential, or proprietary information residing on these systems may create additional and unique vulnerabilities, including when such devices are used internationally. Consequently, controls limiting mobile or other devices approved for remote access to those issued by the firm or enrolled through a mobile device manager could be part of reasonably designed policies and procedures.

In addition, a Covered Entity could consider controls with respect to its network perimeter such as securing remote network access used by teleworking and traveling employees. This could include controls to identify threats on a network's endpoints. For example, Covered Entities could consider using software that monitors and inspects all files on an endpoint, such as a mobile phone or remote laptop, and identifies and blocks incoming unauthorized communications. Covered Entities generally would need to consider potential user-related and access risks relating to the remote access technologies used at their remote work and telework locations to include controls designed to secure such technologies. For example, a Covered Entity's personnel working remotely from home or a co-working space may create unique cybersecurity risks—such as unsecured or less secure Wi-Fi—that threat actors could exploit to access the Covered Entity's information systems and the information residing on those systems. Accordingly, a Covered Entity could consider whether its user security and access policies, procedures, and controls should have controls requiring approval of mobile or other devices for remote access, and whether training on device policies would be appropriate. The training for

remote workers in particular could focus on phishing, social engineering, compromised passwords, and the consequences of weak network security.

c. Information Protection

Information protection is a key aspect of managing cybersecurity risk.[234] Therefore, proposed Rule 10 would specify that the Covered Entity's cybersecurity risk management policies and procedures would need to address information protection in two ways.[235] First, the policies and procedures would need to include measures designed to protect the Covered Entity's information systems and protect the information residing on those systems from unauthorized access or use, based on a periodic assessment of the Covered Entity's information systems and the information that resides on the systems.[236] The periodic assessment would need to take into account: (1) the sensitivity level and importance of the information to the Covered Entity's business operations; (2) whether any of the information is personal information;[237] (3) where and how the information is accessed, stored and transmitted, including the monitoring of information in transmission; (4) the information systems' access controls and malware

---

234 *See generally* NIST Framework ("The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology."); IOSCO Cybersecurity Report ("There are numerous controls and protection measures that regulated entities may wish to consider in enhancing their cyber security. Such measures can be organizational (like the establishment of security operations centers) or technical (like anti-virus and intrusion prevention systems). Risk assessments help determine the minimum level of controls to be implemented within a project, an application or a database. In addition, employee training and awareness initiatives are critical parts of any cyber security program, including induction programs for newcomers, general training, as well as more specific training (for instance, social engineering awareness). Proficiency tests could be conducted to demonstrate staff understanding and third party training could also be organized. Other initiatives which contribute to raising employees' awareness of cyber security threats include monthly security bulletins emailed to all employees, regular communications regarding new issues and discovered vulnerabilities, use of posters and screen savers, and regular reminders sent to employees. Mock tests can also be conducted to assess employees' preparedness. Employees are also often encouraged to report possible attacks.").

235 *See* paragraph (b)(1)(iii) of proposed Rule 10.

236 *See* paragraph (b)(1)(iii)(A) of proposed Rule 10; paragraphs (a)(6) and (7) of proposed Rule 10 (defining, respectively, the terms "information" and "information systems"). *See generally* CISA Cyber Essentials Starter Kit ("Learn what information resides on your network. Inventory critical or sensitive information. An inventory of information assets provides an understanding of what you are protecting, where that information resides, and who has access. The inventory can be tracked in a spreadsheet, updated quickly and frequently").

237 *See* paragraph (a)(9) of proposed Rule 10 (defining the term "personal information").

protection;[238] and (5) the potential effect a cybersecurity incident involving the information could have on the Covered Entity and its customers, counterparties, members, registrants, or users, including the potential to cause a significant cybersecurity incident.[239]

By performing these assessments, a Covered Entity should be able to determine the measures it would need to implement to prevent the unauthorized access or use of information residing on its information systems. Measures that could be used for this purpose include encryption, network segmentation, and access controls to ensure that only authorized users have access to personal, confidential, and proprietary information and data or critical systems. Measures to identify suspicious behavior also could be used for this purpose. These measures could include consistent monitoring of systems and personnel, such as the generation and review of activity logs, identification of potential anomalous activity, and escalation of issues to senior officers, as appropriate. Further data loss prevention measures could include processes to identify personal, confidential, or proprietary information and data (*e.g.*, account numbers, Social Security numbers, trade information, and source code) and block its transmission to external parties. Additional measures could include testing of systems, including penetration tests. A Covered Entity also could consider measures to track the actions taken in response to findings from testing and monitoring, material changes to business operations or technology, or any other significant events. Appropriate measures for preventing the unauthorized use of information may differ depending on the circumstances of a Covered Entity, such as the systems used by the Covered Entity, the Covered Entity's relationship with service providers, or the level of access

---

238 *See generally* CISA Cyber Essentials Starter Kit ("Leverage malware protection capabilities. Malware is designed to spread quickly. A lack of defense against it can completely corrupt, destroy or render your data inaccessible.").

239 *See* paragraphs (b)(1)(iii)(A)(*1*) through (*5*) of proposed Rule 10. *See generally* CISA Cyber Essentials Starter Kit ("Learn how your data is protected. Data should be handled based on its importance to maintaining critical operations in order to understand what your business needs to operate at a basic level. For example, proprietary research, financial information, or development data need protection from exposure in order to maintain operations. Understand the means by which your data is currently protected; focus on where the protection might be insufficient. Guidance from the Cyber Essentials Toolkits, including authentication, encryption, and data protection help identify methods and resources for how to best secure your business information and devices.").

granted by the Covered Entity to employees or contractors. Appropriate measures generally should evolve with changes in technology and the increased sophistication of cybersecurity attacks.

Second, the policies and procedures for protecting information would need to require oversight of service providers that receive, maintain, or process the Covered Entity's information, or are otherwise permitted to access the Covered Entity's information systems and the information residing on those systems, pursuant to a written contract between the covered entity and the service provider.[240] Further, pursuant to that written contract, the service provider would be required to implement and maintain appropriate measures, including the practices described in paragraphs (b)(1)(i) through (v) of proposed Rule 10, that are designed to protect the Covered Entity's information systems and information residing on those systems. These policies and procedures could include measures to perform due diligence on a service provider's cybersecurity risk management prior to using the service provider and periodically thereafter during the relationship with the service provider. Covered Entities also could consider including periodic contract review processes that allow them to assess whether, and help to ensure that, their agreements with service providers contain provisions that require service providers to implement and maintain appropriate measures designed to protect the Covered Entity's information systems and information residing on those systems.

d. Cybersecurity Threat and Vulnerability Management

Rule 10 would specify that the Covered Entity's cybersecurity risk management policies and procedures must include measures designed to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the Covered Entity's information

---

[240] *See* paragraph (b)(1)(iii)(B) of proposed Rule 10; paragraphs (a)(6) and (7) of proposed Rule 10 (defining, respectively, the terms "information" and "information systems").

systems and information residing on those systems.[241] Because Covered Entities depend on information systems to process, store, and transmit personal, confidential, and proprietary information and data and to conduct critical business functions, it is essential that they manage cybersecurity threats and vulnerabilities effectively.[242] Moreover, detecting, mitigating, and remediating threats and vulnerabilities is essential to preventing significant cybersecurity incidents.

Measures to detect cybersecurity threats and vulnerabilities could include ongoing monitoring (*e.g.*, comprehensive examinations and risk management processes), including, for example, conducting network, system, and application vulnerability assessments. This could include scans or reviews of internal systems, externally facing systems, new systems, and systems used by service providers. Further, measures could include monitoring industry and government sources for new threat and vulnerability information that may assist in detecting cybersecurity threats and vulnerabilities.[243]

Measures to mitigate and remediate an identified threat or vulnerability are more effective if they minimize the window of opportunity for attackers to exploit vulnerable hardware and software. These measures could include, for example, implementing a patch

---

241 *See* paragraph (b)(1)(iv) of proposed Rule 10; paragraphs (a)(4) through (7) of proposed Rule 10 (defining, respectively, the terms "cybersecurity threat," "cybersecurity vulnerability," "information," and "information systems"). *See generally* NIST Framework (providing that the third core element of the framework is "detect"—meaning develop and implement appropriate activities to identify the occurrence of a cybersecurity event); CISA Cyber Essentials Starter Kit (stating regarding detection that organizations should (among other things): (1) learn what is happening on their networks; (2) manage network and perimeter components, host and device components, data at rest and in transit, and user behavior and activities: and (3) actively maintain information as it will provide a baseline for security testing, continuous monitoring, and making security-based decisions); IOSCO Cybersecurity Report ("External and internal monitoring of traffic and logs generally should be used to detect abnormal patterns of access (e.g. abnormal user activity, odd connection durations, and unexpected connection sources) and other anomalies. Such detection is crucial as attackers can use the period of presence in the target's systems to expand their footprint and their access gaining elevated privileges and control over critical systems. Many regulated entities have dedicated cyber threat teams and engage in file servers integrity and database activity monitoring to prevent unauthorized modification of critical servers within their organization's enterprise network. Different alarm categories and severity may be defined.").

242 *See* section I.A.2. of this release (discussing how Covered Entities use information systems).

243 *See generally* CISA, *National Cyber Awareness System – Alerts*, *available at* https://us-cert.cisa.gov/ncas/alerts (providing information about current security issues, vulnerabilities, and exploits).

management program to ensure timely patching of hardware and software vulnerabilities and maintaining a process to track and address reports of vulnerabilities.[244] Covered Entities also generally should consider the vulnerabilities associated with "end of life systems" (*i.e.,* systems in which software is no longer supported by the particular vendor and for which security patches are no longer issued). These measures also could establish accountability for handling vulnerability reports by, for example, establishing processes for their intake, assignment, escalation, remediation, and remediation testing. For example, a Covered Entity could use a vulnerability tracking system that includes severity ratings, and metrics for measuring the time it takes to identify, analyze, and remediate vulnerabilities.

Covered Entities also could consider role-specific cybersecurity threat and vulnerability response training.[245] For example, training could include secure system administration courses for IT professionals, vulnerability awareness and prevention training for web application developers, and social engineering awareness training for employees and executives. Covered Entities that do not proactively address threats and discovered vulnerabilities face an increased likelihood of having their information systems—including the Covered Entity's information residing on those systems—accessed or disrupted by threat actors or otherwise compromised. The requirement for Covered Entities to include cybersecurity threats and vulnerabilities measures in their cybersecurity policies and procedures is designed to address this risk and help ensure threats and vulnerabilities are adequately and proactively addressed by Covered Entities.

---

244 *See generally* CISA Cyber Essentials Starter Kit (stating that organizations should: (1) enable automatic updates whenever possible; (2) replace unsupported operating systems, applications and hardware; and (3) test and deploy patches quickly).

245 *See generally* CISA Cyber Essentials Starter Kit ("Leverage basic cybersecurity training. Your staff needs a basic understanding of the threats they encounter online in order to effectively protect your organization. Regular training helps employees understand their role in cybersecurity, regardless of technical expertise, and the actions they take help keep your organization and customers secure. Training should focus on threats employees encounter, like phishing emails, suspicious events to watch for, and simple best practices individual employees can adopt to reduce risk. Each aware employee strengthens your network against attack, and is another 'sensor' to identify an attack.").

e. Cybersecurity Incident Response and Recovery

Proposed Rule 10 would specify that the Covered Entity's cybersecurity risk management policies and procedures must include measures designed to detect, respond to, and recover from a cybersecurity incident.[246] Further, the rule would require that these measures include policies and procedures that are reasonably designed to ensure: (1) the continued operations of the Covered Entity; (2) the protection of the Covered Entity's information systems and the information residing on those systems;[247] (3) external and internal cybersecurity incident information sharing and communications; and (4) the reporting of significant cybersecurity incidents pursuant to the requirements of paragraph (c) of proposed Rule 10 discussed below.[248]

Cybersecurity incidents can lead to significant business disruptions, including losing the ability to send internal or external communications, transmit information, or connect to internal or external systems necessary to carry out the Covered Entity's critical functions and provide services to customers, counterparties, members, registrants, or users.[249] They also can lead to the inability to access accounts holding cash or other financial assets of the Covered Entity or its

---

246 *See* paragraph (b)(1)(v) of proposed Rule 10; paragraph (c)(2) of proposed Rule 10 (defining the term "cybersecurity incident"). *See generally* NIST Framework (providing that the fourth core element of the framework is "respond"—meaning develop and implement appropriate activities to take action regarding a detected cybersecurity incident; and providing that the fifth core element of the framework is "recover"—meaning develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident).

247 *See* paragraphs (a)(6) and (7) of proposed Rule 10 (defining, respectively, the terms "information" and "information systems").

248 *See* section II.B.2. of this release (discussing the requirements to report significant cybersecurity incidents); paragraph (a)(10) of proposed Rule 10 (defining the term "significant cybersecurity incident"). *See generally* CISA Cyber Essentials Starter Kit (stating regarding response and recovery that the objective is to limit damage and accelerate restoration of normal operations and, to this end, organizations (among other things) can: (1) leverage business impact assessments to prioritize resources and identify which systems must be recovered first; (2) "learn who to call for help (e.g., outside partners, vendors, government/industry responders, technical advisors and law enforcement);" (3) develop an internal reporting structure to detect, communicate and contain attacks; and (4) develop in-house containment measures to limit the impact of cyber incidents when they occur); IOSCO Cybersecurity Report ("Regulated entities generally should consider developing response plans for those types of incidents to which the organization is most likely to be subject. Elements associated with response plans may include: preparing communication/notification plans to inform relevant stakeholders; conducting forensic analysis to understand the anatomy of a breach or an attack; maintaining a database recording cyber attacks; and conducting cyber drills, firm specific simulation exercises as well as industry-wide scenario exercises.").

249 *See* sections I.A.1. and I.A.2. of this release (discussing these consequences).

customers, counterparties, members, registrants, or users.[250] Therefore, the proposed incident response and recovery policies and procedures are designed to place the Covered Entity in a position to respond to a cybersecurity incident, which should help to reduce business disruptions and other harms the incident may cause the Covered Entity or its customers, counterparties, members, registrants, or users. A cybersecurity program with a clear incident response plan designed to ensure continued operational capability, and the protection of, and access to, personal, confidential, or proprietary information and data, even if a Covered Entity loses access to its systems, would assist in mitigating the effects of a cybersecurity incident.[251] A Covered Entity, therefore, may wish to consider maintaining physical copies of its incident response plan—and other cybersecurity policies and procedures—to help ensure they can be accessed and implemented during a cybersecurity incident.

Covered Entities generally should focus on operational capability in creating reasonably designed policies and procedures to ensure their continued operations in the event of a cybersecurity incident (*e.g.*, the ability to withstand a DoS attack). The objective is to place Covered Entities in a position to be able to continue providing services to other Market Entities and other participants in the U.S. securities markets (including investors) and, thereby, continue to support the fair, orderly, and efficient operation of the U.S. securities markets. For example, this requirement is designed to place Covered Entities in a position to be able to continue to perform market and member surveillance and oversight in the case of SROs, clearance and settlement in the case of clearing agencies, and brokerage or dealing activities in the case of broker-dealers and SBSDs.

---

250 *Id.*

251 *See generally* CISA Cyber Essentials Starter Kit ("Plan, prepare, and conduct drills for cyber-attacks and incidents as you would a fire or robbery. Make your reaction to cyber incidents or system outages an extension of your other business contingency plans. This involves having incident response plans and procedures, trained staff, assigned roles and responsibilities, and incident communications plans.").

The ability of Covered Entities to recover from a cybersecurity incident in a timeframe that minimizes disruptions to their business or regulatory activities is critically important to the fair, orderly, and efficient operations of the U.S. securities markets and, therefore, to the U.S. economy, investors, and capital formation. A Covered Entity generally should consider implementing safeguards, such as backing up data, which can help facilitate a prompt recovery that allows the Covered Entity to resume operations following a cybersecurity incident.[252] A Covered Entity also generally should consider whether to designate personnel to perform specific roles in the case of a cybersecurity incident. This could entail identifying and/or hiring personnel or third parties who have the requisite cybersecurity and recovery expertise (or are able to coordinate effectively with outside experts) as well as identifying personnel who should be kept informed throughout the response and recovery process. In addition, a Covered Entity could consider an escalation protocol in its incident response plan to ensure that its senior officers, including appropriate legal and compliance personnel, receive necessary information regarding cybersecurity incidents on a timely basis.[253]

Moreover, as discussed in further detail below, under proposed Rule 10, a Covered Entity would need to give the Commission immediate written electronic notice of a significant cybersecurity incident after having a reasonable basis to conclude that the incident has occurred or is occurring.[254] Further, the Covered Entity would need to report information about the

---

[252] *See generally* CISA Cyber Essentials Starter Kit ("Leverage protections for backups, including physical security, encryption and offline copies. Ensure the backed-up data is stored securely offsite or in the cloud and allows for at least seven days of incremental rollback. Backups should be stored in a secure location, especially if you are prone to natural disasters. Periodically test your ability to recover data from backups. Online and cloud storage backup services can help protect against data loss and provide encryption as an added level of security. Identify key files you need access to if online backups are unavailable to access your files when you do not have an internet connection.").

[253] *See generally* CISA Cyber Essentials Starter Kit (stating that: (1) organizations should develop an internal reporting structure to detect, communicate, and contain attacks and that effective communication plans focus on issues unique to security breaches; (2) a standard reporting procedure will reduce confusion and conflicting information between leadership, the workforce, and stakeholders; and (3) communication should be continuous, since most data breaches occur over a long period of time and not instantly and that it should come from top leadership to show commitment to action and knowledge of the situation).

[254] *See* paragraph (c)(1) of proposed Rule 10. *See also* section II.B.2. of this release (discussing this proposed notification requirement in more detail).

significant cybersecurity incident promptly, but no later than 48 hours, after having a reasonable basis to conclude that the incident has occurred or is occurring by filing Part I of proposed Form SCIR with the Commission.[255] Thereafter, the Covered Entity would need to file an amended Part I of proposed Form SCIR with the Commission under certain circumstances.[256] Accordingly, proposed Rule 10 would require the Covered Entity to include in its incident response and recovery policies and procedures measures designed to ensure compliance with these notification and reporting requirements.[257] The Covered Entity also may wish to implement a process to determine promptly whether and how to contact local and Federal law enforcement authorities, such as the FBI, about an incident.[258]

A Covered Entity also could consider including periodic testing requirements in its incident response and recovery policies and procedures.[259] These tests could assess the efficacy of the policies and procedures to determine whether any changes are necessary, for example, through tabletop or full-scale exercises. Relatedly, proposed Rule 10 would require that the incident response and recovery policies and procedures include written documentation of a

---

255 *See* paragraph (c)(2) of proposed Rule 10. *See also* section II.B.2. of this release (discussing this proposed reporting requirement in more detail).

256 The circumstances under which an amended Part I of proposed Form SCIR would need to be filed are discussed below in section II.B.2. of this release.

257 *See* paragraph (b)(1)(v)(A)(*4*) of proposed Rule 10.

258 For example, the FBI has instructed individuals and organizations to contact their nearest FBI field office to report cybersecurity incidents or to report them online at https://www.ic3.gov/Home/FileComplaint. *See* FBI, *What We Investigate, Cyber Crime*, *available at* https://www.fbi.gov/investigate/cyber. *See also* CISA Cyber Essentials Starter Kit ("As part of your incident response, disaster recovery, and business continuity planning efforts, identify and document partners you will call on to help. Consider building these relationships in advance and understand what is required to obtain support. CISA and the Federal Bureau of Investigation (FBI) provide dedicated hubs for helping respond to cyber and critical infrastructure attacks. Both have resources and guidelines on when, how, and to whom an incident is to be reported in order to receive assistance. You should also file a report with local law enforcement, so they have an official record of the incident.").

259 *See generally* CISA Cyber Essentials Starter Kit ("Lead development of an incident response and disaster recovery plan outlining roles and responsibilities. Test it often. Incident response plans and disaster recovery plans are crucial to information security, but they are separate plans. Incident response mainly focuses on information asset protection, while disaster recovery plans focus on business continuity. Once you develop a plan, test the plan using realistic simulations (known as "war-gaming"), where roles and responsibilities are assigned to the people who manage cyber incident responses. This ensures that your plan is effective and that you have the appropriate people involved in the plan. Disaster recovery plans minimize recovery time by efficiently recovering critical systems.").

cybersecurity incident, including the Covered Entity's response to and recovery from the incident.[260] This record could be used by the Covered Entity to assess the efficacy of, and adherence to, its incident response and recovery policies and procedures. It further could be used as a "lessons-learned" document to help the Covered Entity respond more effectively the next time it experiences a cybersecurity incident. The Commission staff and SRO staff also would use the records to review compliance with this aspect of proposed Rule 10.

f. Annual Review and Required Written Reports

In addition to requiring a Covered Entity to establish, maintain, and enforce written policies and procedures to address cybersecurity risk, proposed Rule 10 would require the Covered Entity, at least annually, to: (1) review and assess the design and effectiveness of the cybersecurity policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review; and (2) prepare a written report that describes the review, the assessment, and any control tests performed, explains their results, documents any cybersecurity incident that occurred since the date of the last report, and discusses any material changes to the policies and procedures since the date of the last report.[261] The annual review requirement is designed to require the Covered Entity to evaluate whether its cybersecurity policies and procedures continue to work as designed. In making this assessment, Covered Entities generally should consider whether changes are needed to ensure their continued effectiveness, including oversight of any delegated responsibilities. As discussed earlier, the sophistication of the tactics, techniques, and procedures employed by threat actors is increasing.[262] The review requirement is designed to impose a discipline on Covered

---

260 *See* paragraph (b)(1)(v)(B) of proposed Rule 10.

261 *See* paragraph (b)(2) of proposed Rule 10.

262 *See* section I.A.1. of this release (discussing, for example, how cybersecurity threats are evolving); *see also* Bank of England CBEST Report (stating that "[t]he threat actor community, once dominated by amateur hackers, has expanded to include a broad range of professional threat actors, all of whom are strongly motivated, organised and funded").

Entities to be vigilant in assessing whether their cybersecurity risk management policies and procedures continue to be reasonably designed to address this risk.

The review would need to be conducted no less frequently than annually. As discussed above, one of the required elements that would need to be included in the policies and procedures is the requirement to perform periodic assessments of cybersecurity risks associated with the covered entity's information systems and information residing on those systems.[263] Based on the findings of those risk assessments, a Covered Entity could consider whether to perform a review prior to the one-year anniversary of the last review. In addition, the occurrence of a cybersecurity incident or significant cybersecurity incident impacting the Covered Entity or other entities could cause the Covered Entity to consider performing a review before the next annual review is required.

The Covered Entity would need to document the review in a written report.[264] The required written report generally should be prepared or overseen by the persons who administer the Covered Entity's cybersecurity program. This report requirement is designed to assist the Covered Entity in evaluating the efficacy of organization's cybersecurity risk management policies and procedures. Additionally, the requirement to review and assess the design and effectiveness of the cybersecurity policies and procedures includes whether they reflect changes in cybersecurity risk over the time period covered by the review. Therefore, the Covered Entity generally would need to take into account the periodic assessments of cybersecurity risks performed pursuant to the requirements of paragraphs (b)(1)(i)(A) and (b)(1)(iii)(A) of proposed Rule. This could provide Covered Entities with valuable insights into potential enhancements to the policies and procedures to keep them up-to-date (*i.e.*, reasonably designed to address emerging cybersecurity threats). For example, incorporating the cybersecurity risk assessments

---

263 *See* paragraph (b)(1)(i) of proposed Rule 10. *See also* section II.B.1.a. of this release (discussing the assessment proposal in more detail).

264 *See* paragraph (b)(2)(ii) of proposed Rule 10.

into the required written report could provide senior officers who review the report with information on the specific risks identified in the assessments. This could lead them to ask questions and seek relevant information regarding the effectiveness of the Covered Entity's cybersecurity risk management policies and procedures and its implementation in light of those risks. This could include questions as to whether the Covered Entity has adequate resources with respect to cybersecurity matters, including access to cybersecurity expertise.

g. Request for Comment

The Commission requests comment on all aspects of the requirements that Covered Entities establish, maintain, and enforce written policies and procedures to address their cybersecurity risks, the elements that would need to be included in the cybersecurity risk management policies and procedures, and the required (at least) annual review of the cybersecurity risk management policies and procedure under paragraph (b) of proposed Rule 10. In addition, the Commission is requesting comment on the following specific aspects of the proposals:

21. In designing the cybersecurity risk management policies and procedures requirements of proposed Rule 10, the Commission considered a number of sources cited in the sections above, including, in particular, the NIST Framework and the CISA Cyber Essentials Starter Kit. Are there other sources the Commission should use? If so, identify them and explain why they should be considered and how they could inform potential modifications to the cybersecurity risk management policies and procedures requirements.

22. Should the policies and procedures requirements of paragraph (b)(1) of proposed Rule 10 be modified? For example, are there other elements that should be included in cybersecurity risk management policies and procedures? If so, identify them and explain why they should be included. Should any of the

minimum required elements be eliminated? If so, identify them and explain why it would be appropriate to eliminate them from the rule.

23. Should the policies and procedures requirements of paragraph (b)(1) of proposed Rule 10 be modified to provide more flexibility in how a Covered Entity implements them? If so, identify the requirements that are too prescriptive and explain why and suggest ways to make them more flexible without undermining the objective of having Covered Entities adequately address cybersecurity risks.

24. Should the policies and procedures requirements of paragraph (b)(1) of proposed Rule 10 be modified to provide less flexibility in how a Covered Entity had to implement them? If so, identify the requirements that should be more prescriptive and explain why and suggest ways to make them more prescriptive without undermining the objective of having Covered Entities implement cybersecurity risk management policies and procedures that address their particular circumstances.

25. Should the policies and procedures requirements of paragraph (b)(1) of proposed Rule 10 be deemed to be reasonably designed if they are consistent with industry standards comprised of cybersecurity risk management practices that are widely available to cybersecurity professionals in the financial sector and issued by an authoritative body that is a U.S. governmental entity or agency, association of U.S. governmental entities or agencies, or widely recognized organization? If so, identify the standard or standards and explain why it would be appropriate to deem the policies and procedures requirements of paragraph (b)(1) of proposed Rule 10 reasonably designed if they are consistent with the standard or standards.

26. The policies and procedures requirements of paragraph (b)(1) of proposed Rule 10 would require Covered Entities to cover "information" and "information systems" as defined, respectively, in paragraphs (a)(6) and (7) of proposed Rule

10 without limitation. Should the proposed policies and procedures requirements of paragraph (b)(1) of proposed Rule 10 be modified to address a narrower set of information and information systems? If so, describe how the narrower set of information and information systems should be defined and why it would be appropriate to limit the policies and procedures requirements to this set of information and information systems. For example, should the policies and procedures requirements of paragraph (b)(1) of proposed Rule 10 be limited to information and information systems that, if compromised, would result in, or would be reasonably likely to result in, harm to the Covered Entity or others? If so, explain why. If not, explain why not. Is there another way to limit the application of the policies and procedures requirements to certain information and information systems that would not undermine the objective that Covered Entities implement policies and procedures that adequately address their cybersecurity risks? If so, explain how.

27. Should the requirements of paragraph (b)(1)(i) of proposed Rule 10 relating to periodic assessments of the cybersecurity risks associated with the Covered Entity's information systems and information residing on those systems be modified? If so, explain why. If not, explain why not.

28. Should the requirements of paragraph (b)(1)(i)(A)*(1)* of proposed Rule 10 relating to categorizing and prioritizing cybersecurity risks based on an inventory of the components of the Covered Entity's information systems and information residing on those systems and the potential effect of a cybersecurity incident on the Covered Entity be modified? If so, explain why. If not, explain why not.

29. Should the requirements of paragraph (b)(1)(i)(A)*(2)* of proposed Rule 10 relating to identifying the Covered Entity's service providers that receive, maintain, or process information, or are otherwise permitted to access the Covered Entity's

information systems and any of the Covered Entity's information residing on those systems, and assess the cybersecurity risks associated with the Covered Entity's use of these service providers be modified? If so, explain why. If not, explain why not. Certain Covered Entities may use data feeds from third-party providers that do not receive, maintain, or process information for the Covered Entity but that could nonetheless cause significant disruption for the Covered Entity if they were the subject of a cybersecurity incident. For example, broker-dealers may subscribe to third-party data feeds to satisfy their obligations for best execution under the federal securities laws. If a third-party provider of data feeds experienced a cybersecurity breach, it could lead to faulty market information being shared with the broker-dealer, which could in turn impact the broker-dealer's ability to operate and execute trades for its customers. Likewise, SBS Entities might rely on data from counterparties. Should the Commission require the risk assessment to include service providers that provide data feeds to Covered Entities but do not otherwise have access to the Covered Entities' information systems? If so, should the risk assessment be limited to only those third parties who provide data critical to the Covered Entity's business operations? Are there other cybersecurity risks associated with utilizing a third party who provides data feeds that should be addressed? If so, identify the risks and explain how they could be addressed.

30. Should the requirements of paragraph (b)(1)(i)(B) of proposed Rule 10 relating to requiring written documentation of the risk assessments required by paragraph (b)(1)(i)(A) of proposed Rule 10 be modified? If so, explain why. If not, explain why not.

31. Should the requirements of paragraph (b)(1)(ii) of proposed Rule 10 relating to controls designed to minimize user-related risks and prevent unauthorized access

to the Covered Entity's information systems and the information residing on those systems? If so, explain why. If not, explain why not. Should requirements of paragraph (b)(1)(ii) of proposed Rule 10 be modified to revise the requirement to include the following identified controls: (1) controls requiring standards of behavior for individuals authorized to access the Covered Entity's information systems and the information residing on those systems, such as an acceptable use policy; (2) controls identifying and authenticating individual users, including but not limited to implementing authentication measures that require users to present a combination of two or more credentials for access verification; (3) controls establishing procedures for the timely distribution, replacement, and revocation of passwords or methods of authentication; (4) controls restricting access to specific information systems of the Covered Entity or components thereof and the information residing on those systems solely to individuals requiring access to the systems and information as is necessary for them to perform their responsibilities and functions on behalf of the Covered Entity; and (5) securing remote access technologies? If so, explain why. If not, explain why not. For example, should this paragraph of the proposed rule be modified to include any additional type of controls? If so, identify the controls and explain why they should be included. Should the text of the proposed controls be modified? For example, should the control pertaining to the timely distribution, replacement, and revocation of passwords or methods of authentication use a word other than "distribution"? If so, explain why and suggest an alternative word that would be more appropriate. Would "establishment" or "setting up" be more appropriate in this context? Should this paragraph of the proposed rule be modified to eliminate any of the identified controls? If so, identify the control and explain why it should be eliminated. For example, could the control pertaining to implementing

authentication measures requiring users to present a combination of two or more credentials for access verification potentially become obsolete? If so, explain why and suggest an alternative control that could incorporate this requirement as well as other authentication controls that may develop in the future.

32. CISA has developed a catalog of cyber "bad practices" that are exceptionally risky and can increase risk to an organization's critical infrastructure.[265] These bad practices include the use of unsupported (or end-of-life) software, use of known or default passwords and credentials, and the use of single-factor authentication. In addition, the Federal Financial Institutions Examination Council ("FFIEC") has issued guidance on authentication and access to financial institution services and systems, and suggests that the use of single-factor authentication as a control mechanism has shown to be inadequate against certain cyber threats and adverse impacts from ransomware, customer account fraud, and identity theft.[266] Instead, the FFIEC guidance suggests the use of multi-factor authentication and other measures, such as specific authentication solutions, password controls, and access and transaction controls. Should paragraph (b)(1)(ii) of proposed Rule 10 be modified to specifically require controls that users provide multi-factor authentication before they can access an information system of the Covered Entity? If so, explain why. If not, explain why not. Would it be appropriate to require multi-factor authentication for all of the Covered Entity's information systems or for a more limited set of information

---

265 *See* CISA, *Bad Practices*, *available at* https://www.cisa.gov/BadPractices.

266 *See* FFIEC, *Authentication and Access to Financial Institution Services and Systems* (Aug. 2021), *available at* https://www.ffiec.gov/guidance/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf. *See also* FDIC and the Office of the Comptroller of the Currency ("OCC"), *Joint Statement on Heightened Cybersecurity Risk* (Jan. 16, 2020), *available at* https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-5a.pdf (noting that identity and access management controls include multifactor authentication to segment and safeguard access to critical systems and data on an organization's network).

systems? For example, should multi-factor authentication be required for public-facing information systems such as applications that provide users access to their accounts at the Covered Entity and not required for internal information systems used by the Covered Entity's employees? If so, explain why. If not, explain why not. Should multi-factor authentication be required regardless of whether the information system is public facing if personal, confidential, or proprietary information resides on the information system? If so, explain why. If not, explain why not. Should the rule require phishing-resistant multi-factor authentication? If so, explain why. If not, explain why not.

33. Should the requirements of paragraph (b)(1)(iii)(A) of proposed Rule 10 relating to measures designed to monitor the Covered Entity's information systems and protect the information residing on those systems from unauthorized access or use be modified? For example, should the requirements of paragraph (b)(1)(iii)(A) of proposed Rule 10 specifically require encryption of certain information residing on the Covered Entity's information systems? If so, explain why. If not, explain why not.

34. The measures discussed in paragraph (b)(1)(iii)(A) of proposed Rule 10 designed to monitor the Covered Entity's information systems and protect the information residing on those systems from unauthorized access or use would need to be based on a periodic assessment of the Covered Entity's information systems and the information that resides on the systems that takes into account: (1) the sensitivity level and importance of the information to Covered Entity's business operations; (2) whether any of the information is personal information; (3) where and how the information is accessed, stored and transmitted, including the monitoring of information in transmission; (4) the information systems' access controls and malware protection; and (5) the potential effect a cybersecurity

incident involving the information could have on the Covered Entity and its customers, counterparties, members, or users, including the potential to cause a significant cybersecurity incident. Should this paragraph of the proposed rule be modified to include any additional factors that would need to be taken into account? If so, identify the factors and explain why they should be taken into account. Should this paragraph of the proposed rule be modified to eliminate any of the identified factors that should be taken into account? If so, identify the factors and explain why they should be eliminated.

35. Should the requirements of paragraph (b)(1)(iii)(A) of proposed Rule 10 relating periodic assessments of the Covered Entity's information systems and information residing of the systems be modified to specifically require periodic (*e.g.*, semi-annual or annual) penetration tests? If so, explain why. If not, explain why not. If proposed Rule 10 should be modified to require periodic penetration tests, should the rule specify the information systems and information to be tested? If so, explain why. If not, explain why not. For example, should the penetration tests be performed on all information systems and information of the Covered Entity? Alternatively, should the penetration tests be performed: (1) on a random selection of information systems and information; (2) on a prioritized selection of the information systems and information residing on them that are most critical to the Covered Entity's functions or that maintain information that if accessed by or disclosed to persons not authorized to view it could cause the most harm to the Covered Entity or others; and/or (3) on information systems for which the Covered Entity has identified vulnerabilities pursuant to the requirements of paragraph (b)(1)(iv) of proposed Rule 10? Please explain the advantages and disadvantages of each potential approach to requiring penetration tests.

36. Should the requirements of paragraph (b)(1)(iii)(B) of proposed Rule 10 relating to the oversight of service providers that receive, maintain, or process the Covered Entity's information, or are otherwise permitted to access the Covered Entity's information systems and the information residing on those systems, pursuant to a written contract between the covered entity and the service provider, through which the service providers are required to implement and maintain appropriate measures, including the practices described in paragraphs (b)(1)(i) through (v) of proposed Rule 10, that are designed to protect the Covered Entity's information systems and information residing on those systems be modified? If so, explain why. If not, explain why not. For example, would there be practical difficulties with implementing the requirement to oversee the service providers through a written contract? If so, explain why. If not, explain why not. Are there alternative approaches to addressing the cybersecurity risk that arises when Covered Entities use service providers? If so, describe them and explain why they would be appropriate in terms of addressing this risk. For example, rather than addressing this risk through written contract, could it be addressed through policies and procedures to obtain written assurances or certifications from service providers that the service provider manages cybersecurity risk in a manner that would be consistent with how the Covered Entity would need to manage this risk under paragraph (b) of proposed Rule 10? If so, explain why and describe the type of assurances or certifications Covered Entities could reasonably obtain to ensure that their service providers are taking appropriate measures to manage cybersecurity risk? In responding, please explain how assurances or certifications would be an appropriate alternative to written contracts in terms of addressing the cybersecurity risk caused by the use of service providers.

37. Should the requirements of paragraph (b)(1)(iv) of proposed Rule 10 relating to measures designed to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the Covered Entity's information systems and the information residing on those systems be modified? If so, explain why. If not, explain why not.

38. Should the requirements of paragraph (b)(1)(v)(A) of proposed Rule 10 relating to measures designed to detect, respond to, and recover from a cybersecurity incident be modified? If so, explain why. If not, explain why not. For example, these measures would need to include policies and procedures that are reasonably designed to ensure: (1) the continued operations of the covered entity; (2) the protection of the Covered Entity's information systems and the information residing on those systems; (3) external and internal cybersecurity incident information sharing and communications; and (4) the reporting of significant cybersecurity incidents pursuant to paragraph (c) of proposed Rule 10. Would these four specific design objectives required of the policies and procedures place the Covered Entity in a position to effectively detect, respond to, and recover from a cybersecurity incident? If so, explain why. If not, explain why not. Should this paragraph of the proposed rule be modified to include any additional design objectives for these policies and procedures? If so, identify the design objectives and explain why they should be included. For example, should the rule require policies and procedures that are designed to recover from a cybersecurity incident within a specific timeframe such as 24, 48, or 72 hours or some other period? If so, identify the recovery period and explain why it would be appropriate. Should this paragraph of the proposed rule be modified to eliminate any of the specified design objectives? If so, identify the design objectives and explain why they should be eliminated.

39. Should the requirements of paragraph (b)(1)(v)(B) of proposed Rule 10 relating to written documentation of any cybersecurity incidents be modified? If so, explain why. If not, explain why not. For example, should the written documentation requirements apply to a narrower set of incidents than those that would meet the definition of "cybersecurity incident" under proposed Rule 10? If so, describe the narrower set of incidents and explain why it would be appropriate to limit the written documentation requirements to them.

40. Should the requirements of paragraph (b)(2) of proposed Rule 10 relating to the review and assessment of the policies and procedures and a written report of the review by modified? If so, explain why. If not, explain why not. For example, this paragraph would require: (1) a review and assessment of the design and effectiveness of the cybersecurity risk management policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review; and (2) the preparation of a written report that describes the review, the assessment, and any control tests performed, explains their results, documents any cybersecurity incident that occurred since the date of the last report, and discusses any material changes to the policies and procedures since the date of the last report. Should the review requirement be modified to provide greater flexibility based on the Covered Entity's assessment of what it believes would be most effective in light of its cybersecurity risks? If so, explain why. If not, explain why not. Should the review, assessment, and report be required on a more frequent basis such as quarterly? If so, explain why. If not, explain why not. Should the review, assessment, and report requirement be triggered after certain events regardless of when the previous review was conducted? If so, explain why. If not, explain why not. For example, should the requirement be triggered if the Covered Entity

experiences a significant cybersecurity incident or undergoes a significant business event such as a merger, acquisition, or the commencement of a new business line that relies on information systems? If so, explain why and suggest how a "significant business event" should be defined for the purposes of the review and assessment requirement. If not, explain why not. Should the rule require that persons with a minimum level of cybersecurity expertise or experience must perform the review and assessment or that the review and assessment must be performed by a senior officer of the Covered Entity? If so, explain why. If not, explain why not. Should the rule require that the review and assessment be performed by personnel who are not involved in designing and implementing the cybersecurity policies and procedures? If so, explain why. If not, explain why not. Should the rule require that the annual report be subject to periodic third-party audits or reviews? If so, explain why. If not, explain why not. Should the Commission provide guidance to clarify how the review and report requirements of paragraph (b)(2) proposed Rule 10 interact with the requirements that SBS Entities perform assessments under 17 CFR 240.15Fk-1 or reviews under 17 CFR 250.15c3-4(c)(3)? If so, explain why. If not, explain why not.

2. Notification and Reporting of Significant Cybersecurity Incidents

a. Timing and Manner of Notification and Reporting

FSOC observed that "[s]haring timely and actionable cybersecurity information can reduce the risk that cybersecurity incidents occur and can mitigate the impacts of those that do occur."[267] The Commission is proposing to require that Covered Entities provide immediate notice and subsequent reports about significant cybersecurity incidents to the Commission and,

---

[267] FSOC 2021 Annual Report.

in the case of certain Covered Entities, other regulators. The objective is to improve the Commission's ability to monitor and evaluate the effects of a significant cybersecurity incident on Covered Entities and their customers, counterparties, members, registrants, or users, as well as assess the potential risks affecting financial markets more broadly.

For these reasons, proposed Rule 10 would require a Covered Entity to provide immediate written electronic notice to the Commission of a significant cybersecurity incident upon having a reasonable basis to conclude that the incident has occurred or is occurring.[268] The Commission would keep the notices nonpublic to the extent permitted by law. The notice would need to identify the Covered Entity, state that the notice is being given to alert the Commission of a significant cybersecurity incident impacting the Covered Entity, and provide the name and contact information of an employee of the Covered Entity who can provide further details about the nature and scope of the significant cybersecurity incident.

The immediate notice would need to be submitted by the Covered Entity electronically in written form (as opposed to permitting the notice to made telephonically).[269] The Commission is proposing a written notification requirement because of the number of Market Entities that

---

[268] *See* paragraph (c)(1) of proposed Rule 10. *See also* paragraph (a)(10) of proposed Rule 10 (defining the term "significant cybersecurity incident"). As discussed below in section II.C. of this release, Non-Covered Broker-Dealers would be subject to an identical immediate written electronic notice requirement. *See* paragraph (e)(2) of proposed Rule 10. If proposed Rule 10 is adopted, it is anticipated that a dedicated email address would be set up to receive the notices from Covered Entities and Non-Covered Broker-Dealers. *See, e.g.*, *Staff Guidance for Filing Broker-Dealer Notices, Statements and Reports*, *available at* https://www.sec.gov/divisions/marketreg/bdnotices; *Staff Statement on Submitting Notices, Statements, Applications, and Reports for Security-Based Swap Dealers and Major Security-Based Swap Participants Pursuant to the Financial Responsibility Rules (Exchange Act Rules 18a-1 through 18a-10)*, *available at* https://www.sec.gov/tm/staff-statement-on-submissions.

[269] *See* paragraph (c)(1) of proposed Rule 10. *But see* 17 CFR 242.1002(b)(1) (requiring an SCI entity to provide the Commission with immediate notice after having a reasonable basis to conclude that an SCI event has occurred without specifying that the notice be written); OCC, Federal Reserve Board, FDIC, *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers*, 86 FR 66424 (Nov. 23, 2021) (requiring a banking organization to provide notice to a designated point of contact of a computer-security incident through telephone, email, or similar methods).

would be subject to the requirement and because of the different types of Market Entities.[270] A written notification would also facilitate the Commission in identifying patterns and trends across Market Entities experiencing significant cybersecurity incidents.

The notice requirement would be triggered when the Covered Entity *has a reasonable basis to conclude* that a significant cybersecurity incident has occurred or is occurring.[271] This does not mean that the Covered Entity can wait until it definitively concludes that a significant cybersecurity incident has occurred or is occurring. In the early stages of discovering the existence of a cybersecurity incident, it may not be possible for the Covered Entity to conclude definitively that it is a *significant* cybersecurity incident. For example, the Covered Entity may need to assess which information systems have been subject to the cybersecurity incident and the impact that the incident has had on those systems before definitively concluding that it is a significant cybersecurity incident.[272] The objective of the notification requirement is to alert the Commission staff as soon as the Covered Entity detects the existence of a cybersecurity incident that it has a reasonable basis to conclude is a significant cybersecurity incident and not to wait until the Covered Entity definitively concludes it is a significant cybersecurity incident. This would provide the Commission staff with the ability to begin to assess the situation at an earlier stage of the cybersecurity incident.

---

[270] Non-Covered Broker-Dealers also would be subject to an immediate written electronic notice requirement under paragraph (e)(2) of proposed Rule 10 and, therefore, the Commission potentially could receive notices from all types of Market Entities. As discussed in section V.C. of this release, it is estimated that 1,989 Market Entities would be Covered Entities and 1,969 broker-dealers would be Non-Covered Entities resulting in a 3,958 total Market Entities. This is a far larger number of entities than the 47 entities that currently are SCI entities.

[271] The notice requirement for Non-Covered Broker-Dealers also would be triggered when the broker-dealer has a reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring. *See* paragraph (e)(2) of proposed Rule 10.

[272] *See* paragraph (a)(2) of proposed Rule 10 (defining "cybersecurity incident" to mean an unauthorized occurrence on or conducted through a Market Entity's information systems that jeopardizes the confidentiality, integrity, or availability of the information systems or any information residing on those systems).

This proposed immediate written notification requirement is modelled on other notification requirements that apply to broker-dealers and SBSDs pursuant to other Exchange Act rules. Under these existing requirements, broker-dealers and certain SBSDs must provide the Commission with same-day written notification if they undergo certain adverse events, including falling below their minimum net capital requirements or failing to make and keep current required books and records.[273] The objective of these requirements is to provide the Commission staff with the opportunity to respond when a broker-dealer or SBSD is in financial or operational difficulty.[274] Similarly, the written notification requirements of proposed Rule 10 are designed to provide the Commission staff with the opportunity to begin assessing the situation promptly when a Covered Entity is experiencing a significant cybersecurity incident by, for example, assessing the Covered Entity's operating status and engaging in discussions with the Covered Entity to understand better what steps it is taking to protect its customers, counterparties, members, registrants, or users. In addition, a Covered Entity that is a broker-dealer would need to provide the written notice to its examining authority, and a transfer agent would need to provide the written notice to its ARA.[275] The objective is to notify other supervisory authorities to allow them the opportunity to respond to the significant cybersecurity incident impacting the Covered Entity.

As discussed above, the immediate written electronic notice is designed to alert the Commission on a confidential basis to the existence of a significant cybersecurity incident impacting a Covered Entity so the Commission staff can begin to assess the event. It is not intended as a means to report written information about the significant cybersecurity incident.

---

[273] *See* 17 CFR 240.17a-11 (notification rule for broker-dealers); 17 CFR 240.18a-8 (notification rule for SBS Entities).

[274] *See Recordkeeping and Reporting Requirements for Security-Based Swap Dealers, Major Security-Based Swap Participants, and Broker-Dealers; Capital Rule for Certain Security-Based Swap Dealers*, Exchange Act Release No. 71958 (Apr. 17, 2014) [79 FR 25194, 25247 (May 2, 2014)] ("SBS Entity Recordkeeping and Reporting Proposing Release").

[275] *See* paragraphs (c)(1)(i) and (ii) of proposed Rule 10. Non-Covered Broker-Dealers also would be required to provide the written notice to their examining authority. *See* paragraph (e)(2) of proposed Rule 10.

Therefore, in addition to the immediate written electronic notice, a Covered Entity would be required to report detailed information about the significant cybersecurity incident by filing, on a confidential basis, Part I of proposed Form SCIR with the Commission through the Electronic Data Gathering, Analysis, and Retrieval System ("EDGAR" or "EDGAR system").[276] Because of the sensitive nature of the information and the fact that threat actors could potentially use it to cause more harm, the Commission would not make the filings available to the public to the extent permitted by law.

As with the notice, the requirement to file Part I of proposed Form SCIR would be triggered when the Covered Entity *has a reasonable basis to conclude* that a significant cybersecurity incident has occurred or is occurring. Therefore, the notification and reporting requirements would be triggered at the same time. However, in order to provide the Covered Entity time to gather the information that would be elicited by Part I of proposed Form SCIR, the Covered Entity would need to file the form promptly, but no later than 48 hours, upon having a reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring.

Proposed Rule 10 also would require the Covered Entity to file an amended Part I of proposed Form SCIR with updated information about the significant cybersecurity incident in four circumstances.[277] In each case, the amended Part I of proposed Form SCIR would need to be filed promptly, but no later than 48 hours, after the update requirement is triggered. First, the Covered Entity would need to file an amended Part I of proposed Form SCIR if any information previously reported to the Commission on the form pertaining to the significant cybersecurity

---

[276] *See* paragraph (c)(2) of proposed Rule 10. As discussed below, Part II of proposed Form SCIR would be used by Covered Entities to make public disclosures about the cybersecurity risks they face and the significant cybersecurity incidents they experienced during the current or previous calendar year. *See* sections II.B.2. and II.B.4. of this release (discussing these proposed requirements). Non-Covered Broker-Dealers would not be subject to the requirements to file Part I and Part II of proposed Form SCIR.

[277] *See* paragraphs (c)(2)(ii)(A) through (D) of proposed Rule 10.

incident becomes materially inaccurate.[278] Second, the Covered Entity would need to file an amended Part I of proposed Form SCIR if any new material information pertaining to the significant cybersecurity incident previously reported to the Commission on the form is discovered.[279] The Commission staff generally would use the information reported on Part I of proposed Form SCIR to assess the operating status of the Covered Entity and assess the impact that the significant cybersecurity incident could have on other participants in the U.S. securities markets. The requirement to file an amended Part I of proposed Form SCIR under the first and second circumstances is designed to ensure the Commission and Commission staff have reasonably accurate and complete information when undertaking these activities.

Third, the Covered Entity would need to file an amended Part I of proposed Form SCIR after the significant cybersecurity incident is resolved.[280] A significant cybersecurity incident impacting a Covered Entity would be resolved when the situation no longer meets the definition of "significant cybersecurity incident."[281] The resolution of a significant cybersecurity incident would be a material development in the situation and, therefore, would be a reporting trigger under proposed Rule 10.

Finally, if the Covered Entity conducted an internal investigation pertaining to the significant cybersecurity incident, it would need to file an amended Part I of proposed Form SCIR after the investigation is closed.[282] This would be an investigation of the significant cybersecurity incident that seeks to determine the cause of the incident or to examine whether there was a failure to adhere to the Covered Entity's policies and procedures to address cybersecurity risk or whether those policies and procedures are effective. An internal

---

278 *See* paragraph (c)(2)(ii)(A) of proposed Rule 10.

279 *See* paragraph (c)(2)(ii)(B) of proposed Rule 10.

280 *See* paragraph (c)(2)(ii)(C) of proposed Rule 10.

281 *See* paragraph (a)(10) of proposed Rule 10 (defining the term "significant cybersecurity incident").

282 *See* paragraph (c)(2)(ii)(D) of proposed Rule 10.

investigation could be conducted by the Covered Entity's own personnel (*e.g.*, internal auditors) or by external consultants hired by the Covered Entity. The closure of an internal investigation would be a reporting trigger under proposed Rule 10 because it could yield material new information about the incident that had not been reported in a previously filed Part I of proposed Form SCIR.

As with the immediate written electronic notice, a Covered Broker-Dealer would need to promptly transmit a copy of each Part I of proposed Form SCIR it files with the Commission to its examining authority, and a transfer agent would need to promptly transmit a copy of each Part I of proposed Form SCIR it files with the Commission to its ARA.[283] The objective is to provide these other supervisory authorities with the same information about the significant cybersecurity incident that the Commission receives.

In this regard, the reporting requirements under proposed Rule 10 would provide the Commission and its staff with information to understand better the nature and extent of a particular significant cybersecurity incident and the efficacy of the Covered Entity's response to mitigate the disruption and harm caused by the incident. The Commission staff could use the reports to focus on the Covered Entity's operating status and to facilitate their outreach to, and discussions with, personnel at the Covered Entity who are addressing the significant cybersecurity incident. For example, certain information provided in a report may be sufficient to address any questions the staff has about the incident; and in other instances staff may want to ask follow-up questions to get a better understanding of the matter. In addition, the reporting would provide the staff with a view into the Covered Entity's understanding of the scope and impact of the significant cybersecurity incident. All of this information would be used by the Commission and its staff in assessing the impact of the significant cybersecurity incident on the Covered Entity.

---

[283] *See* paragraphs (c)(2)(iii)(A) and (B) of proposed Rule 10.

The information provided to the Commission under the proposed reporting requirements also would be used to assess the potential cybersecurity risks affecting U.S. securities markets more broadly. This information could be useful in assessing other and future significant cybersecurity incidents. For example, these reports could assist the Commission in identifying patterns and trends across Covered Entities, including widespread cybersecurity incidents affecting multiple Covered Entities at the same time. Further, the reports could be used to evaluate the effectiveness of various approaches to respond to and recover from a significant cybersecurity incident.

b. Part I of Proposed Form SCIR

Proposed Rule 10 would require a Covered Entity to report information about a significant cybersecurity incident confidentially on Part I of proposed Form SCIR.[284] The form would elicit certain information about the significant cybersecurity incident through check boxes, date fields, and narrative fields. Covered Entities would file Part I of proposed Form SCIR electronically with the Commission using the EDGAR system in accordance with the EDGAR Filer Manual, as defined in Rule 11 of Regulation S-T,[285] and in accordance with the requirements of Regulation S-T.[286]

A Covered Entity would need to indicate on Part I of proposed Form SCIR whether the form is being filed with respect to a significant cybersecurity incident as an initial report, amended report, or final amended report by checking the appropriate box. As discussed above, proposed Rule 10 would require a Covered Entity to file Part I of proposed Form SCIR upon having a reasonable basis to conclude that a significant cybersecurity incident has occurred or is

---

284 *See* paragraph (c)(2) of proposed Rule 10.

285 *See* 17 CFR 232.11.

286 *See* paragraphs (c)(2)(i) and (ii) of proposed Rule 10. As discussed below in section II.B.4. of this release, the Covered Entity would need to file Part I of proposed Form SCIR using a structured data language.

occurring.[287] This would be the initial Part I of proposed Form SCIR with respect to the significant cybersecurity incident.[288] Thereafter, a Covered Entity would be required to file an amended Part I of proposed Form SCIR with respect to the significant cybersecurity incident after: (1) any information previously reported to the Commission on Part I of proposed Form SCIR pertaining to the significant cybersecurity incident becomes materially inaccurate; (2) any new material information pertaining to the significant cybersecurity incident previously reported to the Commission on Part I of proposed Form SCIR is discovered; (3) the significant cybersecurity incident is resolved; or (4) an internal investigation pertaining to a significant cybersecurity incident is closed.[289] If a Covered Entity checks the box indicating that the filing is a final Part I of proposed Form SCIR, the firm also would need to check the appropriate box to indicate why a final form was being filed: either the significant cybersecurity incident was resolved or an internal investigation pertaining to the incident was closed.

Part I of proposed Form SCIR would elicit information about the Covered Entity that would be used to identify the filer.[290] In particular, the Covered Entity would need to provide its full legal name and business name (if different from its legal name), tax identification number, unique identification code ("UIC") (if the filer has a UIC), central index key ("CIK number"),[291] and main address.[292] The instructions to proposed Form SCIR (which would be applicable to Parts I and II) would provide that a UIC is an identification number that has been issued by an internationally recognized standards-setting system ("IRSS") that has been recognized by the

---

287 *See* paragraph (c)(2)(i) of proposed Rule 10. *See also* section II.B.2.a. of this release (discussing the proposed filing requirements in more detail).

288 *See* Instruction B.1. of proposed Form SCIR.

289 *See* paragraphs (c)(2)(ii)(A) through (D) of proposed Rule 10.

290 *See* Line Items 1.A. through 1.E. of Part I of proposed Form SCIR.

291 A CIK number is used on the Commission's computer systems to identify persons who have filed disclosures with the Commission.

292 *See* Line Items 1.A. through 1.C. of Part I of proposed Form SCIR.

Commission pursuant to Rule 903(a) of Regulation SBSR.[293] Currently, the Commission has recognized only the Global Legal Entity Identifier Foundation ("GLEIF") – which is responsible for overseeing the Global Legal Entity Identifier System ("GLEIS") – as an IRSS.[294] Part I of proposed Form SCIR also would elicit the name, phone number, and email address of the contact employee of the Covered Entity.[295] The contact employee would need to be an individual authorized by the Covered Entity to provide the Commission with information about the significant cybersecurity incident (*i.e.*, information the individual can provide directly) and make information about the incident available to the Commission (*e.g.*, information the individual can provide by, for example, making other employees of the Covered Entity available to answer questions of the Commission staff).[296] The Covered Entity also would need to indicate the type of Market Entity it is by checking the appropriate box or boxes.[297] For example, if the Covered Entity is dually registered as a broker-dealer and SBSD, it would need to check the box for each of those entity types.

Page 1 of Part I of proposed Form SCIR also would contain fields for the individual executing the form to sign and date the form. By signing the form, the individual would: (1) certify that the form was executed on behalf of, and with the authority of, the Covered Entity; (2)

---

293 *See* Instruction A.5.g. of proposed Form SCIR. *See also*, *e.g.*, Form SBSE *available at* https://www.sec.gov/files/form-sbse.pdf (providing a similar definition of UIC).

294 *See Regulation SBSR – Reporting and Dissemination of Security-Based Swap Information*, Exchange Act Release No. 74244 (Feb. 11, 2015), 80 FR 14563, 14632 (Mar. 19, 2015) ("Regulation SBSR Release"). LEIs are unique alphanumeric codes that identify legal entities in financial transactions in international markets. *See* Financial Stability Board ("FSB"), *Options to Improve Adoption of the LEI, in Particular for Use in Cross-Border Payments* (July 7, 2022). Information associated with the LEI, which is a globally-recognized digital identifier that is not specific to the Commission, includes the "official name of the legal entity as recorded in the official registers[,]" the entity's address, country of incorporation, and the "legal form of the entity." *Id.* Accordingly, in proposing to require each Covered Entity to provide its UIC if it has a UIC, the Commission is proposing to require each Covered Entity identify itself with an LEI if it has an LEI.

295 *See* Line Item 1.D. of Part I of proposed Form SCIR.

296 *See* Instruction B.4. of proposed Form SCIR.

297 *See* Line Item 1.E. of Part I of proposed Form SCIR (setting forth check boxes to indicate whether the Covered Entity is a broker-dealer, clearing agency, MSBSP, the MRSB, a national securities association, a national securities exchange, SBSD, SBSDR, or transfer agent).

represent individually, and on behalf of the Covered Entity, that the information and statements contained in the form are current, true and complete; and (3) represent individually, and on behalf of the Covered Entity, that to the extent any information previously submitted is not amended such information is current, true, and complete. The form of the certification is designed to ensure that the Covered Entity, through the individual executing the form, provides information that the Commission and Commission staff can rely on to evaluate the operating status of the Covered Entity, assess the impact the significant cybersecurity incident may have on other participants in the U.S. securities markets, and formulate an appropriate response to the incident.

Line Items 2 through 14 of Part I of proposed Form SCIR would elicit information about the significant cybersecurity incident and the Covered Entity's response to the incident. After discovering the existence of a significant cybersecurity incident, a Covered Entity may need time to determine the scope and impact of the incident in order to provide meaningful responses to these questions. For example, the Covered Entity may be working diligently to investigate and resolve the significant cybersecurity incident at the same time it would be required to complete and file Part I of proposed Form SCIR. The Covered Entity's priorities in the early stages after detecting the significant cybersecurity incident may be to devote its staff resources to mitigating the harms caused by the incident or that could be caused by the incident if necessary corrective actions are not promptly implemented. Moreover, during this period, the Covered Entity may not have a complete understanding of the cause of the significant cybersecurity incident, all the information systems impacted by the incident, the harm caused by the incident, or how to best resolve and recover from the incident (among other relevant information).

Therefore, the first form filed with respect to a given significant cybersecurity incident should include information that is known to the Covered Entity at the time of filing and not include speculative information. If information is unknown at the time of filing, the Covered Entity should indicate that on the form. Understanding the aspects of the significant

cybersecurity incident that are not yet known would inform the Commission's assessment. The process of filing an amended Part I of proposed Form SCIR is designed to update earlier filings as information becomes known to the Covered Entity. In particular, proposed Rule 10 would require the Covered Entity to file an amended Part I of proposed Form SCIR if information reported on a previously filed form pertaining to the significant cybersecurity incident becomes materially incomplete because new information is discovered.[298] Therefore, as the Covered Entity reasonably concludes that additional information about the significant cybersecurity incident is necessary to make its filing not materially inaccurate, it would need to file amended forms. In this way, the reporting requirements of proposed Rule 10 are designed to provide the Commission and Commission staff with current known information and provide a means for the Covered Entity to report information as it becomes known.

This does not mean that the Covered Entity can refrain from providing known information in Part I of proposed Form SCIR. As discussed above, the Covered Entity must certify through the individual executing the form that the information and statements in the form are current, true, and complete, among other things. A failure to provide current, true, and complete information that is known to the Covered Entity would be inconsistent with this required certification. In addition, failing to investigate the significant cybersecurity incident would be inconsistent with the policies and procedures required by proposed Rule 10. As discussed above, the cybersecurity incident response and recovery policies and procedures that would be required by proposed Rule 10 would need to include policies and procedures that are reasonably designed to ensure the reporting of significant cybersecurity incidents as required by the rule.[299] The failure to diligently investigate the significant cybersecurity incident could indicate that the Covered Entity's incident response and recovery policies and procedures are not

---

298 *See* paragraph (c)(2)(ii)(B) of proposed Rule 10.

299 *See* paragraph (b)(1)(v)(A)(*4*) of proposed Rule 10. *See also* section II.B.1.e. of this release (discussing these proposed required policies and procedures in more detail).

reasonably designed or are not being enforced by the Covered Entity as required by proposed Rule 10.[300] Moreover, reasonably designed policies and procedures to detect, respond to, and recover from a cybersecurity incident, as required by proposed Rule 10 generally should require diligent investigation of the significant cybersecurity incident.[301] Further, diligently investigating the significant cybersecurity incident would be in the interest of the Covered Entity as it could lead to a quicker resolution of the incident by revealing—for example—its cause and impact.

In terms of the information about the significant cybersecurity incident elicited in Part I of proposed Form SCIR, the Covered Entity first would be required to provide the approximate date that it discovered the significant cybersecurity incident.[302] As discussed above, a Covered Entity would be required to provide the Commission with immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the incident has occurred or is occurring.[303] This can be based on, for example, the Covered Entity reviewing or receiving a record, alert, log, or notice about the incident. In addition, reaching this conclusion would trigger the requirement to file promptly (but within 48 hours) an initial Part I of proposed Form SCIR with the Commission to first report the significant cybersecurity incident using the form.[304] The date that would need to be reported on proposed Part I of Form SCIR is the date the Covered Entity has a reasonable basis to conclude that the incident has occurred or is occurring.[305]

---

300 *See* paragraph (b)(1) of proposed Rule 10 (requiring that the Covered Entity establish, maintain, and enforce written policies and procedures that are reasonably designed to address the covered entity's cybersecurity risks).

301 *See* paragraph (b)(1)(v)(A) of proposed Rule 10. *See also* section II.B.1.e. of this release (discussing these proposed required policies and procedures in more detail).

302 *See* Line Item 2 of Part I of proposed Form SCIR.

303 *See* paragraph (c)(1) of proposed Rule 10. *See also* section II.B.2.a. of this release (discussing the proposed notification requirement in more detail).

304 *See* paragraph (c)(2)(i) of proposed Rule 10. *See also* section II.B.2.a. of this release (discussing the proposed reporting trigger in more detail).

305 *See* Instruction B.5.a. of proposed Form SCIR.

Line Item 3 of Part I of proposed Form SCIR would elicit information about the approximate duration of the significant cybersecurity incident.[306] First, the Covered Entity would need to indicate whether the significant cybersecurity incident is ongoing.[307] The form would provide the option of answering yes, no, or unknown. Second, the Covered Entity would need to provide the approximate start date of the cybersecurity incident or indicate that it does not know the start date.[308] The start date may be well before the date the Covered Entity discovered the significant cybersecurity incident. Therefore, the start date of the incident reported on Line Item 3 may be different than the discovery date reported on Line Item 2. Third, the Covered Entity would need to provide the approximate date the significant cybersecurity incident is resolved.[309] This would be the date the Covered Entity was no longer undergoing a significant cybersecurity incident.[310] As discussed above, the resolution of the significant cybersecurity incident triggers the requirement to file an amended Part I of proposed Form SCIR under proposed Rule 10.[311]

Line Item 4 of Part I of proposed Form SCIR would require the Covered Entity to indicate whether an internal investigation pertaining to the significant cybersecurity incident was being conducted. An "internal investigation" would be defined as a formal investigation of the significant cybersecurity incident by internal personnel of the Covered Entity or external personnel hired by the Covered Entity that seeks to determine any of the following: the cause of the significant cybersecurity incident; whether there was a failure to adhere to the Covered Entity's policies and procedures to address cybersecurity risk; or whether the Covered Entity's

---

306 *See* Line Items 3.A. through 3.C. of Part I of proposed Form SCIR.

307 *See* Line Item 3.A. of Part I of proposed Form SCIR.

308 *See* Line Item 3.B. of Part I of proposed Form SCIR.

309 *See* Line Item 3.C. of Part I of proposed Form SCIR.

310 *See* Instruction B.5.b. of proposed Form SCIR. *See also* paragraph (a)(10) of proposed Rule 10 (defining the term "significant cybersecurity incident").

311 See paragraph (c)(2)(ii)(C) of proposed Rule 10. *See* section II.B.2.a. of this release (discussing the notification requirements in more detail).

policies and procedures to address cybersecurity are effective.[312] If an internal investigation is conducted, the Covered Entity also would need to provide the date the investigation was closed. As discussed above, the closure of an internal investigation pertaining to the significant cybersecurity incident triggers the requirement to file an amended Part I of Form SCIR under proposed Rule 10.[313]

Line Item 5 of Part I of proposed Form SCIR would require the Covered Entity to indicate whether a law enforcement or government agency (other than the Commission) had been notified of the significant cybersecurity incident.[314] If so, the Covered Entity would need to identify each law enforcement or government agency. The Commission and Commission staff could use this information to coordinate with other law enforcement and government agencies if needed both to assess the incident and to share information as appropriate to understand the impact of the incident better.

Line Item 6 of Part I of proposed Form SCIR would require the Covered Entity to describe the nature and scope of the significant cybersecurity incident, including the information systems affected by the incident and any effect on the Covered Entity's critical operations.[315] This item would enable the Commission to obtain information about the incident to understand better how it is impacting the Covered Entity's operating status and whether the Covered Entity can continue to provide services to its customers, counterparties, members, registrants, or users. This would include understanding which services and systems have been impacted and whether the incident was the result of a cybersecurity incident that occurred at a service provider.

Line Item 7 of Part I of proposed Form SCIR would require the Covered Entity to indicate whether the threat actor(s) causing the significant cybersecurity incident has been

---

312 *See* Instruction A.5.d. of proposed Form SCIR.

313 *See* paragraph (c)(2)(ii)(D) of proposed Rule 10. *See also* section II.B.2.a. of this release (discussing the notification requirement in more detail).

314 *See* Line Item 5 of Part I of proposed Form SCIR.

315 *See* Line Item 6 of Part I of proposed Form SCIR.

identified.[316] If so, the Covered Entity would be required to identify the threat actor(s). In addition, the Covered Entity would need to indicate in Line Item 7 whether there has been communication(s) from or with the threat actor(s) that caused or claims to have caused the significant cyber security incident.[317] The Covered Entity would need to answer the question even if the threat actor(s) has not been identified. If there had been communications, the Covered Entity would need to describe them. This information would help the Commission staff to assess whether the same threat actor(s) had sought to access information systems of other Commission registrants and to warn other registrants (as appropriate) about the threat posed by the actor(s). It also could help in developing measures to protect against the risk to Commission registrants posed by the threat actor. In addition, the information would help the Commission assess the impact on the Covered Entity experiencing the significant cybersecurity incident to the extent other Commission registrants has been attacked by the same threat actor(s) using similar tactics, techniques, and procedures.

Line Item 8 of Part I of proposed Form SCIR would require the Covered Entity to describe the actions taken or planned to respond to and recover from the significant cybersecurity incident.[318] The objective is to obtain information to assess the Covered Entity's operating status, including its critical operations. This information also could assist the Commission and Commission staff in considering if the response measures are effective or ineffective in addressing the Covered Entity's significant cybersecurity incident.

Line Item 9 of Part I of proposed Form SCIR would require the Covered Entity to indicate whether any data was stolen, altered, or accessed or used for any other unauthorized purpose.[319] The Covered Entity would have the option of checking yes, no, or unknown. If yes,

---

316 *See* Line Item 7.A. of Part I of proposed Form SCIR.

317 *See* Line Item 7.B. of Part I of proposed Form SCIR.

318 *See* Line Item 8 of Part I of proposed Form SCIR.

319 *See* Line Item 9 of Part I of proposed Form SCIR.

the Covered Entity would need to describe the nature and scope of the data. This information would help the Commission and its staff understand the potential harm to the Covered Entity and its customers, counterparties, members, registrants, or users that could result from the compromise of the data. It also would provide insight into how the significant cybersecurity incident could impact other Market Entities.

Line Item 10 of Part I of proposed Form SCIR would require the Covered Entity to indicate whether any personal information was lost, stolen, modified, deleted, destroyed, or accessed without authorization as a result of the significant cybersecurity incident.[320] The Covered Entity would have the option of checking yes, no, or unknown. If yes, the Covered Entity would need to describe the nature and scope of the information. Additionally, if the Covered Entity answered yes, it would need to indicate whether notification has been provided to persons whose personal information was lost, stolen, damaged, or accessed without authorization.[321] If the answer is no, the Covered Entity would need to indicate whether this notification is planned.[322] For the purposes of proposed Form SCIR, the term "personal information" would have the same meaning as that term is defined in proposed Rule 10.[323] The compromise of personal information can have severe consequences on the persons to whom the information relates. For example, it potentially can be used to steal their identities or access their accounts at financial institutions to steal assets held in those accounts. Consequently, this information would help the Commission assess the extent to which the significant cybersecurity

---

320 *See* Line Item 10.A. of Part I of proposed Form SCIR.

321 *See* Line Item 10.B.i. of Part I of proposed Form SCIR.

322 *See* Line Item 10.B.ii. of Part I of proposed Form SCIR.

323 *See* Instruction A.5.e. of proposed Form SCIR. *See also* paragraph (a)(9) of proposed Rule 10 (defining "personal information" to mean any information that can be used, alone or in conjunction with any other information, to identify a person, such as name, date of birth, place of birth, telephone number, street address, mother's maiden name, government passport number, Social Security number, driver's license number, electronic mail address, account number, account password, biometric records, or other non-public authentication information).

incident has created this risk and the potential harm that could result from the compromise of personal data.

Line Item 11 of Part I of proposed Form SCIR would require the Covered Entity to indicate whether any of its assets were lost or stolen as a result of the significant cybersecurity incident.[324] The Covered Entity would have the option of checking yes, no, or unknown. If yes, the Covered Entity would need to describe the types of assets that were lost or stolen and include an approximate estimate of their value, if known. This question is not limited to particular types of assets and, therefore, the Covered Entity would need to respond affirmatively if, among other types of assets, financial assets such as cash and securities were lost or stolen or intellectual property was lost or stolen. The loss or theft of the Covered Entity's assets could potentially cause the entity to fail financially or put a strain on its liquidity. Further, to the extent counterparties become aware of the loss or theft, it could cause them to withdraw assets from the entity or stop transacting with the entity further straining its financial condition. Consequently, the objective is to understand whether the significant cybersecurity incident has created this risk and whether there may be other spillover effects or consequences to the U.S. securities markets.

Line Item 12 of Part I of proposed Form SCIR would require the Covered Entity to indicate whether any assets of the Covered Entity's customers, counterparties, clients, members, registrants, or users were lost or stolen as a result of the significant cybersecurity incident.[325] The Covered Entity would have the option of checking yes, no, or unknown. If yes, the Covered Entity would need to describe the types of assets that were lost or stolen and include an approximate estimate of their value, if known. Additionally, if the Covered Entity answered yes, it would need to indicate whether notification has been provided to persons whose assets were

---

[324] *See* Line Item 11 of Part I of proposed Form SCIR.

[325] *See* Line Item 12.A. Part I of proposed Form SCIR.

lost or stolen.[326] If the answer is no, the Covered Entity would need to indicate whether this notification is planned.[327]

Certain types of Covered Entities hold assets belonging to other persons or maintain ownership records of the assets of other persons.[328] For example, certain broker-dealers maintain custody of securities and cash for other persons and clearing agencies hold clearing deposits of their members. A significant cybersecurity incident impacting a Covered Entity that results in the loss or theft of assets can cause severe financial hardship to the owners of those assets. It also can impact the financial condition of the Covered Entity if it is liable for the loss or theft. Consequently, the objective is to understand whether the significant cybersecurity incident has created this risk.

As discussed in more detail below, proposed Rule 10 would require a Covered Entity to make a public disclosure that generally describes each significant cybersecurity incident that has occurred during the current or previous calendar year and promptly update this disclosure after the occurrence of a new significant cybersecurity incident or when information about a previously disclosed significant cybersecurity incident materially changes.[329] The Covered Entity would be required to make the disclosure on the Covered Entity's business Internet website and by filing Part II of proposed Form SCIR through the EDGAR system.[330] In addition, if the Covered Entity is a carrying or introducing broker-dealer, it would need to make the disclosure to its customers using the same means that a customer elects to receive account statements.[331]

---

326 *See* Line Item 11.B.i. of Part I of proposed Form SCIR.

327 *See* Line Item 12.B.ii. of Part I of proposed Form SCIR.

328 *See* Section I.A.2. of this release (discussing the functions of Market Entities).

329 *See* paragraph (d)(1)(ii) of proposed Rule 10. *See also* sections II.B.3. and II.B.4. of this release (discussing these proposed disclosure requirements in more detail).

330 *See* paragraphs (d)(2)(i) and (ii) of proposed Rule 10.

331 *See* paragraph (d)(3) of proposed Rule 10. *See* section II.B.3.b. of this release (discussing the broker-dealer disclosure requirement in more detail).

Line Item 13 of Part I of proposed Form SCIR would require the Covered Entity to indicate whether the significant cybersecurity incident has been disclosed pursuant to the requirements of proposed Rule 10.[332] The Covered Entity also would need to indicate whether it made the required disclosures of Part II of proposed Form SCIR on its website and through EDGAR and, if it had made the disclosure, it would need to indicate the date of the disclosure.[333] A Covered Entity that is a carrying or introducing broker-dealer would need to indicate separately whether it made the required disclosure of Part II of proposed Form SCIR to its customers.[334] The Covered Entity would not need to indicate a date for the customer disclosure because it could be made in a number of ways (*e.g.*, by email or mail) and that process could span a number of days. If the Covered Entity has not disclosed the significant cybersecurity incident as required by proposed Rule 10, it would need to explain why. The requirement to report this information is designed to promote compliance with the disclosure requirements of proposed Rule 10.

Line Item 14 of Part I of proposed Form SCIR would elicit information about any insurance coverage the Covered Entity may have with respect to the significant cybersecurity incident.[335] First, the Covered Entity would need to indicate whether the significant cybersecurity incident is covered by an insurance policy of the Covered Entity.[336] The Covered Entity would have the option of checking yes, no, or unknown. If yes, the Covered Entity would need to indicate whether the insurance company has been contacted. The existence of insurance coverage to cover losses could be relevant to Commission staff in assessing the potential magnitude of harm to the Covered Entity's customers, counterparties, members, registrants, or

---

332 *See* Line Items 13.A. through C. of proposed Form SCIR.

333 *See* Line Items 13.A. through B. of proposed Part I of Form SCIR.

334 *See* Line Item 13.C. of Part I of proposed Form SCIR.

335 *See* Line Items 14.A. and B. of Part I of proposed Form SCIR.

336 *See* Line Item 14.A. of Part I of proposed Form SCIR.

users and to the Covered Entity's financial condition. For example, the existence of insurance coverage, to the extent the significant cybersecurity incident is covered by the policy, could indicate a greater possibility that the Covered Entity and/or any of its customers, counterparties, members, registrants, or users affected by the incident are made whole.

Finally, Line Item 15 of Part I of proposed Form SCIR would permit the Covered Entity to include in the form any additional information the entity would want the Commission and Commission staff to know as well as provide any comments about the information included in the report.[337]

c. Request for Comment

The Commission requests comment on all aspects of the proposed requirements to report significant cybersecurity incidents on Part I of proposed Form SCIR. In addition, the Commission is requesting comment on the following specific aspects of the proposals:

41. Should paragraph (c)(1) of proposed Rule 10 be modified to revise the immediate notification requirement? For example, should the requirement permit the notice to be made by telephone or email? If so, explain why. If not, explain why not. If telephone or email notice is permitted, should the rule specify the Commission staff, Division, or Office to phone or email?

42. Should paragraph (c)(1) of proposed Rule 10 be modified to revise the requirement to provide immediate written electronic notice to specify how the notice must be transmitted to the Commission? For example, should the rule specify an email address or other type of electronic portal to be used to transmit the notice? If so, explain why. If not, explain why not. Should the rule be modified to require that the notice be transmitted to the Commission through the EDGAR system? If so, explain why. If not, explain why not. Should the rule be

---

[337] *See* Line Item 15 of proposed Part I of Form SCIR.

modified to require that the notice be transmitted to the Commission through the EDGAR system using a structured data language other than custom XML format?

43. Should paragraph (c)(1) of proposed Rule 10 be modified to revise the requirement to provide immediate written electronic notice to require the notice to be provided within a specific timeframe such as on the same day the requirement was triggered or within 24 hours? If so, explain why. If not, explain why not.

44. Should paragraph (c)(1) of proposed Rule 10 be modified to revise the trigger for the immediate notification and reporting requirements? If so, explain why. If not, explain why not. For example, should the trigger be when the Covered Entity "detects" a significant cybersecurity incident (rather than when it has a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring)? If so, explain why. If not, explain why not. For example, would a detection standard be a less subjective standard? If so, explain why. If not, explain why not. Is there another trigger standard that would be more appropriate? If so, identify it and explain why it would be more appropriate.

45. If the immediate notification requirement of paragraph (c)(1) is adopted as proposed, it is anticipated that a dedicated email address would be established to receive these notices. Are there other methods the Commission should use for receiving these notices? If so, identity them and explain why they would be more appropriate than email. For example, should the notices be received through the EDGAR system? If so, explain why. If not, explain why not.

46. Should paragraph (c)(2) of proposed Rule 10 be modified to revise the reporting requirements to incorporate the cybersecurity reporting program that CISA will implement under recently adopted legislation ("CISA Reporting Program") to the

extent it will be applicable to Covered Entities?[338] If so, explain why and suggest modifications to the proposed reporting requirements for Covered Entities to incorporate the CISA Reporting Program. For example, if a Covered Entity would be required to file a report under the CISA Reporting Program, should that report satisfy the obligations to report to the Commission a significant cybersecurity incident under paragraph (c) of proposed Rule 10? If so, explain why. If not, explain why not.

47. Should paragraph (c)(2) of proposed Rule 10 be modified to revise the timeframe for filing an initial Part I of proposed Form SCIR? If so, explain why. If not, explain why not. For example, should the reporting requirements be revised to permit Covered Entities more than 48 hours to file an initial Part I of proposed Form SCIR with the Commission? If yes, explain how long they should have to file the initial Part I of proposed Form SCIR and why that timeframe would be appropriate. For example, should Covered Entities have 72 or 96 hours to file the initial Part I of proposed Form SCIR? If so, explain why. If not, explain why not. Would providing more time to file the initial Part I of proposed Form SCIR make the filing more useful insomuch as the Covered Entity would have more time to investigate the significant cybersecurity incident? If so, explain why and how to balance that benefit against the delay in providing this information to the Commission within 48 hours. Would the immediate notification requirement of paragraph (c) of proposed Rule 10 make it appropriate to lengthen the timeframe for when the Covered Entity would need to file the initial Part I of proposed Form SCIR? If so, explain why. If not, explain why not. For example, could the immediate notification requirement and the ability of the Commission staff to

---

338 *See* CIRCIA.

follow-up with the contact person identified on the notification serve as an appropriate alternative to receiving the initial Part I of proposed Form SCIR within 48 hours. If so, explain why. If not, explain why not. Conversely, should the timeframe for filing an initial Part I of proposed Form SCIR be shortened to 24 hours or some other period of time that is less than 48 hours? If so, explain why. If not, explain why not.

48. Should paragraph (c)(2) of proposed Rule 10 be modified to revise the timeframe for filing an initial or amended Part I of proposed Form SCIR so the timeframes are expressed in business days or calendar days instead of hours? If so, explain why. If not, explain why not. For example, should Covered Entities have two, five, or some other number business or calendar days to file an initial or amended Part I of proposed Form SCIR? Would business or calendar days be more appropriate given that Part I of proposed Form SCIR would be filed through the EDGAR system?[339] If so, explain why. If not, explain why not.

49. Should paragraph (c)(2) of proposed Rule 10 be modified to revise the timeframe for filing an initial or amended Part I of proposed Form SCIR so that it must be filed promptly after the filing requirement is triggered without specifying the 48 hour limit? If so, explain why and describe how "promptly" should be interpreted for purposes of the reporting requirements of paragraph (c) of proposed Rule 10. If not, explain why not.

---

339 The Commission accepts electronic submissions through the EDGAR system Monday through Friday, except federal holidays, from 6:00am to 10:00pm Eastern Time. *See* Chapter 2 of the EDGAR Filer Manual (Volume I), version 41 (Dec. 2022). Further, filings submitted by direct transmission commencing on or before 5:30 p.m. Eastern Standard Time or Eastern Daylight Saving Time, whichever is currently in effect, shall be deemed filed on the same business day, and all filings submitted by direct transmission commencing after 5:30 p.m. Eastern Standard Time or Eastern Daylight Saving Time, whichever is currently in effect, shall be deemed filed as of the next business day. 17 CFR 232.13.

50. Should paragraph (c)(2) of proposed Rule 10 be modified to revise the reporting requirements to include the filing of an initial Part I of proposed Form SCIR and a final Part I of proposed Form SCIR but not require the filing of interim amended forms? If so, explain why. If not, explain why not. For example, could informal communications between the Commission staff and the Covered Entity facilitated by the contact employee identified in the immediate notice that would be required under paragraph (c)(1) of proposed Rule 10 be an appropriate alternative to requiring the filing of interim amended forms? If so, explain why. If not, explain why not.

51. Should paragraph (c)(2) of proposed Rule 10 be modified to revise the reporting requirements to include the filing of interim amended forms on a pre-set schedule? If so, explain why. If not, explain why not. For example, should Covered Entities be required to file an initial Part I of proposed Form SCIR and a final Part I of proposed Form SCIR pursuant to the requirements of paragraph (c) of proposed Rule 10 but file interim amended forms on a pre-set schedule? If so, explain why this would be appropriate, including why a pre-set reporting requirement would not undermine the objectives of the proposed reporting requirements, and how often the interim reporting should be required (*e.g.*, weekly, bi-weekly, monthly, quarterly). Would a pre-set reporting cadence (*e.g.*, weekly, bi-weekly, monthly, quarterly) undermine the objectives of the proposed reporting requirements by inappropriately delaying the Commission's receipt of important information about a significant cybersecurity incident? If so, explain why. If not, explain why not. Would the immediate notification requirement and the ability of the Commission staff to follow-up with the contact person identified on the notification mitigate this potential consequence? If so, explain why. If not, explain why not.

52. Should paragraph (c)(2)(ii)(D) of proposed Rule 10 and Part I of proposed Form SCIR be modified to revise the reporting requirements relating to internal investigations? If so, explain why. If not, explain why not. For example, would these reporting requirements create a disincentive for Covered Entities to perform internal investigations in response to significant cybersecurity incidents? If so, explain why. If not, explain why not.

53. Should Part I of proposed Form SCIR be modified? If so, explain why. If not, explain why not. For example, does the form strike an appropriate balance of providing enough detail to the Commission to be helpful while also not being unduly burdensome to Covered Entities? If so, explain why. If not, explain why not. Is certain information that would be elicited in Part I of Form SCIR unnecessary? If so, identify the information and explain why it would be unnecessary. Is there additional information that should be required to be included in Part I of proposed Form SCIR? If so, identify the information and explain why it would be appropriate to require a Covered Entity to report it in the form.

54. Should Part I of proposed Form SCIR be modified to require that Covered Entities provide a UIC—such as an LEI[340] (which would require each Covered Entity without a UIC (such as an LEI) to obtain one to comply with the rule)? If so, explain why. If not, explain why not. For example, would a requirement to provide a UIC allow the Commission staff to better evaluate cyber-threats to Covered Entities? If so, explain why. If not, explain why not. Should the form be modified to require Covered Entities to provide another type of standard

---

[340] The Commission approved a UIC (namely, the LEI) in a previous rulemaking. *See* section II.B.2.b. of this release; *see also Regulation SBSR Release*, 80 FR at 14632. The Commission is aware that additional identifiers could be recognized as UICs in the future, but for the purposes of this release, the Commission is equating the UIC with the LEI.

identifier other than a CIK number and UIC (if they have a UIC)? If so, explain why. If not, explain why not.

3. Disclosure of Cybersecurity Risks and Incidents

a. Cybersecurity Risks and Incidents Disclosure

Proposed Rule 10 would require a Covered Entity to make two types of public disclosures relating to cybersecurity on Part II of proposed Form SCIR.[341] First, the Covered Entity would need to, in plain English, provide a summary description of the cybersecurity risks that could materially affect its business and operations and how the Covered Entity assesses, prioritizes, and addresses those cybersecurity risks.[342] A cybersecurity risk would be material to a Covered Entity if there is a substantial likelihood that a reasonable person would consider the information important based on the total mix of facts and information.[343] The facts and circumstances relevant to determining materiality in this context may include, among other things, the likelihood and extent to which the cybersecurity risk or resulting incident: (1) could disrupt or degrade the Covered Entity's ability to maintain critical operations; (2) could adversely affect the confidentiality, integrity, or availability of information residing on the Covered Entity's information systems, including whether the information is personal, confidential, or proprietary information; and/or (3) could harm the Covered Entity or its customers, counterparties, members, registrants, users, or other persons.

The second element of the disclosure would be a summary description of each significant cybersecurity incident that occurred during the current or previous calendar year, if applicable.[344] The look-back period of the current and previous calendar years is designed to make the

---

341 *See* paragraph (d)(1) of proposed Rule 10.

342 *See* paragraph (d)(1)(i) of proposed Rule 10; Line Item 2 of Part II proposed of Form SCIR.

343 *See, e.g.*, *S.E.C. v. Steadman*, 967 F.2d 636, 643 (D.C. Cir. 1992); *cf. Basic Inc. v. Levinson*, 485 U.S. 224, 231-232 (1988); *TSC Industries v. Northway, Inc.*, 426 U.S. 438, 445, 449 (1976).

344 *See* paragraph (d)(1)(ii) of proposed Rule 10; Line Item 3 of Part II proposed of Form SCIR. *See also* paragraph (a)(10) of proposed Rule 10 (defining the term "significant cybersecurity incident").

disclosure period consistent across all Covered Entities. The look-back period also is designed to provide a short history of significant cybersecurity incidents affecting the Covered Entity while not overburdening the firm with a longer disclosure period. The summary description of each significant cybersecurity incident would need to include: (1) the person or persons affected;[345] (2) the date the incident was discovered and whether it is ongoing; (3) whether any data was stolen, altered, or accessed or used for any other unauthorized purpose; (4) the effect of the incident on the Covered Entity's operations; and (5) whether the Covered Entity, or service provider, has remediated or is currently remediating the incident.[346] This disclosure—because it addresses actual significant cybersecurity incidents—would serve as another way for market participants to evaluate the Covered Entity's cybersecurity risks and vulnerabilities apart from the general disclosure of its cybersecurity risk. For example, a Covered Entity's disclosure of multiple significant cybersecurity incidents during the current or previous calendar year (particularly, if they did not impact other Covered Entities) would be useful in assessing whether the Covered Entity is adequately addressing cybersecurity risk or is more vulnerable to that risk as compared with other Covered Entities.

The objective of these disclosures is to provide greater transparency to customers, counterparties, registrants, or members of the Covered Entity, or to users of its services, about the Covered Entity's exposure to material harm as a result of a cybersecurity incident, which, in turn, could cause harm to customers, counterparties, members, registrants, or users. This information could be used by these persons to manage their own cybersecurity risk and, to the extent they have choice, select a Covered Entity with which to transact or otherwise conduct

---

345 This element of the disclosure would not need to include the identities of the persons affected or personal information about those persons. Instead, the disclosure could use generic terms to identify the person or persons affected. For example, the disclosure could state that "customers of the broker-dealer," "counterparties of the SBSD," or "members of the SRO" are affected (as applicable).

346 *See* paragraphs (d)(1)(ii)(A) through (E) of proposed Rule 10; Line Item 3 of Part II proposed of Form SCIR.

business. Information about prior attacks and their degree of success is immensely valuable in mounting effective countermeasures.[347]

However, the intent of the disclosure on Part II of proposed Form SCIR is to avoid overly detailed disclosures that could increase cybersecurity risk for the Covered Entity and other persons. Revealing too much information could assist future attackers as well as lead to loss of customers, reputational harm, litigation, or regulatory scrutiny, which would be a cost associated with public disclosure.[348] Therefore, under proposed Rule 10, the Covered Entity would be required to provide only a summary description of its cybersecurity risk and significant cybersecurity incidents.[349] The requirement that the disclosures contain summary descriptions only is designed to produce meaningful disclosures but not disclosures that would reveal information (*e.g.*, proprietary or confidential methods of addressing cybersecurity risk or known cybersecurity vulnerabilities) that could be used by threat actors to cause harm to the Covered Entity or its customers, counterparties, members, users, or other persons. This requirement is also designed to produce high-level disclosures about the Covered Entity's cybersecurity risks and significant cybersecurity incidents that can be easily reviewed by interested parties in order to give them a general understanding of the Covered Entity's risk profile.

b. Disclosure Methods and Updates

Proposed Rule 10 would require a Covered Entity to make the public disclosures discussed above (*i.e.*, the information about cybersecurity risks and significant cybersecurity incidents) on Part II of proposed Form SCIR.[350] Part II of proposed Form SCIR would elicit

---

347 *See* Peter W. Singer and Allan Friedman. Cybersecurity and Cyberwar: What Everyone Needs to Know. *Oxford University Press* 222 (2014).

348 *See, e.g., Federal Trade Commission v. Equifax, Inc*., FTC Matter/File Number: 172 3203, Civil Action Number: 1:19-cv-03297-TWT (2019), *available at* https://www.ftc.gov/enforcement/cases-proceedings/172-3203/equifax-inc ("FTC Equifax Civil Action").

349 *See* paragraphs (d)(1)(i) and (ii) of proposed Rule 10.

350 *See* paragraph (d) of proposed Rule 10.

information about the Covered Entity that would be used to identify the filer.[351] In particular, the Covered Entity would need to provide its full legal name and business name (if different from its legal name), UIC (if the filer has a UIC),[352] CIK number, and main address.[353] The Covered Entity also would need to indicate the type of Market Entity it is by checking the appropriate box or boxes.[354] For example, if the Covered Entity is dually registered as a broker-dealer and SBSD, it would need to check the box for each of those entity types.

Page 1 of Part II of proposed Form SCIR also would contain fields for the individual executing the form to sign and date the form. By signing the form, the individual would: (1) certify that the form was executed on behalf of, and with the authority of, the Covered Entity; and (2) represent individually, and on behalf of the Covered Entity, that the information and statements contained in the form are current, true and complete. The form of the certification is designed to ensure that the Covered Entity, through the individual executing the form, discloses information that can be used by the Covered Entity's customers, counterparties, members, registrants, or users, or by other interested persons to assess the Covered Entity's cybersecurity risk profile and compare it with the risk profiles of other Covered Entities.

As discussed above, proposed Rule 10 would require the Covered Entity to publicly disclose a summary description of the cybersecurity risks that could materially affect the Covered Entity's business and operations and how the Covered Entity assesses, prioritizes, and addresses those cybersecurity risks.[355] Line Item 2 of Part II of proposed Form SCIR would

---

351 *See* Line Items 1.A. through 1.D. of Part II of proposed Form SCIR.

352 As mentioned previously, the Commission approved a UIC—namely, the LEI—in a prior rulemaking. *See* section II.B.2.b. of this release. Therefore, for the purposes of this release, the Commission is proposing to require those Covered Entities that already have LEIs to identify themselves with LEIs on Part II of Form SCIR.

353 *See* Line Items 1.A. through 1.C. of Part I of proposed Form SCIR. *See also* section II.B.2.b. of this release (discussing UIC and CIK numbers in more detail with respect to Part I of proposed Form SCIR).

354 *See* Line Item 1.D. of Part II of proposed Form SCIR (setting forth check boxes to indicate whether the Covered Entity is a broker-dealer, clearing agency, MSBSP, the MRSB, a national securities association, a national securities exchange, SBSD, SBSDR, or transfer agent).

355 *See* paragraph (d)(1)(i) of proposed Rule 10.

contain a narrative field in which the Covered Entity would provide this summary description.[356] In order to provide context to the meaning of the disclosure, the beginning of Line Item 2 would set forth the definition of "cybersecurity risk" in proposed Rule 10 as well as the definitions of "cybersecurity incident," "cybersecurity threat," and "cybersecurity vulnerability" because these three terms are used in the definition of "cybersecurity risk."[357]

Line Item 3 of Part II of proposed Form SCIR would be used to make the disclosure about each significant cybersecurity incident that occurred during the current and previous calendar year.[358] The definition of "significant cybersecurity incident" would be set forth at beginning of Line Item 3 in order to provide context to the meaning of the disclosure. To complete the line item, the Covered Entity first would need to indicate by checking "yes" or "no" whether it had experienced one or more significant cybersecurity incidents during the current or previous calendar year. If the answer is yes, the Covered Entity would need to provide in a narrative field on Line Item 3 the summary description of each significant cybersecurity incident.[359]

As discussed next, there would be two methods of making the disclosure, which would be required of all Covered Entities under proposed Rule 10, and an additional third method that would be required of Covered Entities that are carrying or introducing broker-dealers. First, Covered Entities would be required to file Part II of Form SCIR with the Commission electronically through the EDGAR system in accordance with the EDGAR Filer Manual, as defined in Rule 11 of Regulation S-T,[360] and in accordance with the requirements of Regulation

---

356 *See* Line Item 2 of Part II of proposed Form SCIR.

357 *Id. See also* paragraphs (a)(2) through (5) of proposed Rule 10 (defining, respectively, "cybersecurity incident," "cybersecurity risk," "cybersecurity threat," and "cybersecurity vulnerability").

358 *See* Line Item 3 of Part II of proposed Form SCIR.

359 *See* paragraph (d)(1)(ii) of proposed Rule 10.

360 *See* 17 CFR 232.11.

S-T.[361] The Commission would make these filings available to the public. The objective of requiring centralized EDGAR-filing of Part II of proposed Form SCIR is to facilitate the ability to compare disclosures across different Covered Entities or categories of Covered Entities in the same manner that EDGAR filing facilitates comparison of financial statements, annual reports, and other disclosures across Commission registrants. By creating a single location for all of the disclosures, Commission staff, investors, market participants, and analysts as well as Covered Entities' customers, counterparties, members, registrants, or users would be able to run search queries to compare the disclosures of multiple Covered Entities. Centralized EDGAR filing could make it easier for Commission staff and others to assess the cybersecurity risk profiles of different types of Covered Entities and could facilitate trend analysis of significant cybersecurity incidents. Thus, by providing a central location for the cybersecurity disclosures, filing Part II of proposed Form SCIR through EDGAR could lead to greater transparency of the cybersecurity risks in the U.S. securities markets.

Second, proposed Rule 10 would require the Covered Entity to post a copy of the Part II of proposed Form SCIR most recently filed on EDGAR on an easily accessible portion of its business Internet website that can be viewed by the public without the need of entering a password or making any type of payment or providing any other consideration.[362] Consequently, the disclosures could not be located behind a "paywall" or otherwise require a person to pay a registration fee or provide any other consideration to access them. The purpose of requiring the form to be posted on the Covered Entity's business Internet website is that individuals naturally

---

361 *See* paragraph (d)(2)(i) of proposed Rule 10.

362 *See* paragraph (d)(2)(ii) of proposed Rule 10. In addition to the disclosure to be made available to security-based swap counterparties as required by paragraph (d)(2)(ii) of proposed Rule 10, current Commission rules require that SBS Entities' trading relationship documentation between certain counterparties address cybersecurity. Specifically, an SBS Entity's trading relationship documentation must include valuation methodologies for purposes of complying with specified risk management requirements, which would include the risk management requirements of proposed Rule 10 (if it is adopted). *See* 17 CFR 250.15Fi-5(b)(4). This documentation would include a dispute resolution process or alternative methods for determining value in the event of a relevant cybersecurity incident. *See also* section IV.C.1.b.iii. of this release (discussing disclosure requirements of Rule 15Fh-3(b)).

may visit a company's business Internet website when seeking timely and updated information about the company, particularly if the company is experiencing an incident that disrupts or degrades the services it provides. Therefore, requiring the form to be posted on the website is designed to make it available through this commonly used method of obtaining information. Additionally, individuals may naturally visit a company's business Internet website as part of their due diligence process in determining whether to use its services. Therefore, posting the form on the Covered Entity's business Internet website could provide individuals with information about the Covered Entity's cybersecurity risks before they elect to enter into an arrangement with the firm. It could serve a similar purpose for individuals considering whether to maintain an ongoing business relationship with the Covered Entity.

In addition to those two disclosure methods, a Covered Entity that is either a carrying or introducing broker-dealer would be required to provide a copy of the Part II of proposed Form SCIR most recently filed on EDGAR to a customer as part of the account opening process.[363] Thereafter, the Covered Entity would need to provide the customer with the most recently posted form annually and when it is updated. The broker-dealer would need to deliver the form using the same means that the customer elects to receive account statements (*e.g.*, by email or through the postal service).[364] This additional method of disclosure is designed to make the information readily available to the broker-dealer's customers (many of whom may be retail investors) through the same processes that other important information (*i.e.*, information about their securities accounts) is communicated to them. Requiring a broker-dealer to deliver copies of the

---

363 *See* paragraph (d)(3) of proposed Rule 10.

364 If the disclosure requirements of proposed Rule 10 are adopted, the Commission would establish a compliance date by which a Covered Entity would need to make its first public disclosure on Part II of proposed Form SCIR. At a minimum, the initial disclosure would need to include a summary description of the cybersecurity risks that could materially affect the Covered Entity's business and operations and how the Covered Entity assesses, prioritizes, and addresses those cybersecurity risks. In setting an initial compliance date, the Commission could take a bifurcated approach in which each method of disclosure has a different compliance date. For example, the compliance date for making the website disclosure could come before the compliance date for making the EDGAR disclosure and the additional disclosure required of carrying and introducing broker-dealers. The Commission seeks comment below on a potential compliance date or compliance dates for the disclosure requirements.

form is designed to enhance investor protection by enabling customers to take protective or remedial measures to the extent appropriate. It would also assist customers in determining whether their engagement of that particular broker-dealer remains appropriate and consistent with their investment objectives.

Finally, a Covered Entity would be required to file on EDGAR an updated Part II of proposed Form SCIR promptly if the information required to be disclosed about cybersecurity risks or significant cybersecurity incidents materially changes, including, in the case of the disclosure about significant cybersecurity incidents, after the occurrence of a new significant cybersecurity incident or when information about a previously disclosed significant cybersecurity incident materially changes.[365] The Covered Entity also would need to post a copy of the updated Part II of proposed Form SCIR promptly on its business Internet website and, if it is a carrying broker-dealer or introducing broker-dealer, deliver copies of the form to its customers. Given the potential effect that significant cybersecurity incidents could have on a Covered Entity's customers, counterparties, members, registrants, or users—such as exposing their personal or other confidential information or resulting in a loss of cash or securities from their accounts—time is of the essence, and requiring a Covered Entity to update the disclosures promptly would enhance investor protection by enabling customers, counterparties, members, registrants, or users to take proactive or remedial measures to the extent appropriate.

---

[365] *See* paragraph (d)(4) of proposed Rule 10. *See also* Instruction C.2. of proposed Form SCIR. As discussed earlier, a Covered Entity would be required to file Part I of proposed Form SCIR with the Commission promptly, but no later than 48 hours, upon having a reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring. *See* paragraph (c)(2)(i) of proposed Rule 10; *see also* section II.B.2.a. of this release (discussing this requirement in more detail). Therefore, the Covered Entity would need to file a Part I and an updated Part II of proposed Form SCIR with the Commission relatively contemporaneously. Depending on the facts and circumstances, the Part I and updated Part II could be filed at the same time or one could proceed the other if the Covered Entity, for example, has the information to complete Part II first but needs more time to gather the information to complete Part I (which elicits substantially more information than Part II). However, as discussed above, Part I must be filed no later than 48 hours after the Covered Entity has a reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring and the Covered Entity must include in the initial filing the information that is known at that time and file an updated Part I as more information becomes known to the Covered Entity.

Accordingly, the timing of the filing of an updated disclosure should take into account the exigent nature of significant cybersecurity incidents which would generally militate toward swiftly filing the update. Furthermore, requiring Covered Entities to update their disclosures following the occurrence of a new significant cybersecurity incident would assist market participants in determining whether their business relationship with that particular Covered Entity remains appropriate and consistent with their goals.

A Covered Entity also would need to file an updated Part II of proposed Form SCIR if the information in the summary description of a significant cybersecurity incident included on the form is no longer within the look-back period (*i.e.*, the current or previous calendar year). For example, the information that would need to be included in the summary description includes whether the significant cybersecurity incident is ongoing and whether the Covered Entity had remediated it. The Covered Entity would need to file an updated Part II of proposed Form SCIR if the significant cybersecurity incident was remediated and ended on a date that was beyond the look-back period. The updated Part II of proposed Form SCIR would no longer include a summary description of that specific significant cybersecurity incident. The objective is to focus the most recently filed disclosure on events within the relative near term. The history of the Covered Entity's significant cybersecurity incidents would be available in previous filings.

c. Request for Comment

The Commission requests comment on all aspects of the proposed disclosure requirements. In addition, the Commission is requesting comment on the following specific aspects of the proposals:

55. Should paragraph (d)(1)(i) of proposed Rule 10 be modified to revise the requirements that Covered Entities publicly disclose the cybersecurity risks that could materially affect their business and operations and to publicly disclose a description of how the Covered Entity assesses, prioritizes, and addresses those cybersecurity risks? If so, explain why. If not, explain why not. For example,

would the public disclosures required by paragraph (d)(1)(i) of proposed Rule 10 be useful or provide meaningful information to a Covered Entity's customers, counterparties, members, registrants, or users? If so, explain why. If not, explain why not. Could the proposed disclosure requirement be modified to make it more useful? If so, explain how. Could the public disclosures required by paragraph (d)(1)(i) of proposed Rule 10 assist threat actors in engaging in cyber crime? If so, explain why. If not, explain why not. Could the proposed disclosure requirements be modified to eliminate this risk without negatively impacting the usefulness of the disclosures? If so, explain how.

56. Should paragraph (d)(1)(ii) of proposed Rule 10 be modified to revise the requirements that Covered Entities publicly disclose information about each significant cybersecurity incident that has occurred during the current or previous calendar year? If so, explain why. If not, explain why not. For example, would the public disclosures required by paragraph (d)(1)(ii) of proposed Rule 10 be useful or provide meaningful information to a Covered Entity's customers, counterparties, members, registrants, or users? If so, explain why. If not, explain why not. Could the proposed disclosure requirement be modified to make it more useful? If so, explain how. Could the public disclosures required by paragraph (d)(1)(ii) of proposed Rule 10 assist threat actors in engaging in cyber crime? If so, explain why. If not, explain why not. Could the proposed disclosure requirements be modified to eliminate this risk without negatively impacting the usefulness of the disclosures? If so, explain how.

57. Should paragraph (d)(1)(ii) of proposed Rule 10 be modified to revise the required current and previous year look-back period for the disclosure of significant cybersecurity incidents? If so, explain why. If not, explain why not. For example, should the look-back period be a shorter period of time (*e.g.*, only

the current calendar year)? If so, explain why. If not, explain why not. Alternatively, should the look-back period be longer (*e.g.*, the current calendar year and previous two calendar years)? If so, explain why. If not, explain why not. Should the look-back period be expressed in months rather than calendar years? For example, should the look-back period be 12, 18, 24, 30, or 36 months? If so, explain why. If not, explain why not.

58. Should paragraph (d)(1)(ii) of proposed Rule 10 be modified to provide that the requirement to include a summary description of each significant cybersecurity incident that occurred during the current or previous calendar year in Part II of proposed Form SCIR be prospective and, therefore, limited to significant cybersecurity incidents that occur on or after the compliance date of the disclosure requirement? If so, explain why. If not, explain why not.

59. Should the public disclosure requirements of paragraphs (d)(1)(i) and (ii) of proposed Rule 10 be modified to require the disclosure of additional or different information? If so, identify the additional or different information and explain why it would be appropriate to require its public disclosure by Covered Entities.

60. Should 17 CFR 240.15Fh-3(b) be amended to specify that required counterparty disclosure includes the information that would be required by paragraph (d)(1) of proposed Rule 10 and publicly disclosed on Part II of proposed Form SCIR? If so, explain why. If not explain why not.

61. Should paragraph (d)(2) of proposed Rule 10 be modified to revise the methods of making the public disclosures? If so, explain why. If not, explain why not. For example, should Covered Entities be required to file Part II of proposed Form SCIR on EDGAR but not be required to post a copy of the form on their business Internet websites? If so, explain why. If not, explain why not. Would requiring the public cybersecurity disclosures to be filed in a centralized electronic system,

such as EDGAR, make it easier for investors, analysts, and others to access and gather information from the cybersecurity disclosures than if those disclosures were only posted on Covered Entity websites? Alternatively, should Covered Entities be required to post an executed copy of Part II of proposed Form SCIR on their business Internet websites but not be required to file the form on EDGAR? If so, explain why. If not, explain why not. Why or why not?

62. Should paragraph (d)(2) of proposed Rule 10 be modified to revise the requirement to post a copy of Part II of proposed Form SCIR on business Internet website of the Covered Entity to permit the Covered Entity to post a link to the EDGAR filing? If so, explain why. If not, explain why not.

63. Should paragraph (d)(3) of proposed Rule 10 be modified to revise the additional methods of making the public disclosures required of carrying and introducing broker-dealers? If so, explain why. If not, explain why not. For example, would filing Part II of proposed Form SCIR on EDGAR and posting a copy of the form on the Covered Entity's business Internet website be sufficient to meet the objectives of the disclosure requirements discussed above and, therefore, obviate the need for a carrying broker-dealer or introducing broker-dealer to additionally send copies of the form to customers? If so, explain why. If not, explain why not. Rather than requiring the broker-dealer or introducing broker-dealer to send a copy of the Part II of proposed Form SCIR most recently filed on EDGAR to each customer, would it be sufficient that the most recently filed form as of the end of each quarter or the calendar year be sent to the customers? If so, explain why. If not, explain why not.

64. Should paragraph (d)(3) of proposed Rule 10 be modified to permit the Covered Entity to send a website link to the EDGAR filing to customers instead of a copy of the EDGAR filing? If so, explain why. If not, explain why not.

65. Should paragraph (d)(3) of proposed Rule 10 be modified to require other types of Covered Entities to send a copy of the most recently filed Part II of proposed Form SCIR to their customers, counterparties, members, registrants, or users? If so, explain why. If not, explain why not. For example, should transfer agents be required to send the most recently filed Part II of proposed Form SCIR to their securityholders? If so, explain why. If not, explain why not.

66. Should paragraph (d)(4) of proposed Rule 10 be modified to revise the requirement that a Covered Entity must "promptly" provide an updated disclosure on Part II of proposed Form SCIR if the information on the previous disclosure materially changes to provide that the Commission shall allow registrants to delay publicly disclosing a significant cybersecurity incident where the Attorney General requests such a delay from the Commission based on the Attorney General's written determination that the delay is in the interest of national security?

67. Should paragraph (d)(4) of proposed Rule 10 be modified to revise the requirement that a Covered Entity must "promptly" provide an updated disclosure on Part II of proposed Form SCIR if the information on the previous disclosure materially changes to specify a timeframe within which the updated filing must be promptly made? If so, explain why. If not, explain why not. For example, should the rule be modified to require that the updated disclosure must be made within 24, 36, 48, or 60 hours of the information on the previous disclosure materially changing? If so, explain why. If not, explain why not. Should the timeframe for making the updated disclosure be expressed in business days? If so, explain why. If not, explain why not. For example, should the updated disclosure be required to be made within two, three, four, or five business days (or

some other number of days) of the information on the previous disclosure materially changing? If so, explain why. If not, explain why not.

68. Should paragraph (d)(4) of proposed Rule 10 be modified to revise the requirement that a Covered Entity must "promptly" provide an updated disclosure on Part II of proposed Form SCIR if the information on the previous disclosure materially changes to require the update to be made within 30 days (similar to the requirement for updating Form CRS)?[366] If so, explain why. If not, explain why not. For example, would this approach appropriately balance the objective of requiring timely disclosure with the objective of providing accurate and complete disclosure? If so, explain why. If not, explain why not.

69. Should paragraph (d)(4) of proposed Rule 10 be modified to revise the requirements that trigger when an updated Part II of proposed Form SCIR must be filed on EDGAR, posted on the Covered Entity's business Internet website, and, if applicable, sent to customers? If so, explain why. If not, explain why not. For example, should the rule require that an updated form must be publically disclosed through these methods on a quarterly, semi-annual, or annual basis if the information on the previously filed form has materially changed? If so, explain why. If not, explain why not.

70. Should Part II of proposed Form SCIR be modified to require that Covered Entities provide a UIC—such as an LEI (which would require Covered Entities without a UIC (such as an LEI) to obtain one to comply with the rule)?[367] If so, explain why. If not, explain why not. For example, would requiring Covered

---

366 *See* Form CRS Instructions, *available at* https://www.sec.gov/files/formcrs.pdf.

367 As mentioned previously in section II.B.2.b. of this release, the Commission approved a UIC (namely, the LEI) in a previous rulemaking. The Commission is aware that additional identifiers could be recognized as UICs in the future, but for the purposes of this release, the Commission is equating the UIC with the LEI.

Entities to provide a UIC better allow investors, analysts, and third-party data aggregators to evaluate the cyber security risk profiles of Covered Entities? If so, explain why. If not, explain why not. Should the form be modified to require Covered Entities to provide another type of standard identifier other than a CIK number and UIC (if they have a UIC)? If so, explain why. If not, explain why not.

71. If the disclosure requirements of proposed Rule 10 are adopted, what would be an appropriate compliance date for the disclosure requirements? For example, should the compliance date be three, six, nine, or twelve months after the effective date of the rule (or some other period of months)? Please suggest a compliance period and explain why it would be appropriate. Should the compliance date for the website disclosure be sooner than the compliance date for the EDGAR disclosure or vice versa? If so, explain why. If not, explain why not. Should the compliance date for the additional disclosure methods that would be required of carrying and introducing broker-dealers be different than the compliance dates for the website disclosure and the EDGAR disclosure? If so, explain why. If not, explain why not. If the requirement to provide a summary description of each significant cybersecurity incident that occurred during the current and previous calendar year is prospective (*i.e.*, does not apply to incidents that occurred before the compliance date), should the compliance period be shorter than if the requirement was retrospective, given that the initial disclosure, in most cases, would limited to a summary description of the cybersecurity risks that could materially affect the Covered Entity's business and operations and how the Covered Entity assesses, prioritizes, and addresses those cybersecurity risks? If so, explain why. If not, explain why not.

4. Filing Parts I and II of Proposed Form SCIR in EDGAR Using a Structured Data Language

a. Discussion

Proposed Rule 10 would require Covered Entities would file Parts I and II of proposed Form SCIR electronically with the Commission using the EDGAR system in accordance with the EDGAR Filer Manual, as defined in Rule 11 of Regulation S-T,[368] and in accordance with the requirements of Regulation S-T.[369] In addition, under the proposed requirements, Covered Entities would file Parts I and II of Form SCIR in a structured (*i.e.*, machine-readable) data language.[370] Specifically, Covered Entities would file Parts I and II of proposed Form SCIR in an eXtensible Markup Language ("XML")-based data language specific to the form ("custom XML," and in this release "SCIR-specific XML"). While the majority of filings through the EDGAR system are submitted in unstructured HTML or ASCII formats, certain EDGAR-system filings are submitted using custom XML languages that are each specific to the particular form being submitted.[371] For such filings, filers are typically provided the option to either submit the filing directly to the EDGAR system in the relevant custom XML data language, or to manually input the information into a fillable web-based form developed by the Commission that converts the completed form into a custom XML document.[372]

Requiring Covered Entities to file Parts I and II of proposed Form SCIR through the EDGAR system would allow the Commission to download Form SCIR information directly from a central location, thus facilitating efficient access, organization, and evaluation of the information contained in the forms. Use of the EDGAR system also would enable technical

---

368 *See* 17 CFR 232.11.

369 *See* paragraphs (c) and (d) of proposed Rule 10.

370 Requirements related to custom-XML filings are generally covered in the EDGAR Filer Manual, which is incorporated in Commission regulations by reference via Regulation S-T. *See* 17 CFR 232.11; 17 CFR 232.101.

371 *See* Commission, *Current EDGAR Technical Specifications* (Dec. 5, 2022), *available at* https://www.sec.gov/edgar/filer-information/current-edgar-technical-specifications.

372 *See* Chapters 8 and 9 of the EDGAR Filer Manual (Volume II), version 64 (Dec. 2022).

validation of the information reported on Form SCIR, which could potentially reduce the incidence of non-discretionary errors (*e.g.*, leaving required fields blank). Thus, the proposed requirement to file Parts I and II of proposed Form SCIR through the EDGAR system would allow the Commission and, in the case of Part II, the public to more effectively examine and analyze the reported information. In this regard, the proposed requirement to file Parts I and II of proposed Form SCIR through the EDGAR system using SCIR-specific XML, a machine-readable data language, is designed to facilitate more thorough review and analysis of the reported information.

b. Request for Comment

The Commission requests comment on all aspects of the proposed requirements to file Parts I and II of Form SCIR in EDGAR using a structured data language. In addition, the Commission is requesting comment on the following specific aspects of the proposals:

72. Should the Commission modify the structured data language requirement for both Parts I and II of Form SCIR in accordance with the alternatives discussed in Section IV.F. below?[373] Should Covered Entities be required to file the cybersecurity risk and incident disclosures on Part II of Form SCIR in the EDGAR system in a structured data language? Why or why not? Would custom XML or Inline eXtensible Business Reporting Language ("iXBRL") be the most suitable data language for this information? Or would another data language be more appropriate?

5. Recordkeeping

a. Amendments to Covered Entity Recordkeeping Rules

As discussed above, proposed Rule 10 would require a Covered Entity to: (1) establish, maintain, and enforce reasonably designed policies and procedures to address cybersecurity

---

[373] *See* section IV.F. of this release.

risks;[374] (2) create written documentation of risk assessments;[375] (3) create written documentation of any cybersecurity incident, including its response to and recovery from the incident;[376] (4) prepare a written report each year describing its annual review of its policies and procedures to address cybersecurity risks;[377] (5) provide immediate electronic written notice to the Commission of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring;[378] (6) report, not later than 48 hours, upon having a reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring on Part I of proposed Form SCIR;[379] and (7) provide a written summary disclosure about its cybersecurity risks that could materially affect its business and operations, and how the Covered Entity assesses, prioritizes, and addresses those risks, and significant cybersecurity incidents that occurred during the current or previous calendar year on Part II of proposed Form SCIR.[380] Consequently, proposed Rule 10 would require a Covered Entity to make several different types of records (collectively, the "Rule 10 Records"). The proposed cybersecurity rule would not include requirements specifying how long these records would need to be preserved and the manner in which they would need to be maintained. Instead, as discussed below, preservation and maintenance requirements applicable to Rule 10 Records

---

374 *See* paragraph (b)(1) of proposed Rule 10. *See also* sections II.B.1.a. through II.B.1.e. of this release (discussing this proposed requirement in more detail).

375 *See* paragraph (b)(1)(i)(B) of proposed Rule 10. *See also* section II.B.1.a. of this release (discussing this proposed requirement in more detail).

376 *See* paragraph (b)(1)(v)(B) of proposed Rule 10. *See also* section II.B.1.e. of this release (discussing this proposed requirement in more detail).

377 *See* paragraph (b)(2)(ii) of proposed Rule 10. *See also* section II.B.1.f. of this release (discussing this proposed requirement in more detail).

378 *See* paragraph (c)(1) of proposed Rule 10. *See also* section II.B.2.a. of this release (discussing this proposed requirement in more detail).

379 *See* paragraph (c)(2) of proposed Rule 10. *See also* Section II.B.2.b. of this release (discussing this proposed requirement in more detail).

380 *See* paragraph (d) of proposed Rule 10. *See also* Section II.B.3. of this release (discussing this proposed requirement in more detail).

would be imposed through amendments, as necessary, to the existing record preservation and maintenance rules applicable to the Covered Entities.

In particular, broker-dealers, transfer agents, and SBS Entities are subject to existing requirements that specify how long the records they are required to make must be preserved (*e.g.*, three or six years) and how the records must be maintained (*e.g.*, maintenance requirements for electronic records).[381] The Commission is proposing to amend these record preservation and maintenance requirements to identify Rule 10 Records specifically as records that would need to be preserved and maintained pursuant to these existing requirements. In particular, the Commission is proposing to amend the record preservation and maintenance rules for: (1) broker-dealers;[382] (2) transfer agents;[383] and (3) SBS entities.[384] The proposed amendments would specify that the Rule 10 Records must be retained for three years. In the case of the written policies and procedures to address cybersecurity risks, the record would need to be maintained until three years after the termination of the use of the policies and procedures. These amendments would subject the Rule 10 Records to the record maintenance requirements of Rules 17a-4, 17ad-7, and 18a-6, including the requirements governing electronic records.[385]

Exchange Act Rule 17a-1 ("Rule 17a-1")—the record maintenance and preservation rule applicable to registered clearing agencies, the MSRB, national securities associations, and

---

381 *See* 17 CFR 240.17a-4 ("Rule 17a-4") (setting forth record preservation and maintenance requirements for broker-dealers); 17 CFR 240.17Ad-7 ("Rule 17ad-7") (setting forth record preservation and maintenance requirements for transfer agents); 17 CFR 240.18a-6 ("Rule 18a-6") (setting forth record preservation and maintenance requirements for SBS Entities). The Commission's proposal includes an amendment to a CFR designation in order to ensure regulatory text conforms more consistently with section 2.13 of the Document Drafting Handbook. *See* Office of the Federal Register, Document Drafting Handbook (Aug. 2018 Edition, Revision 1.4, dated January 7, 2022), *available at* https://www.archives.gov/files/federal-register/write/handbook/ddh.pdf. In particular, the proposal is to amend the CFR section designation for Rule 17Ad-7 (17 CFR 240.17Ad-7) to replace the uppercase letter with the corresponding lowercase letter, such that the rule would be redesignated as Rule 17ad-7 (17 CFR 240.17ad-7).

382 This amendment would add a new paragraph (e)(13) to Rule 17a-4.

383 This amendment would add a new paragraph (j) to Rule 17ad-7.

384 This amendment would add a new paragraph (d)(6) to Rule 18a-6 .

385 *See* paragraphs (f) of Rule 17a-4, (f) of Rule 17ad-7, and (e) of Rule 18a-6 (setting forth requirements for electronic records applicable to broker-dealers, transfer agents, and SBS Entities, respectively).

national securities exchanges—as it exists today would require the preservation of the Rule 10 Records.[386] In particular, Rule 17a-1 requires these types of Covered Entities to keep and preserve at least one copy of all documents, including all correspondence, memoranda, papers, books, notices, accounts, and other such records as shall be made or received by the Covered Entity in the course of its business as such and in the conduct of its self-regulatory activity.[387] Furthermore, Rule 17a-1 provides that the Covered Entity must keep the documents for a period of not less than five years, the first two years in an easily accessible place, subject to the destruction and disposition provisions of Exchange Act Rule 17a-6.[388] Consequently, under the existing provisions of Rule 17a-1, registered clearing agencies, the MSRB, national securities associations, and national securities exchanges would be required to preserve at least one copy of the Rule 10 Records for at least five years, the first two years in an easily accessible place. In the case of the written policies and procedures to address cybersecurity risks, pursuant to Rule 17a-1 the record would need to be maintained until five years after the termination of the use of the policies and procedures.[389]

Similarly, Exchange Act Rule 13n-7 ("Rule 13n-7")—the record maintenance and preservation rule applicable to SBSDRs—as it exists today would require the preservation of the Rule 10 Records.[390] In particular, Rule 13n-7 requires SBSDRs to, among other things, keep and preserve at least one copy of all documents, including all documents and policies and procedures required by the Exchange Act and the rules and regulations thereunder, correspondence,

---

386 *See* 17 CFR 240.17a-1.

387 *See* paragraph (a) of Rule 17a-1.

388 *See* paragraph (b) of Rule 17a-1; 17 CFR 240.17a-6 ("Rule 17a-6"). Rule 17a-6 of the Exchange Act provides that an SRO may destroy such records at the end of the five year period or at an earlier date as is specified in a plan for the destruction or disposition of any such documents if such plan has been filed with the Commission by SRO and has been declared effective by the Commission.

389 *See, e.g.*, *Nationally Recognized Statistical Rating Organizations*, Exchange Act Release No. 72936 (Aug. 27, 2014) [79 FR 55078, 55099-100 (Sept. 15, 2014)] (explaining why preservation periods for written policies and procedures are based on when a version of the policies and procedures is updated or replaced).

390 *See* 17 CFR 240.13n-7.

memoranda, papers, books, notices, accounts, and other such records as shall be made or received by it in the course of its business as such.[391] Furthermore, Rule 13n-7 provides that the SBSDR must keep the documents for a period of not less than five years, the first two years in a place that is immediately available to representatives of the Commission for inspection and examination.[392] Consequently, under the existing provisions of Rule 13n-7, SBSDRs would be required to preserve at least one copy of the Rule 10 Records for at least five years, the first two years in a place that is immediately available to representatives of the Commission for inspection and examination. In the case of the written policies and procedures to address cybersecurity risks, the Commission interprets this provision of Rule 13n-7 to require that the record would need to be maintained until five years after the termination of the use of the policies and procedures.

Clearing agencies that are exempt from registration would be Covered Entities under proposed Rule 10.[393] Exempt clearing agencies are not subject to Rule 17a-1. However, while exempt clearing agencies—as entities that have limited their clearing agency functions—might not be subject to the full range of clearing agency regulation, the Commission has stated that, for example, an entity seeking an exemption from clearing agency registration for matching services would be required to, among other things, allow the Commission to inspect its facilities and records.[394] In this regard, exempt clearing agencies are subject to conditions that mirror certain

---

391 *See* paragraph (b)(1) of Rule 13n-7.

392 *See* paragraph (b)(2) of Rule 13n-7.

393 *See* paragraph (a)(1)(ii) of proposed Rule 10 (defining as a "covered entity" a clearing agency (registered or exempt) under section 3(a)(23)(A) of the Exchange Act). *See also* section I.A.2.c. of this release (discussing the clearing agency exemptions provided by the Commission).

394 *See Confirmation and Affirmation of Securities Trades; Matching*, Exchange Act Release No. 39829 (Apr. 6, 1998) [63 FR 17943 (Apr. 13, 1998)] (providing interpretive guidance and requesting comment on the confirmation and affirmation of securities trades and matching).

of the recordkeeping requirements in Rule 17a-1,[395] as set forth in the respective Commission orders exempting each exempt clearing agency from the requirement to register as a clearing agency (the "clearing agency exemption orders").[396] Pursuant to the terms and conditions of the clearing agency exemption orders, the Commission may modify by order the terms, scope, or conditions if the Commission determines that such modification is necessary or appropriate in the public interest, for the protection of investors, or otherwise in furtherance of the purposes of the Exchange Act.[397] In support of the public interest and the protection of investors, the Commission is proposing to amend the clearing agency exemption orders to add a condition that each exempt clearing agency must retain the Rule 10 Records for a period of at least five years after the record is made or, in the case of the written policies and procedures to address cybersecurity risks, for at least five years after the termination of the use of the policies and procedures.

b. Request for Comment

The Commission requests comment on all aspects of the proposed recordkeeping requirements. In addition, the Commission is requesting comment on the following specific aspects of the proposals:

73. Should the proposed amendments to Rules 17a-4, 18a-6, and/or 17ad-7 be modified? If so, describe how they should be modified and explain why the modification would be appropriate. For example, should the retention periods for

---

395 *See, e.g.,* BSTP SS&C Order, 80 FR at 75411 (conditioning BSTP's exemption by requiring BSTP to, among other things, preserve a copy or record of all trade details, allocation instructions, central trade matching results, reports and notices sent to customers, service agreements, reports regarding affirmation rates that are sent to the Commission or its designee, and any complaint received from a customer, all of which pertain to the operation of its matching service and ETC service. BSTP shall retain these records for a period of not less than five years, the first two years in an easily accessible place.).

396 *See* DTCC ITP Matching Order, 66 FR 20494; BSTP SS&C Order, 80 FR 75388; Euroclear Bank Order, 81 FR 93994.

397 *See* Clearstream Banking Order, 62 FR 9225.

the records be five years (consistent with Rule 17a-1) or some other period of years as opposed to three years? If so, explain why. If not, explain why not.

74. As discussed above, the Commission is proposing to amend the clearing agency exemption orders to specifically require the exempt clearing agencies to retain the Rule 10 Records. Should the ordering language be consistent with the proposed amendments to Rules 17a-4, 17ad-7, and18a-6? For example, should the ordering language provide that the exempt clearing agency must maintain and preserve: (1) the written policies and procedures required to be adopted and implemented pursuant to paragraph (b)(1) of proposed Rule 10 until five years after the termination of the use of the policies and procedures; (2) the written documentation of any risk assessment pursuant to paragraph (b)(1)(i)(B) of proposed Rule 10 for five years; (3) the written documentation of the occurrence of a cybersecurity incident pursuant to paragraph (b)(1)(v)(B) of proposed Rule 10, including any documentation related to any response and recovery from such an incident, for five years; (4) the written report of the annual review required to be prepared pursuant to paragraph (b)(2)(ii) of proposed Rule 10 for five years; (5) a copy of any notice transmitted to the Commission pursuant to paragraph (c)(1) of proposed Rule 10 or any Part I of proposed Form SCIR filed with the Commission pursuant to paragraph (c)(2) of proposed Rule 10 for five years; and (6) a copy of any Part II of proposed Form SCIR filed with the Commission pursuant to paragraph (d) of proposed Rule 10 for five years? Additionally, should the ordering language provide that the exempt clearing agency must allow the Commission to inspect its facilities and records? If so, explain why. If not, explain why not.

C. Proposed Requirements for Non-Covered Broker-Dealers

1. Cybersecurity Policies and Procedures, Annual Review, Notification, and Recordkeeping

As discussed earlier, not all broker-dealers would be Covered Entities under proposed Rule 10.[398] Consequently, these Non-Covered Broker-Dealers would not be subject to the requirements of proposed Rule 10 to: (1) include certain elements in their cybersecurity risk management policies and procedures;[399] (2) file confidential reports that provide information about the significant cybersecurity incident with the Commission and, for some Covered Entities, other regulators;[400] and (3) make public disclosures about their cybersecurity risks and the significant cybersecurity incidents they experienced during the current or previous calendar year.[401]

In light of their limited business activities, Non-Covered Broker-Dealers would not be subject to the same requirements as would Covered Entities. Instead, Non-Covered Broker-Dealers would be required to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks taking into account the size, business, and operations of the firm.[402] They also would be required to review and assess the design and effectiveness of their cybersecurity policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review. They also would be required to make a record with respect to the annual review. In addition, they would be required to provide the Commission and their examining authority with

---

398 *See* section II.A.1. of this release (discussing the definition of "covered entity" and why certain broker-dealers would not be included within the definition).

399 *See* paragraphs (b)(1)(i) through (v) of proposed Rule 10.

400 *See* paragraph (c)(2) of proposed Rule 10. *See also* paragraph (a)(10) of proposed Rule 10 (defining the term "significant cybersecurity risk").

401 *See* paragraph (d) of proposed Rule 10.

402 *See* paragraph (e)(1) of proposed Rule 10.

immediate written electronic notice of a significant cybersecurity incident affecting them.[403] Finally, they would be required to maintain and preserve versions of their policies and procedures and the record of the annual review.

A Non-Covered Broker-Dealer could be a firm that limits its business to selling mutual funds on a subscription-way basis or a broker-dealer that limits its business to engaging in private placements for clients. Alternatively, it could be a broker-dealer that limits its business to effecting securities transactions in order to facilitate mergers, acquisitions, business sales, and business combinations or a broker-dealer that limits its business to engaging in underwritings for issuers. Moreover, a Non-Covered Broker-Dealer—because it does not meet the definition of "covered entity"—would not a be a broker-dealer that: maintains custody of customer securities and cash;[404] connects to a broker-dealer that maintains custody of customer securities through an introducing relationship;[405] is a large proprietary trading firm;[406] operates as a market maker;[407] or operates an ATS.[408]

A broker-dealer that limits its business to one of the activities described above and that does not engage in functions that would make it a Covered Entity under proposed Rule 10 generally does not use information systems to carry out its operations to the same degree as a

---

403 *See* paragraph (e)(2) of proposed Rule 10.

404 *See* paragraph (a)(1)(i)(A) of proposed Rule 10 (defining "covered entity" to include a broker-dealer that maintains custody of cash and securities for customers or other broker-dealers and is not exempt from the requirements of Rule 15c3-3).

405 *See* paragraph (a)(1)(i)(B) of proposed Rule 10 (defining "covered entity" to include a broker-dealer that introduces customer accounts on a fully disclosed basis to another broker-dealer that maintains custody of cash and securities for customers or other broker-dealers and is not exempt from the requirements of Rule 15c3-3).

406 *See* paragraphs (a)(1)(i)(C) and (D) of proposed Rule 10 (defining "covered entity" to include a broker-dealer with regulatory capital equal to or exceeding $50 million or total assets equal to or exceeding $1 billion).

407 *See* paragraph (a)(1)(i)(E) of proposed Rule 10 (defining "covered entity" to include a broker-dealer that is a market maker under the Exchange Act or the rules thereunder (which includes a broker-dealer that operates pursuant to Rule 15c3-1(a)(6)) or is a market maker under the rules of an SRO of which the broker-dealer is a member).

408 *See* paragraph (a)(1)(i)(F) of proposed Rule 10 (defining "covered entity" to include a broker-dealer that is an ATS).

broker-dealer that is a Covered Entity. For example, the information systems used by a Non-Covered Broker-Dealer could be limited to smart phones and personal computers with internet and email access. Moreover, this type of firm may have a small staff of employees using these information systems. Therefore, the overall footprint of the information systems used by a Non-Covered Broker-Dealer may be materially smaller in scale and complexity than the footprint of the information systems used by a broker-dealer that is a Covered Entity. In addition, the amount of data stored on these information systems relating to the Non-Covered Broker-Dealer's business may be substantially less than the amount of data stored on a Covered Entity's information systems. This means the information system perimeter of these firms that needs to be protected from cybersecurity threats and vulnerabilities is significantly smaller than that of a Covered Broker-Dealer. For these reasons, proposed Rule 10 would provide that the written policies and procedures required of a Non-Covered Broker-Dealer must be reasonably designed to address the cybersecurity risks of the firm taking into account the size, business, and operations of the firm.

Therefore, unlike the requirements for a Covered Entity, proposed Rule 10 does not specify minimum elements that would need to be included in a Non-Covered Broker-Dealer's policies and procedures.[409] Nonetheless, a Non-Covered Broker-Dealer may want to consider whether any of those required elements would be appropriate components of it policies and procedures for addressing cybersecurity risk.[410]

Proposed Rule 10 also would require that the Non-Covered Broker-Dealer annually review and assess the design and effectiveness of its cybersecurity policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time

---

[409] *See* paragraph (b)(1) of proposed Rule 10 (setting forth the elements that would need to be included in a Covered Entity's policies and procedures).

[410] As discussed earlier, the elements are consistent with industry standards for addressing cybersecurity risk. *See* section II.B.1. of this release (discussing the policies and procedures requirements for Covered Entities).

period covered by the review.[411] The annual review and assessment requirement is designed to require Non-Covered Broker-Dealers to evaluate whether their cybersecurity policies and procedures continue to work as designed. Non-Covered Broker-Dealers could consider using this information to determine whether changes are needed to assure their continued effectiveness (*i.e.*, to make sure their policies and procedures continue to be reasonably designed to address their cybersecurity risks as required by the rule).

The rule also would require the Non-Covered Broker-Dealer to make a written record that documents the steps taken in performing the annual review and the conclusions of the annual review. Therefore, Non-Covered Broker-Dealers would need to make a record of the review rather than documenting the review in a written report, as would be required of Covered Entities.[412] A report is a means to communicate information within an organization. The personnel that prepare the report for the Covered Entity would be able to use it to communicate their assessment of the firm's policies and procedures to others within the organization such as senior managers. For purposes of proposed Rule 10, a record, among other things, is a means to document that an activity took place, for example, to demonstrate compliance with a requirement. As discussed above, Non-Covered Broker-Dealers generally would be smaller and less complex organizations than Covered Entities. A record of the annual review could be used by Commission examination staff to review the Non-Covered Broker-Dealer's compliance with the annual review requirement without imposing the additional process involved in creating an internal report.

As discussed earlier, Covered Entities would be subject to a requirement to give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or

---

411 *See* paragraph (e)(1) of proposed Rule 10.

412 *See* section II.B.1.f. of this release (discussing in more detail the annual report that would be required of Covered Entities).

is occurring.[413] Non-Covered Broker-Dealers would be subject to the same immediate written electronic notice requirement. In particular, they would be required to give immediate written electronic notice to the Commission of a significant cybersecurity incident upon having a reasonable basis to conclude that the incident has occurred or is occurring.[414] The Commission would keep the notices nonpublic to the extent permitted by law. The notice would need to identify the Non-Covered Broker-Dealer, state that the notice is being given to alert the Commission of a significant cybersecurity incident impacting the Non-Covered Broker-Dealer, and provide the name and contact information of an employee of the Non-Covered Broker-Dealer who can provide further details about the nature and scope of the significant cybersecurity incident. In addition, Non-Covered Broker-Dealers—like Covered Broker-Dealers—would need to give the notice to their examining authority.[415] The immediate written electronic notice is designed to alert the Commission on a confidential basis to the existence of a significant cybersecurity incident impacting a Non-Covered Broker-Dealer so the Commission staff can quickly begin to assess the event.

Finally, as discussed above, proposed Rule 10 would require the Non-Covered Broker-Dealer to: (1) establish, maintain, and enforce written policies and procedures that are reasonably designed to address the cybersecurity risks of the firm; (2) make a written record that documents its annual review; and (3) provide immediate electronic written notice to the Commission of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring.[416] The Commission is proposing to amend the broker-dealer record preservation and maintenance rule to identify these records specifically

---

413 *See* paragraph (c)(1) of proposed Rule 10. *See also* section II.B.2.a. of this release (discussing the immediate notification requirement for Covered Entities in more detail).

414 *See* paragraph (e)(2) of proposed Rule 10. *See also* paragraph (a)(10) of proposed Rule 10 (defining the term "significant cybersecurity incident").

415 *See* paragraph (e)(2) of proposed Rule 10. *See* also paragraph (c)(1)(i) of proposed Rule 10 (requiring Covered Broker-Dealers to provide the notice to their examining authority).

416 *See* paragraph (e) of proposed Rule 10.

as being subject to the rule's requirements.[417] Under the amendments, the written policies and procedures would need to be maintained until three years after the termination of the use of the policies and procedures and all other records would need to be maintained for three years.

2. Request for Comment

The Commission requests comment on all aspects of the proposed requirements for non-covered broker-dealers. In addition, the Commission is requesting comment on the following specific aspects of the proposals:

75. Should paragraph (e)(1) of proposed Rule 10 be modified to specify certain minimum elements that would need to be included in the policies and procedures of Non-Covered Broker-Dealers? If so, identify the elements and explain why they should be included. For example, should paragraph (e) of proposed Rule 10 specify that the policies and procedures must include policies and procedures to address any or all of the following: (1) risk assessment; (2) user security and access; (3) information protection; (4) cybersecurity threat and vulnerability management; and (5) cybersecurity incident response and recovery? If so, explain why. If not, explain why not.

76. Should paragraph (e)(2) of proposed Rule 10 be modified to require the notice to be given within a specific timeframe such as on the same day the requirement was triggered or within 24 hours? If so, explain why. If not, explain why not.

77. Should paragraph (e)(2) of proposed Rule 10 be modified to revise the trigger for the immediate notification requirement? If so, explain why. If not, explain why not. For example, should the trigger be when the Non-Covered Broker-Dealer "detects" a significant cybersecurity incident (rather than when it has a reasonable basis to conclude that the significant cybersecurity incident has occurred or is

---

[417] This amendment would add a new paragraph (e)(13) to Rule 17a-4.

occurring)? If so, explain why. If not, explain why not. For example, would a detection standard be a less subjective standard? If so, explain why. If not, explain why not. Is there another trigger standard that would be more appropriate? If so, identify it and explain why it would be more appropriate.

78. Should paragraph (e)(2) of proposed Rule 10 be modified to eliminate the requirement that a Non-Covered Broker-Dealer give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring? If so, explain why. If not, explain why not. For example, would this requirement be unduly burdensome on Non-Covered Broker-Dealers? Please explain.

79. If the immediate notification requirement of paragraph (e)(2) is adopted as proposed, it is anticipated that a dedicated email address would be established to receive these notices. Are there other methods the Commission should use for receiving these notices? If so, identity them and explain why they would be more appropriate than email. For example, should the notices be received through the EDGAR system? If so, explain why. If not, explain why not.

80. Should paragraph (e) of proposed Rule 10 be modified to include any other requirements that would be applicable to Covered Entities under proposed Rule 10 that also should be required of Non-Covered Broker-Dealers? If so, identify them and explain why they should apply to Non-Covered Broker-Dealers. For example, should the paragraph be modified to require Non-Covered Broker-Dealers to report information about a significant cybersecurity incident confidentially on Part I of proposed Form SCIR? If so, explain why. If not, explain why not. Should the timeframe for filing Part I of Proposed Form SCIR be longer for Non-Covered Broker-Dealers? For example, should the reporting

timeframe be within 72 or 96 hours instead of 48 hours? Please explain. If Non-Covered Broker-Dealers were required to file Part I of Form SCIR, should they be permitted to provide more limited information about the significant cybersecurity incident than Covered Entities? If so, identify the more limited set of information and explain why it would be appropriate to permit Non-Covered Broker-Dealers omit the additional information that Covered Entities would need to report.

81. Should Non-Covered Broker-Dealers be required to make and preserve for three years in accordance with Rule 17a-4 a record of any significant cybersecurity incident that impacts them containing some or all of the information that would be reported by Covered Entities on Part I of proposed Form SCIR? If so, explain why. If not, explain why not.

82. Should paragraph (e) of proposed Rule 10 be modified to require a Non-Covered Broker-Dealer to prepare a written report of the annual review (rather than a record, as proposed)? If so, explain why. If not, explain why not.

D. Cross-Border Application of the Proposed Cybersecurity Requirements to SBS Entities

1. Background on the Cross-Border Application of Title VII Requirements

Security-based swap transactions take place across national borders, with agreements negotiated and executed between counterparties in different jurisdictions (which might then be booked and risk-managed in still other jurisdictions).[418] Mindful that this global market developed prior to the enactment of the Dodd-Frank Act and the fact that the application of Title VII[419] to cross-border activities raises issues of potential conflict or overlap with foreign

---

418 *See* Cross-Border Proposing Release, 78 FR at 30976, n. 48.

419 Unless otherwise indicated, references to "Title VII" in this section of this release are to Subtitle B of Title VII of the Dodd-Frank Act.

regulatory regimes,[420] the Commission has adopted a taxonomy to classify requirements under section 15F of the Exchange Act as applying at either the transaction-level or at the entity-level.[421] Transaction-level requirements under section 15F of the Exchange Act are those that primarily focus on protecting counterparties to security-based swap transactions by requiring SBSDs to, among other things, provide certain disclosures to counterparties, adhere to certain standards of business conduct, and segregate customer funds, securities, and other assets.[422] In contrast to transaction-level requirements, entity-level requirements under section 15F of the Exchange Act are those that are expected to play a role in ensuring the safety and soundness of the SBS Entity and thus relate to the entity as a whole.[423] Entity-level requirements include capital and margin requirements, as well as other requirements relating to a firm's identification and management of its risk exposure, including the risk management procedures required under section 15F(j) of the Exchange Act, a statutory basis for rules applicable to SBS Entities that the Commission is proposing in this release.[424] Because these requirements relate to the entire entity, they apply to SBS Entities on a firm-wide basis, without exception.[425]

The Commission applied this taxonomy in 2016 when it adopted rules to implement business conduct standards for SBS Entities. At that time, the Commission also stated that the

---

420 *See* Cross-Border Proposing Release, 78 FR at 30975.

421 *See id*. at 31008-25. *See also Business Conduct Standards for Security-Based Swap Dealers and Major Security-Based Swap Participants*, Exchange Act Release No. 77617 (Apr. 14, 2016) [81 FR 29959, 30061-69 (May 13, 2016)] ("Business Conduct Standards Adopting Release").

422 Cross-Border Proposing Release, 78 FR at 31010.

423 *See id*. at 31011, 31035.

424 *See id*. at 31011-16 (addressing the classification of capital and margin requirements, as well as of the risk management requirements of section 15F(j) of the Exchange Act and other entity-level requirements applicable to SBSDs).

425 *See id*. at 31011, 31024-25. *See also id*. at 31035 (applying the analysis to MSBSPs). In reaching this conclusion, the Commission explained that it "preliminarily believes that entity-level requirements are core requirements of the Commission's responsibility to ensure the safety and soundness of registered security based swap dealers," and that "it would not be consistent with this mandate to provide a blanket exclusion to foreign security-based swap dealers from entity-level requirements applicable to such entities." *Id*. at 31024 (footnotes omitted). The Commission further expressed the preliminary view that concerns regarding the application of entity-level requirements to foreign SBSDs would largely be addressed through the proposed approach to substituted compliance. *See id*.

rules and regulations prescribed under section 15F(j) should be treated as entity-level requirements.[426] The Commission has not, however, expressly addressed the entity-level treatment of the cybersecurity requirements under proposed Rule 10, except with regard to recordkeeping and reporting.[427]

2. Proposed Entity-Level Treatment

a. Proposal

Consistent with its approach to the obligations described in Section 15F(j) and to capital,[428] margin,[429] risk mitigation,[430] and recordkeeping,[431] the Commission is proposing to apply the requirements of proposed Rule 10 to an SBS Entity's entire security-based swap business without exception, including in connection with any security-based swap business it conducts with foreign counterparties.[432]

Cybersecurity policies and procedures and the related requirements of proposed Rule 10 serve as an important mechanism for allowing SBS Entities and their counterparties to manage risks associated with their operations, including risks related to the entity's safety and soundness.[433] An alternative approach that does not require an SBS Entity to take steps to

---

426 *See* Business Conduct Standards Adopting Release, 81 FR at 30064-65.

427 The Commission has previously stated that recordkeeping and reporting requirements are entity-level requirements. *See Recordkeeping and Reporting Requirements for Security-Based Swap Dealers, Major Security-Based Swap Participants, and Broker-Dealers*, Exchange Act Release No. 87005 (Sept. 19, 2019), 84 FR 68550, 68596-97 (Dec. 16, 2019) ("SBS Entity Recordkeeping and Reporting Adopting Release").

428 *See* Capital, Margin, and Segregation Requirements for Security-Based Swap Dealers and Major Security-Based Swap Participants and Capital and Segregation Requirements for Broker-Dealers. Exchange Act Release No. 86175 (Jun. 21, 2019), 84 FR 43872, 43879 (Aug, 22, 2019) ("Capital, Margin, and Segregation Requirements Adopting Release").

429 *Id.*

430 *See Risk Mitigation Techniques for Uncleared Security-Based Swaps*, Exchange Act Release No. 87782 (Dec. 18, 2019) [85 FR 6359, 6378 (Feb. 4, 2020) ("SBS Entity Risk Mitigation Adopting Release")

431 *See* SBS Entity Recordkeeping and Reporting Adopting Release, 84 FR at 68596-97.

432 As entity-level requirements, transaction-level exceptions such as in 17 CFR 3a71-3(c) and 17 CFR 3a67-10(d), would not be available for the proposed cybersecurity requirements.

433 *See* sections I.A. and II.B.1. of this release (discussing, respectively, cybersecurity risks and how those risks can be managed by certain policies, procedures, and controls). *See also* sections II.B.2-5 of this release.

manage cybersecurity risk throughout the firm's entire business could contribute to operational risk affecting the entity's security-based swap business as a whole, and not merely specific security-based swap transactions. Moreover, to the extent that these risks affect the safety and soundness of the SBS Entity, they also may affect the firm's counterparties and the functioning of the broader security-based swap market. Accordingly, the Commission proposes to apply the requirements to the entirety of an SBS Entity's business.[434] However, as described below, the Commission is proposing that foreign SBS Entities have the potential to avail themselves of substituted compliance to satisfy the cybersecurity requirements under proposed Rule 10.

b. Request for Comment

The Commission generally requests comments on the proposed entity-level application of proposed Rule 10. In addition, the Commission requests comments on the following specific issues:

83. Does the proposed approach appropriately treat the proposed requirements as entity-level requirements applicable to the entire business conducted by foreign SBS Entities? If not, please identify any particular aspects of proposed Rule 10 that should not be applied to a foreign SBS Entity, or applied only to specific

---

[434] The Commission has expressed the view that an entity that has registered with the Commission subjects itself to the entire regulatory system governing such registered entities. Cross-Border Proposing Release, 78 FR at 30986. *See also* Business Conduct Standards Adopting Release, 81 FR at n.1306 (determining that the requirements described in section 15F(j) of the Exchange Act should be treated as entity-level requirements, and stating that such treatment would not be tantamount to applying Title VII to persons that are "transact[ing]a business in security-based swaps without the jurisdiction of the United States," within the meaning of section 30(c) of the Exchange Act). That treatment of section 15F(j) of the Exchange Act was also deemed necessary or appropriate as a prophylactic measure to help prevent the evasion of the provisions of the Exchange Act that were added by the Dodd-Frank Act, and thus help prevent the relevant purposes of the Dodd-Frank Act from being undermined. *Id.* (citing *Application of "Security-Based Swap Dealer" and "Major Security-Based Swap Participant" Definitions to Cross-Border Security-Based Swap Activities; Republication*, Exchange Act Release No. 72472 (June 25, 2014) [79 FR 47277, 47291-92 (Aug. 12, 2014)] ("SBS Entity Definitions Adopting Release") (interpreting anti-evasion provisions of the Exchange Act, section 30(c)). A different approach in connection with proposed Rule 10 would not be consistent with the purposes of Title VII of the Dodd-Frank Act and could allow SBS Entities to avoid compliance with these proposed rules for portions of their business in a manner that could increase the risk to the registered entity.

transactions, and explain how such an approach would be consistent with the goals of Title VII of the Dodd-Frank Act.

84. Should the Commission apply the same cross-border approach to the application of proposed Rule 10 for both SBSDs and MSBSPs? If not, please describe how the cross-border approach for SBSDs should differ from the cross-border approach for MSBSPs, and explain the reason(s) for any potential differences in approach.

85. What types of conflicts might a foreign SBS Entity face if it had to comply with proposed Rule 10 in more than one jurisdiction? In what situations would compliance with more than one of these requirements be difficult or impossible? For Market Entities that are U.S. persons, could compliance with the proposed rules create compliance challenges with requirements in a foreign jurisdiction?

86. As an alternative to treating the proposed requirements as entity-level requirements, should the Commission instead treat the proposed requirements as transaction-level requirements? If so, to which cross-border security-based swap transactions should these requirements apply and why? Please describe how these requirements would apply differently if classified as transaction-level requirements instead of as entity-level requirements.

3. Availability of Substituted Compliance

a. Existing Substituted Compliance Rule

In 2016,[435] the Commission adopted Exchange Act Rule 3a71-6 ("Rule 3a71-6")[436] to provide that the Commission may, by order, make a determination that compliance with specified requirements under a foreign financial regulatory system by non-U.S. SBS Entities[437] may satisfy certain business conduct requirements under Exchange Act section 15F, subject to certain conditions. The rule in part provides that the Commission shall not make a determination providing for substituted compliance unless the Commission determines, among other things, that the foreign regulatory requirements are comparable to otherwise applicable requirements.[438]

When the Commission adopted this substituted compliance rule that addressed the specified business conduct requirements, the Commission also noted that Exchange Act section 15F(j)(7) authorizes the Commission to prescribe rules governing the duties of SBS Entities.[439] The Commission stated that it was not excluding that provision from the potential availability of substituted compliance, and that it expected to separately consider whether substituted compliance may be available in connection with any future rules promulgated pursuant to that provision.[440] Further, the Commission stated that it expected to assess the potential availability of substituted compliance in connection with other requirements when the Commission considers

---

435 *See* Business Conduct Standards Adopting Release, 81 FR at 30070-81. Separately, in 2015, the Commission adopted a rule making substituted compliance potentially available in connection with certain regulatory reporting and public dissemination requirements related to security-based swaps. *See Regulation SBSR-Reporting and Dissemination of Security-Based Swap Information*, Exchange Act Release No. 74244 (Feb. 11, 2015) [80 FR 14563 (Mar. 19, 2015)] (adopting 17 CFR 242.908 ("Rule 908")). Paragraph (c) of Rule 908 does not contemplate substituted compliance for the rules being proposing today.

436 *See* 17 CFR 240.3a71-6.

437 If the Commission makes a substituted compliance determination under paragraph (a)(1) of Rule 3a71-6, SBS Entities that are not U.S. persons (as defined in 17 CFR 240.3a71-3(a)(4) ("Rule 3a71-3(a)(4)")), but not SBS Entities that are U.S. persons, may satisfy specified requirements by complying with comparable foreign requirements and any conditions set forth in the substituted compliance determination made by the Commission. *See* paragraphs (b) and (d) of Rule 3a71-6.

438 *See* paragraph (a)(2) of 3a71-6. *See also* Business Conduct Standards Adopting Release, 81 FR at 30074.

439 Business Conduct Standards Adopting Release, 81 FR at n. 1438.

440 *Id.*

final rules to implement those requirements.[441] Consistent with these statements, the Commission subsequently amended Rule 3a71-6 to provide SBS Entities that are non U.S. persons with the potential to avail themselves of substituted compliance with respect to the following Title VII requirements: (1) trade acknowledgment and verification,[442] (2) capital and margin requirements,[443] (3) recordkeeping and reporting,[444] and (4) portfolio reconciliation, portfolio compression, and trading relationship documentation.[445]

b. Proposed Amendment to Rule 3a71-6

The Commission is proposing to further amend Rule 3a71-6 to provide SBS Entities that are not U.S. persons (as defined in Rule 3a71-3(a)(4) of the Exchange Act) with the potential to avail themselves of substituted compliance to satisfy the cybersecurity requirements of proposed Rule 10 and Form SCIR as applicable to SBS Entities.[446] In proposing to amend the rule, the Commission preliminarily believes that the principles associated with substituted compliance, as previously adopted in connection with both the business conduct requirements and the recordkeeping and reporting requirements, in large part should similarly apply to the cyber security risk management requirements being proposing today. The discussions in the Business Conduct Standards Adopting Release, including for example those regarding consideration of supervisory and enforcement practices,[447] certain multi-jurisdictional issues,[448] and application

---

441 *See* Business Conduct Standards Adopting Release, 81 FR at 30074.

442 *See Trade Acknowledgment and Verification of Security-Based Swap Transactions*, Exchange Act Release No. 78011 (Jun. 8, 2016) [81 FR 39807, 39827-28 (Jun. 17, 2016)] ("SBS Entity Trade Acknowledgment and Verification Adopting Release").

443 *See* Capital, Margin, and Segregation Requirements Adopting Release, 84 FR at 43948-50.

444 *See* SBS Entity Recordkeeping and Reporting Adopting Release, 84 FR at 68597-99.

445 *See* SBS Entity Risk Mitigation Adopting Release, 85 FR at 6379-80.

446 Substituted compliance would only be available to eligible SBS Entities. For example, substituted compliance would not be available to a Market Entity registered as both an SBS Entity and a broker-dealer with respect to the broker-dealer's obligations under the proposed rules.

447 Business Conduct Standards Adopting Release, 81 FR at 30079.

448 Business Conduct Standards Adopting Release, 81 FR at 30079-80.

procedures[449] are applicable to the proposed cybersecurity requirements. Accordingly, the proposed substituted compliance rule would apply to the cybersecurity risk management requirements in the same manner as it already applies to existing business conduct requirements and the recordkeeping and reporting requirements.

Making substituted compliance available for the cybersecurity risk management requirements would be consistent with the approach the Commission has taken with other rules applicable to SBS Entities. This approach takes into consideration the global nature of the security-based swap market and the prevalence of cross-border transactions within that market.[450] The application of the cybersecurity risk management requirements may lead to requirements that are duplicative of, or in conflict with, applicable foreign requirements, even when the two sets of requirements implement similar goals and lead to similar results. Those results have the potential to disrupt existing business relationships and, more generally, to reduce competition and market efficiency. To address those effects, under certain circumstances it may be appropriate to allow the possibility of substituted compliance, whereby non-U.S. market participants may satisfy the cybersecurity risk management requirements by complying with comparable foreign requirements. Allowing for the possibility of substituted compliance in this manner would help achieve the benefits of those particular requirements in a way that helps avoid regulatory conflict and minimizes duplication, thereby promoting market efficiency, enhancing competition, and contributing to the overall functioning of the global security-based swap market.

Accordingly, the Commission is proposing to amend paragraph (d)(1) of Rule 3a71-6 to make substituted compliance available for proposed Rule 10 and Form SCIR if the Commission determines with respect to a foreign financial regulatory system that compliance with specified

---

449 Business Conduct Standards Adopting Release, 81 FR at 30080-81.

450 *See generally* Business Conduct Standards Adopting Release, 81 FR at 30073-74 (addressing the basis for making substituted compliance available in the context of the business conduct requirements).

requirements under such foreign financial regulatory system by a registered SBS Entity, or class thereof, satisfies the corresponding requirements of proposed Rule 10 and Form SCIR.[451] However, the proposal would not amend Rule 3a71-6 in connection with the proposed amendments to Rule 18a-6 regarding records to be preserved by certain SBS Entities. Rule 3a71-6 currently permits eligible applicants to seek a substituted compliance determination from the Commission with regard to the requirements of Rule 18a-6.[452]

c. Comparability Criteria, and Consideration of Related Requirements

If adopted, the proposed amendment to paragraph (d)(1) of Rule 3a71-6 would provide that eligible applicants may request that the Commission make a substituted compliance determination with respect to one or more of the requirements Rule 10 and Form SCIR.[453] Further, existing paragraph (d)(6) of Rule 3a71-6 would permit eligible applicants to request that the Commission make a substituted compliance determination with respect to one or more of the requirements of the proposed amendments to Rule 18a-6, if adopted. A positive substituted compliance determination with respect to requirements existing before adoption of the proposed Rule 10, Form SCIR, and the related record preservation requirements would not automatically result in a positive substituted compliance determination with respect to proposed Rule 10, Form SCIR or the proposed amendments to Rule 18a-6. Before making a substituted compliance determination, the substance of each foreign regulatory system to which substituted compliance would apply should be evaluated for comparability to such newly adopted requirements. As such, if the Commission adopts the proposed amendment to Rule 3a71-6, eligible applicants[454]

---

451 Paragraph (a)(1) of Rule 3a71-6 provides that the Commission may, conditionally or unconditionally, by order, make a determination with respect to a foreign financial regulatory system that compliance with specified requirements under the foreign financial system by an SBS Entity, or class thereof, may satisfy the corresponding requirements identified in paragraph (d) of the rule that would otherwise apply. *See* section II.D.3.c. of this release.

452 *See* paragraph (d)(6) of Rule 3a71-6.

453 *See* paragraph (c) of Rule 3a71-6.

454 *See* 17 CFR 3a71-6(c).

seeking a Commission determination permitting SBS Entities that are not U.S. persons to satisfy the requirements of proposed Rule 10, Form SCIR, or the proposed amendments to Rule 18a-6 by complying with comparable foreign requirements would be required to file an application, pursuant to the procedures set forth in 17 CFR 240.0-13, requesting that the Commission make a such a determination pursuant to 17 CFR 3a71-6(a)(1).[455]

The Commission has taken a holistic approach in determining the comparability of foreign requirements for substituted compliance purposes, focusing on regulatory outcomes as a whole, rather than on a requirement-by-requirement comparison.[456] The Commission preliminarily believes that such a holistic approach would be appropriate for determining comparability for substituted compliance purposes in connection with the requirements of proposed Rule 10, Form SCIR, and the proposed amendments to Rule 18a-6. Under the proposed amendment to Rule 3a71-6, the Commission's comparability assessments associated with the proposed cybersecurity risk management requirements accordingly would consider whether, in the Commission's view, the foreign regulatory system achieves regulatory outcomes that are comparable to the regulatory outcomes associated with those requirements. Rule 3a71-6 provides that the Commission's substituted compliance determination will take into account factors that the Commission determines appropriate, such as, for example, the scope and objectives of the relevant foreign regulatory requirements (taking into account the applicable criteria set forth in paragraph (d) of the rule), as well as the effectiveness of the supervisory

---

455 Existing Commission substituted compliance determinations do not address the requirements of the proposed new rules or the proposed amendments. If the Commission adopts the requirements in the proposed new or amended rules, SBS Entities (or the relevant foreign financial regulatory authority or authorities) seeking a substituted compliance determination with respect to those requirements would be required to file an application requesting that the Commission make the determination. Applicants may not request that the Commission make a substituted compliance determination related to the new requirements by amending a previously filed application that requested a substituted compliance determination related to other Commission requirements. However, new applications may incorporate relevant information from the applicant's previously filed requests for substituted compliance determinations if the information remains accurate.

456 *See* Business Conduct Standards Adopting Release, 81 FR at 30078-79. *See also* SBS Entity Trade Acknowledgment and Verification Adopting Release, 81 FR at 39828; SBS Entity Recordkeeping and Reporting Adopting Release, 84 FR at 68598-99.

compliance program administered, and the enforcement authority exercised, by a foreign financial regulatory authority or authorities in such foreign financial regulatory system to support its oversight of the SBS Entity (or class thereof) or of the activities of such SBS Entity (or class thereof).[457]

The Commission may determine to conduct its comparability analyses regarding Rule 10, Form SCIR, and the related record preservation requirements in conjunction with comparability analyses regarding other Exchange Act requirements that, like the requirements being proposed today, relate to risk management, recordkeeping, reporting, and notification requirements of SBS Entities. If the Commission adopts the proposed amendment to Rule 3a71-6, substituted compliance requests related to Rule 10, Form SCIR, and the related record preservation requirements may be filed by (i) applicants filing a request for a substituted compliance determination solely in connection with Rule 10, Form SCIR, and the related record preservation requirements,[458] and (ii) applicants filing a request for a substituted compliance determination in connection with Rule 10, Form SCIR, and the related record preservation requirements combined with a request for a substituted compliance determination related to other eligible requirements. In either event, depending on the applicable facts and circumstances, the Commission's comparability assessment associated with the Rule 10, Form SCIR, or the related record preservation requirements may constitute part of a broader assessment of Exchange Act risk management, recordkeeping, reporting, and notification requirements for SBS Entities, and the applicable comparability decisions may be made at the level of those risk management, recordkeeping, reporting, and notification requirements for SBS Entities as a whole.

d. Request for Comment

The Commission generally requests comments on all aspects of the proposed amendment

---

457 *See* 17 CFR 240.3a71-6(a)(2)(i).

458 This category of applicants would include those who previously filed requests for the Commission to make substituted compliance determinations related to other requirements eligible for substituted compliance determinations under Rule 3a71-6.

to Rule 3a71-6 and proposed availability of substituted compliance. In addition, the Commission requests comments on the following specific issues:

87. Should the Commission make substituted compliance available with respect to proposed Rule 10, Form SCIR, and the related record preservation requirements? Why or why not? If you believe that substituted compliance should not be available with respect to these requirements, how would you distinguish this policy decision from the Commission's previous determination to make substituted compliance potentially available with respect to other Title VII requirements (*i.e.*, the business conduct, trade acknowledgment and verification, capital and margin, recordkeeping and reporting, and portfolio reconciliation, portfolio compression, and trading relationship documentation rules)?

88. Are there other aspects of the scope of the substituted compliance rule for which the Commission should amend or provide additional guidance in light of proposed Rule 10, Form SCIR, and the proposed amendment to Rule 18a-6? If so, what other amendments or additional guidance would be appropriate and why?

89. Are the items identified in Rule 3a71-6 as factors the Commission will consider prior to making a substituted compliance determination in connection with proposed Rule 10, Form SCIR, and the related record preservation requirements appropriate? If so, explain why. If not, explain why not. Should any of those items be modified or deleted? Should additional considerations be added? If so, please explain.

E. Amendments to Rule 18a-10

1. Proposal

Exchange Act Rule 18a-10 ("Rule 18a-10") permits an SBSD that is registered as a swap dealer and predominantly engages in a swaps business to elect to comply with the capital, margin, segregation, recordkeeping, and reporting requirements of the Commodity Exchange Act

and the CFTC's rules in lieu of complying with the capital, margin, segregation, recordkeeping, and reporting requirements of Exchange Act Rules 18a-1, 18a-3, 18a-4, 18a-5, 18a-6, 18a-7, 18a-8, and 18a-9.[459] An SBSD may elect to operate pursuant to Rule 18a-10 if it meets certain conditions.[460] First, the firm must be registered with the Commission as a stand-alone SBSD (*i.e.*, not also registered as a broker-dealer or an OTC derivatives dealer) and registered with the CFTC as a swap dealer. Second, the firm must be exempt from the segregation requirements of Rule 18a-4. Third, the aggregate gross notional amount of the firm's outstanding security-based swap positions must not exceed the lesser of two thresholds as of the most recently ended quarter of the firm's fiscal year.[461] The thresholds are: (1) a maximum fixed-dollar gross notional amount of open security-based swaps of $250 billion;[462] and (2) 10% of the combined aggregate gross notional amount of the firm's open security-based swap and swap positions.

As discussed above, Rule 18a-6 is proposed to be amended to require SBSDs to maintain and preserve the records required to be made pursuant to proposed Rule 10.[463] However, because Rule 18a-6 is within the scope of Rule 18a-10, an SBSD operating pursuant to Rule 18a-10 would not be subject to the maintenance and preservation requirements of Rule 18a-6 with respect to the records required to be made pursuant to proposed Rule 10. Therefore, while an SBSD would be subject to proposed Rule 10 and need to make these records, the firm would not need to maintain or preserve them in accordance with Rule 18a-6. For these reasons, the Commission is proposing to amend Rule 18a-10 to exclude from its scope the record

---

459 *See* 17 CFR 240.18a-10.

460 *See* Capital, Margin, and Segregation Requirements Adopting Release, 84 at 43944-46 (discussing the conditions and the reasons for them). *See also* SBS Entity Recordkeeping and Reporting Adopting Release 84 FR at 68549.

461 The gross notional amount is based on the notional amounts of the firm's security-based swaps and swaps that are outstanding as of the quarter end. It is not based on transaction volume during the quarter.

462 The maximum fixed-dollar threshold of $250 billion is set for a transition period of 3 years from the compliance date of the rule. Three years after that date it will drop to $50 billion (unless the Commission issues an order retaining the $250 billion threshold or lesser amount that is greater than $50 billion).

463 *See* section II.B.5. of this release (discussing these proposals in more detail).

maintenance and preservation requirements of Rule 18a-6 as they pertain to the records required to be made pursuant to proposed Rule 10.[464] Therefore, the records required to be made pursuant to proposed Rule 10 would need to be preserved and maintained in accordance with Rule 18a-6, as it is proposed to be amended.

2. Request for Comment

The Commission requests comment on all aspects of the proposed amendments relating to Rule 18a-10. In addition, the Commission is requesting comment on the following specific aspects of the proposals:

90. Should the proposed amendments to Rule 18a-10 be modified? If so, describe how and explain why the modification would be appropriate. For example, would the records required to be made pursuant to proposed Rule 10 be subject to CFTC record preservation and maintenance rules? If so, identify the rules and explain the preservation and maintenance requirements they would impose on the records required to be made pursuant to proposed Rule 10. In addition, explain whether it would be appropriate to permit an SBSD operating pursuant to Rule 18a-10 to comply with these CFTC rules in terms of preserving and maintaining the records required to be made pursuant to proposed Rule 10 in lieu of the complying with the preservation and maintenance requirements that would apply to the records under the proposed amendments to Rule 18a-6.

F. Market Entities Subject to Regulation SCI, Regulation S-P, Regulation ATS, and Regulation S-ID

1. Discussion

---

464 *See* proposed paragraph (g) of Rule 18a-10.

a. Introduction

As discussed in more detail below, certain types of Market Entities are subject to Regulation SCI and Regulation S-P.[465] The Commission separately is proposing to amend Regulation SCI and Regulation S-P.[466] Regulation SCI and Regulation S-P (currently and as they would be amended) have or would have provisions requiring policies and procedures that address certain types of cybersecurity risks.[467] Regulation SCI (currently and as it would be amended) also requires immediate written or telephonic notice and subsequent reporting to the Commission on Form SCI of certain types of incidents.[468] These notification and subsequent reporting requirements of Regulation SCI could be triggered by a "significant cybersecurity incident" as that term would be defined in proposed Rule 10.[469] Finally, Regulation SCI and Regulation S-P (currently and as they would be amended) have or would have provisions requiring disclosures to persons affected by certain incidents.[470] These current or proposed disclosure requirements of Regulation SCI and Regulation S-P could be triggered by a cybersecurity-related event that also would be a "significant cybersecurity incident" as that term would be defined in proposed Rule 10.[471] Consequently, if proposed Rule 10 is adopted (as proposed), Market Entities could be subject to requirements in that rule and in Regulation SCI and Regulation S-P that pertain to cybersecurity. While the Commission preliminarily believes that these requirements are nonetheless appropriate, it is seeking comment on the proposed

---

465 *See* 17 CFR 242.1000 through 1007 (Regulation SCI); 17 CFR 248.1 through 248.30 (Regulation S-P). *See also* section II.F.1.b. of this release (discussing the types of Market Entities that are or would be subject to Regulation SCI and/or Regulation S-P).

466 *See* Regulation SCI 2023 Proposing Release; Regulation S-P 2023 Proposing Release.

467 *See* section II.F.1.c. of this release (discussing the existing and proposed requirements of Regulation SCI and Regulation S-P to have policies and procedures that address certain cybersecurity risks).

468 *See* section II.F.1.d. of this release (discussing the existing and proposed immediate notification and subsequent reporting requirements of Regulation SCI).

469 *See* paragraph (a)(10) of proposed Rule 10 (defining the term "significant cybersecurity incident").

470 *See* section II.F.1.e. of this release (discussing the existing and proposed disclosure requirements of Regulation SCI and Regulation S-P).

471 *See* paragraph (a)(10) of proposed Rule 10 (defining the term "significant cybersecurity incident").

amendments, given the following: (1) each proposal has a different scope and purpose; (2) the policies and procedures related to cybersecurity that would be required under each of the proposed rules would be consistent; (3) the public disclosures or notifications required by the proposed rules would require different types of information to be disclosed, largely to different audiences at different times; and (4) it should be appropriate for entities to comply with the proposed requirements.

The Commission encourages interested persons to provide comments on the discussion below, as well as on the potential related application of proposed Rule 10, Regulation SCI, and Regulation S-P. More specifically, the Commission encourages commenters: (1) to identify any areas where they believe the requirements of proposed Rule 10 and the existing or proposed requirements of Regulation SCI and Regulation S-P would be particularly costly or create practical implementation difficulties; (2) to provide details on what in particular about implementation would be difficult; and (3) to make recommendations on how to minimize these potential impacts. To assist this effort, the Commission is seeking specific comment below on these topics.[472]

b. Market Entities That Are Or Would Be Subject to Regulation SCI and Regulation S-P

Certain Market Entities that would be subject to the requirements of proposed Rule 10 applicable to Covered Entities are subject to the existing requirements of Regulation SCI. In particular, SCI entities include the following Covered Entities that also would be subject to the requirements of proposed Rule 10: (1) ATSs that trade certain stocks exceeding specific volume thresholds; (2) registered clearing agencies; (3) certain exempt clearing agencies; (4) the MSRB; (5) FINRA; and (6) national securities exchanges.[473] Therefore, if proposed Rule 10 is adopted

---

472 *See* section II.F.2. of this release.

473 *See* 17 CFR 242.1000 (defining the terms "SCI alternative trading system," "SCI self-regulatory system," and "Exempt clearing agency subject to ARP," and including all of those defined terms in the definition of

(as proposed), these Covered Entities would be subject to its requirements and the requirements of Regulation SCI (currently and as it would be amended). The Commission is separately proposing to revise Regulation SCI to expand the definition of "SCI entity" to include the following Covered Entities that also would be subject to the requirements of proposed Rule 10: (1) broker-dealers that exceed an asset-based size threshold or a volume-based trading threshold in NMS stocks, exchange-listed options, agency securities, or U.S. treasury securities; (2) *all* exempt clearing agencies; and (3) SBSDRs.[474] Therefore, if these amendments to Regulation SCI are adopted and proposed Rule 10 is adopted (as proposed), these additional Covered Entities would be subject to the requirements of proposed Rule 10 and also to the requirements of Regulation SCI. Additionally, broker-dealers and transfer agents that would be subject to proposed Rule 10 also would be subject to some or all of the existing or proposed requirements of Regulation S-P.[475]

"SCI Entity"). The definition of "SCI entities" includes additional Commission registrants that would not be subject to the requirements of proposed Rule 10: plan processors and SCI competing consolidators. However, the Commission is seeking comment on whether these registrants should be subject to the requirements of proposed Rule 10.

474 All exempt clearing agencies and SBSDRs would be subject to the requirements of proposed Rule 10 applicable to Covered Entities. *See* paragraphs (a)(1)(ii) and (vii) of proposed Rule 10 (defining these registrants as "covered entities"). Broker-dealers that exceed the asset-based size threshold under the proposed amendments to Regulation SCI (which would be several hundred billion dollars) also would be subject to the requirements of proposed Rule 10 applicable to Covered Entities, as they would exceed the $1 billion total assets threshold in the broker-dealer definition of "covered entity." *See* paragraph (a)(1)(i)(D) of proposed Rule 10. A broker-dealer that exceeds one or more of the volume-based trading thresholds under the proposed amendments to Regulation SCI likely would meet one of the broker-dealer definitions of "covered entity" in proposed Rule 10 given their size and activities. For example, it would either be a carrying broker-dealer, have regulatory capital equal to or exceeding $50 million, have total assets equal to or exceeding $1 billion, or operate as a market maker. *See* paragraphs (a)(1)(i)(A), (C), (D), and (E) of proposed Rule 10. The Commission is seeking comment above on whether a broker-dealer that is an SCI entity should be defined specifically as a "covered entity" under proposed Rule 10.

475 Broadly, Regulation S-P's requirements apply to all broker-dealers, except for "notice-registered broker-dealers" (as defined in 17 CFR 248.30), who in most cases will be deemed to be in compliance with Regulation S-P if they instead comply with the financial privacy rules of the CFTC, and are otherwise explicitly excluded from certain of Regulation S-P's obligations. *See* 17 CFR 248.2(c). For the purposes of this section II.F. of this release, the term "broker-dealer" when used to refer to broker-dealers that are subject to Regulation S-P (currently and as it would be amended) excludes notice-registered broker-dealers. Currently, transfer agents registered with the Commission ("SEC-registered transfer agents") (but not transfer agents registered with another appropriate regulatory agency) are subject to Regulation S-P's "disposal rule" ("Regulation S-P Disposal Rule"). *See* 17 CFR 248.30(b). However, no transfer agent is currently subject to any other portion of Regulation S-P, including the "safeguards rule" under Regulation

c. Policies and Procedures to Address Cybersecurity Risks

i. Different Scope and Purpose of the Policies and Procedures Requirements

Each of the policies and procedures requirements has a different scope and purpose. Regulation SCI (currently and as it would be amended) limits the scope of its requirements to certain systems of the SCI Entity that support securities market related functions. Specifically, it does and would require an SCI Entity to have reasonably designed policies and procedures applicable to its SCI systems and, for purposes of security standards, its indirect SCI systems.[476] While certain aspects of the policies and procedures required by Regulation SCI (as it exists today and as proposed to be amended) are designed to address certain cybersecurity risks (among other things),[477] the policies and procedures required by Regulation SCI focus on the SCI entities' operational capability and the maintenance of fair and orderly markets.

S-P ("Regulation S-P Safeguards Rule"). *See* 17 CFR 248.30(a). Under the proposed amendments to Regulation S-P, SEC-registered transfer agents and transfer agents registered with another appropriate regulatory agency (as defined in 15 USC 78c(34)(B)) would be subject to the Regulation S-P Safeguards Rule and the Regulation S-P Disposal Rule. Regulation S-P also applies to additional financial institutions that would not be subject to proposed Rule 10. *See* 17 CFR 248.3.

476 *See* 17 CFR 242.1001(a)(1). "SCI systems" are defined as electronic or similar systems of, or operated by or on behalf of, an SCI entity that directly support at least one of six market functions: (1) trading; (2) clearance and settlement; (3) order routing; (4) market data; (5) market regulation; or (6) market surveillance. 17 CFR 242.1000. "Indirect SCI systems" are defined as those 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. 17 CFR 242.1000. The distinction between SCI systems and indirect SCI systems seeks to encourage SCI Entities that their SCI systems, which are core market-facing systems, should be physically or logically separated from systems that perform other functions (*e.g.*, corporate email and general office systems for member regulation and recordkeeping). *See Regulation Systems Compliance and Integrity*, Release No. 34-73639 79 FR 72251 (Dec. 5, 2014), at 79 FR at 72279-81 ("Regulation SCI 2014 Adopting Release"). Indirect SCI systems are subject to Regulation SCI's requirements with respect to security standards. Further, "critical SCI systems" (a subset of SCI systems) are defined as those that directly support functionality relating to: (1) clearance and settlement systems of clearing agencies; (2) openings, reopenings, and closings on the primary listing market; (3) trading halts; (4) initial public offerings; (5) the provision of market data by a plan processor; or (6) exclusively-listed securities; and as a catchall, systems that provide functionality to the securities markets for which the availability of alternatives is significantly limited or nonexistent and without which there would be a material impact on fair and orderly markets. 17 CFR 242.1000.

477 *See* 17 CFR 242.1000 (defining "indirect SCI systems"). The distinction between SCI systems and indirect SCI systems seeks to encourage SCI Entities that their SCI systems, which are core market-facing systems, should be physically or logically separated from systems that perform other functions (*e.g.*, corporate email and general office systems for member regulation and recordkeeping). *See* Regulation SCI 2014 Adopting Release, 79 FR at 72279-81. Indirect SCI systems are subject to Regulation SCI's requirements with respect to security standards.

Similarly, Regulation S-P (currently and as it would be amended) also has a distinct focus. The policies and procedures required under Regulation S-P, both currently and as proposed to be amended, are limited to protecting a certain type of information—customer records or information and consumer report information[478]—and they apply to such information even when stored outside of SCI systems or indirect SCI systems. Furthermore, these policies and procedures need not address other types of information stored on the systems of the broker-dealer or transfer agent.

Proposed Rule 10 would have a broader scope than Regulation SCI and Regulation S-P (currently and as they would be amended) because it would require Market Entities to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks.[479] Unlike Regulation SCI, these requirements would therefore cover SCI systems, indirect SCI systems, and information systems that are not SCI systems or indirect SCI systems. And, unlike Regulation S-P, the proposed requirements would also encompass information beyond customer information and consumer information.

To illustrate, a Market Entity could use one comprehensive set of policies and procedures to satisfy the requirements of proposed Rule 10 and the existing and proposed cybersecurity-related requirements of Regulation SCI and Regulation S-P, so long as: (1) the cybersecurity-related policies and procedures required under Regulation S-P and Regulation SCI fit within and are consistent with the scope of the policies and procedures required under proposed Rule 10; and (2) and the policies and procedures requirements of proposed Rule 10 also address the more narrowly-focused existing and proposed cybersecurity-related policies and procedures requirements under Regulation SCI and Regulation S-P.

---

478 Or as proposed herein, "customer information" and "consumer information." *See* proposed rules 248.30(e)(5) and (e)(1), respectively.

479 *See* paragraphs (b) and (e) of proposed Rule 10 (setting forth the requirements of Covered Entities and Non-Covered Entities, respectively, to have policies and procedures to address their cybersecurity risks).

ii. Consistency of the Policies and Procedures Requirements

Covered Entities

As discussed above, the Market Entities that would be SCI Entities under the existing and proposed requirements of Regulation SCI would be subject the policies and procedures requirements of proposed Rule 10 applicable to Covered Entities. In addition, broker-dealers and transfer agents are subject to the requirements of Regulation S-P (currently and as it would be amended).[480] Transfer agents would be Covered Entities under proposed Rule 10 and, therefore, subject to the policies and procedures requirements of that rule applicable to Covered Entities.[481] Further, the two categories of broker-dealers that likely would have the largest volume of customer information and consumer information subject to the existing or proposed requirements of Regulation S-P would be Covered Entities under proposed Rule 10: carrying broker-dealers and introducing broker-dealers.[482] For these reasons, the Commission first analyzes the potential overlap between proposed Rule 10 and the current and proposed requirements of Regulation SCI and Regulation S-P by taking into account the policies and procedures requirements of proposed Rule 10 that would apply to Covered Entities.

Regulation SCI and Regulation S-P General Policies and Procedures Requirements.

Regulation SCI, Regulation S-P, and proposed Rule 10 all include requirements that address certain cybersecurity-related risks. Regulation SCI requires an SCI Entity to have reasonably designed policies and procedures to ensure that its SCI systems and, for purposes of security standards, indirect SCI systems, have levels of capacity, integrity, resiliency,

---

480 As discussed above, SEC-registered transfer agents are subject to the Regulation S-P Disposal Rule but not to the Regulation S-P Safeguards Rule. The proposed amendments to Regulation S-P would apply the Regulation S-P Safeguards Rule and the Regulation S-P Disposal Rule to all transfer agents.

481 *See* paragraph (b)(1) of proposed Rule 10 (setting forth the policies and procedures requirements for Covered Entities).

482 *See* paragraphs (a)(1)(i)(A) and (B) of proposed Rule 10 (defining, respectively, carrying broker-dealers and introducing broker-dealers as Covered Entities).

availability, and security, adequate to maintain the SCI entity's operational capability and promote the maintenance of fair and orderly markets.[483]

The Regulation S-P Safeguards Rule requires broker-dealers (but not transfer agents) to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information.[484] The Regulation S-P Safeguards Rule further provides that these policies and procedures must: (1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.[485] Additionally, the Regulation S-P Disposal Rule requires broker-dealers *and* SEC-registered transfer agents that maintain or otherwise possess consumer report information for a business purpose to properly dispose of the information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.[486]

Proposed Rule 10 would require a Covered Entity to establish, maintain, and enforce written policies and procedures that are reasonably designed to address the Covered Entity's cybersecurity risks. In addition, Covered Entities would be required to include the following elements in their policies and procedures: (1) periodic assessments of cybersecurity risks associated with the Covered Entity's information systems and written documentation of the risk assessments; (2) controls designed to minimize user-related risks and prevent unauthorized access to the Covered Entity's information systems; (3) measures designed to monitor the

---

483 *See* 17 CFR 242.1001(a)(1).

484 *See* 17 CFR 248.30(a).

485 *See* 17 CFR 248.30(a)(1) through (3).

486 *See* 17 CFR 248.30(b)(2). Regulation S-P currently defines the term "disposal" to mean: (1) the discarding or abandonment of consumer report information; or (2) the sale, donation, or transfer of any medium, including computer equipment, on which consumer report information is stored. *See* 17 CFR 248.30(b)(1)(iii).

Covered Entity's information systems and protect the Covered Entity's information from unauthorized access or use, and oversight of service providers that receive, maintain, or process information, or are otherwise permitted to access the Covered Entity's information systems; (4) measures to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the Covered Entity's information systems; and (5) measures to detect, respond to, and recover from a cybersecurity incident and written documentation of any cybersecurity incident and the response to and recovery from the incident.[487]

As discussed earlier, the inclusion of these elements in proposed Rule 10 is designed to enumerate the core areas that Covered Entities would need to address when designing, implementing, and assessing their policies and procedures.[488] Taken together, these requirements are designed to position Covered Entities to be better prepared to protect themselves against cybersecurity risks, to mitigate cybersecurity threats and vulnerabilities, and to recover from cybersecurity incidents. They are also designed to help ensure that Covered Entities focus their efforts and resources on the cybersecurity risks associated with their operations and business practices.

A Covered Entity that implements reasonably designed policies and procedures in compliance with the requirements of proposed Rule 10 described above that cover its SCI systems and indirect SCI systems should generally satisfy the existing general policies and procedures requirements of Regulation SCI that pertain to cybersecurity.[489] Similarly, policies

---

487 *See* sections II.B.1.a. through II.B.1.e. of this release (discussing these proposed requirements in more detail).

488 *See* section II.B.1. of this release.

489 As noted above, the CAT System is a facility of each of the Participants and an SCI system. *See also* CAT NMS Plan Approval Order, 81 FR at 84758. It would also qualify as an "information system" of each national securities exchange and each national securities association under proposed Rule 10. The CAT NMS Plan requires the CAT's Plan Processor to follow certain security protocols and industry standards, including the NIST Cyber Security Framework, subject to Participant oversight. *See, e.g.*, CAT NMS Plan at appendix D, section 4.2. For the reasons discussed above and below with respect to SCI systems, the policies and procedures requirements of proposed Rule 10 are not intended to be inconsistent with the

and procedures implemented by a Covered Broker-Dealer that are reasonably designed in compliance with the requirements of proposed Rule 10 should generally satisfy the existing general policies and procedures requirements of the Regulation S-P Safeguards Rule discussed above that pertain to cybersecurity, to the extent that such information is stored electronically and, therefore, falls within the scope of proposed Rule 10. In addition, reasonably designed policies and procedures implemented by a Covered Broker-Dealer or SEC-registered transfer agent in compliance with the requirements of proposed Rule 10 should generally satisfy the existing requirements of the Regulation S-P Disposal Rule discussed above.

Regulation SCI and Regulation S-P Requirements to Oversee Service Providers. Under the amendments to Regulation SCI, the policies and procedures required of SCI entities would need to include a program to manage and oversee third party providers that provide functionality, support or service, directly or indirectly, for SCI systems and indirect SCI systems.[490] In addition, proposed amendments to the Regulation S-P Safeguards Rule would require broker-dealers and transfer agents to include written policies and procedures within their response programs that require their service providers, pursuant to a written contract, to take appropriate measures that are designed to protect against unauthorized access to or use of customer information, including notification to the broker-dealer or transfer agent as soon as possible, but no later than 48 hours after becoming aware of a breach, in the event of any breach in security

---

security protocols set forth in the CAT NMS Plan. Moreover, to the extent the CAT NMS Plan requires security protocols beyond those that would be required under proposed Rule 10, those additional security protocols should generally fit within and be consistent with the policies and procedures required under proposed Rule 10 to address all cybersecurity risks.

490 *See* Regulation SCI 2023 Proposing Release. These policies and procedures would need to include initial and periodic review of contracts with such vendors for consistency with the SCI entity's obligations under Regulation SCI; and a risk-based assessment of each third party provider's criticality to the SCI entity, including analyses of third party provider concentration, of key dependencies if the third party provider's functionality, support, or service were to become unavailable or materially impaired, and of any potential security, including cybersecurity, risks posed. *Id.*

resulting in unauthorized access to customer information maintained by the service provider to enable the broker-dealer or transfer agent to implement its response program expeditiously.[491]

Proposed Rule 10 would have several policies and procedures requirements that are designed to address similar cybersecurity risks as these proposed amendments to Regulation SCI and Regulation S-P. First, a Covered Entity's policies and procedures under proposed Rule 10 would need to require periodic assessments of cybersecurity risks associated with the Covered Entity's information systems and information residing on those systems.[492] This element of the policies and procedures would need to include requirements that the Covered Entity identify its service providers that receive, maintain, or process information, or are otherwise permitted to access its information systems and any of its information residing on those systems, and assess the cybersecurity risks associated with its use of these service providers.[493] Second, under proposed Rule 10, a Covered Entity's policies and procedures would need to require oversight of service providers that receive, maintain, or process its information, or are otherwise permitted to access its information systems and the information residing on those systems, pursuant to a written contract between the Covered Entity and the service provider, through which the service providers would need to be required to implement and maintain appropriate measures that are designed to protect the Covered Entity's information systems and information residing on those systems.[494]

A Covered Entity that implements these requirements of proposed Rule 10 with respect to its SCI systems and indirect SCI systems generally should satisfy the proposed requirements of Regulation SCI that the SCI entity's policies and procedures include a program to manage and

---

491 *See* Regulation S-P 2023 Proposing Release.

492 *See* paragraph (b)(1)(i)(A) of proposed Rule 10; *see also* section II.B.1.a. of this release (discussing this requirement in more detail).

493 *See* paragraph (b)(1)(i)(A)(*2*) of proposed Rule 10.

494 *See* paragraphs (b)(1)(iii)(B) of proposed Rule 10; *see also* section II.B.1.c. of this release (discussing this requirement in more detail).

oversee third party providers that provide functionality, support or service, directly or indirectly, for SCI systems and indirect SCI systems. Similarly, a broker-dealer or transfer agent that implements these requirements of proposed Rule 10 generally would comply with the proposed requirements of the Regulation S-P Safeguards Rule relating to the oversight of service providers.

Regulation SCI and Regulation S-P Unauthorized Access Requirements. Under the proposed amendments to Regulation SCI, SCI entities would be required to have a program to prevent the unauthorized access to their SCI systems and indirect SCI systems, and information residing therein.[495] The proposed amendments to the Regulation S-P Disposal Rule would require broker-dealers and transfer agents that maintain or otherwise possess consumer information or customer information for a business purpose to properly dispose of this information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.[496] The broker-dealer or transfer agent would be required to adopt and implement written policies and procedures that address the proper disposal of consumer information and customer information in accordance with this standard.[497]

Proposed Rule 10 would have several policies and procedures requirements that are designed to address similar cybersecurity-related risks as these proposed requirements of Regulation SCI and the Regulation S-P Disposal Rule. First, a Covered Entity's policies and procedures under proposed Rule 10 would need to require controls: (1) requiring standards of behavior for individuals authorized to access the Covered Entity's information systems and the information residing on those systems, such as an acceptable use policy; (2) identifying and

---

495 *See* Regulation SCI 2023 Proposing Release.

496 *See* Regulation S-P 2023 Proposing Release. As discussed above, the general policies and procedures requirements of the Regulation S-P Safeguards Rule require the policies and procedures—among other things—to protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer. *See* 17 CFR 248.30(a)(3).

497 *See* Regulation S-P 2023 Proposing Release.

authenticating individual users, including but not limited to implementing authentication measures that require users to present a combination of two or more credentials for access verification; (3) establishing procedures for the timely distribution, replacement, and revocation of passwords or methods of authentication; (4) restricting access to specific information systems of the Covered Entity or components thereof and the information residing on those systems solely to individuals requiring access to the systems and information as is necessary for them to perform their responsibilities and functions on behalf of the Covered Entity; and (5) securing remote access technologies.[498]

Second, under proposed Rule 10, a Covered Entity's policies and procedures would need to include measures designed to protect the Covered Entity's information systems and protect the information residing on those systems from unauthorized access or use, based on a periodic assessment of the Covered Entity's information systems and the information that resides on the systems.[499] The periodic assessment would need to take into account: (1) the sensitivity level and importance of the information to the Covered Entity's business operations; (2) whether any of the information is personal information; (3) where and how the information is accessed, stored and transmitted, including the monitoring of information in transmission; (4) the information systems' access controls and malware protection; and (5) the potential effect a cybersecurity incident involving the information could have on the Covered Entity and its customers, counterparties, members, registrants, or users, including the potential to cause a significant cybersecurity incident.[500]

A Covered Entity that implements these requirements of proposed Rule 10 with respect to its SCI systems and indirect SCI systems generally should satisfy the proposed requirements

---

498 *See* paragraphs (b)(1)(ii)(A) through (E) of proposed Rule 10; *see also* section II.B.1.b. of this release (discussing these requirements in more detail).

499 *See* paragraph (b)(1)(iii)(A) of proposed Rule 10; *see also* section II.B.1.c. of this release (discussing these requirements in more detail).

500 *See* paragraphs (b)(1)(iii)(A)(*1*) through (*5*) of proposed Rule 10.

of Regulation SCI that the SCI entity's policies and procedures include a program to prevent the unauthorized access to their SCI systems and indirect SCI systems, and information residing therein. Similarly, a broker-dealer or transfer agent that implements these requirements of proposed Rule 10 should generally satisfy the proposed requirements of the Regulation S-P Disposal Rule to adopt and implement written policies and procedures that address the proper disposal of consumer information and customer information.

Regulation SCI and Regulation S-P Response Programs. Regulation SCI requires SCI entities to have policies and procedures to monitor its SCI systems and indirect SCI systems for SCI events, which include systems intrusions for unauthorized access, and also requires them to have policies and procedures that include escalation procedures to quickly inform responsible SCI personnel of potential SCI events.[501]

The amendments to Regulation S-P's safeguards provisions would require the policies and procedures to include a response program for unauthorized access to or use of customer information. Further, the response program would need to be reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, including procedures, among others: (1) to assess the nature and scope of any incident involving unauthorized access to or use of customer information and identify the customer information systems and types of customer information that may have been accessed or used without authorization;[502] and (2) to take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information.[503]

---

501 *See* 17 CFR 242.1001(a)(2)(vii) and (c)(1), respectively.

502 Regulation SCI's obligation to take corrective action may include a variety of actions, such as determining the scope of the SCI event and its causes, among others. *See* Regulation SCI 2014 Adopting Release, 79 FR at 72251, 72317. *See also* 17 CFR 242.1002(a).

503 *See* Regulation S-P 2023 Proposing Release. The response program also would need to have procedures to notify each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization unless the covered institution determines, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information, the sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience. *See id.*

The amendments to the Regulation S-P Safeguards Rule would require the policies and procedures to include a response program for unauthorized access to or use of customer information. Further, the response program would need to be reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information, including procedures, among others: (1) to assess the nature and scope of any incident involving unauthorized access to or use of customer information and identify the customer information systems and types of customer information that may have been accessed or used without authorization; and (2) to take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information.[504]

Proposed Rule 10 would have several policies and procedures requirements that are designed to address similar cybersecurity-related risks as these proposed requirements of the Regulation S-P Safeguards Rule. First, under proposed Rule 10, a Covered Entity's policies and procedures would need to require measures designed to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the Covered Entity's information systems and the information residing on those systems.[505] Second, under proposed Rule 10, a Covered Entity's policies and procedures would need to have measures designed to detect, respond to, and recover from a cybersecurity incident, including policies and procedures that are reasonably designed to ensure (among other things): (1) the continued operations of the Covered Entity; (2) the protection of the Covered Entity's information systems and the information

---

504 *See* Regulation S-P 2023 Proposing Release. As discussed below, the response program also would need to have procedures to notify each affected individual whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization unless the covered institution determines, after a reasonable investigation of the facts and circumstances of the incident of unauthorized access to or use of sensitive customer information, the sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience. *See id.*

505 *See* paragraph (b)(1)(iv) of proposed Rule 10; *see also* section II.B.1.d. of this release (discussing this requirement in more detail).

residing on those systems; and (3) external and internal cybersecurity incident information sharing and communications.[506]

A Covered Entity that implements reasonably designed policies and procedures in compliance with these requirements of proposed Rule 10 generally should satisfy the proposed requirements of the Regulation SCI and Regulation S-P Safeguards Rule to have a response program relating to response programs for unauthorized access.

Regulation SCI Review Requirements. Regulation SCI currently prescribes certain elements that must be included in each SCI entity's policies and procedures.[507] These required elements include policies and procedures that must provide for regular reviews and testing of SCI systems and indirect SCI systems, including backup systems, to identify vulnerabilities from internal and external threats.[508] In addition, Regulation SCI requires SCI entities to conduct penetration tests as part of a review of their compliance with Regulation SCI.[509] While these reviews must be conducted not less than once each calendar year, the penetration tests currently need to be conducted not less than once every three years.[510] The amendments to Regulation SCI would increase the required frequency of the penetration tests to not less than once each calendar year.[511] The amendments to Regulation SCI also would require that the penetration tests include tests of any vulnerabilities of the SCI entity's SCI systems and indirect SCI systems identified under the existing requirement to perform regular reviews and testing of SCI systems and indirect SCI systems, including backup systems, to identify vulnerabilities from internal and external threats.[512]

---

506 *See* paragraph (b)(1)(v) of proposed Rule 10; *see also* section II.B.1.e. of this release (discussing this requirement in more detail).

507 *See* 17 CFR 242.1001(a)(2).

508 17 CFR 242.1001(a)(2)(iv).

509 *See* 17 CFR 242.1003(b)(1)(i).

510 *Id.*

511 *See* Regulation SCI 2023 Proposing Release.

512 *See* Regulation SCI 2023 Proposing Release; 17 CFR 242.1001(a)(2)(iv).

Proposed Rule 10 would have several policies and procedures requirements that are designed to address similar cybersecurity-related risks as these existing and proposed requirements of Regulation SCI. First, a Covered Entity's policies and procedures under proposed Rule 10 would need to require periodic assessments of cybersecurity risks associated with the Covered Entity's information systems and information residing on those systems.[513] Moreover, this element of the policies and procedures would need to include requirements that the Covered Entity categorize and prioritize cybersecurity risks based on an inventory of the components of the Covered Entity's information systems and information residing on those systems and the potential effect of a cybersecurity incident on the Covered Entity.[514] Second, under proposed Rule 10, a Covered Entity's policies and procedures would need to require measures designed to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the Covered Entity's information systems and the information residing on those systems.[515]

A Covered Entity that implements these requirements of proposed Rule 10 with respect to its SCI systems and indirect SCI systems generally should satisfy the current requirements of Regulation SCI that the SCI entity's policies and procedures require regular reviews and testing of SCI systems and indirect SCI systems, including backup systems, to identify vulnerabilities from internal and external threats.

Further, while proposed Rule 10 does not require penetration testing, the proposed rule—as discussed above—requires measures designed to protect the Covered Entity's information systems and protect the information residing on those systems from unauthorized access or use, based on a periodic assessment of the Covered Entity's information systems and the information

---

513 *See* paragraph (b)(1)(i)(A) of proposed Rule 10; *see also* section II.B.1.a. of this release (discussing this requirement in more detail).

514 *See* paragraph (b)(1)(i)(A)(*1*) of proposed Rule 10.

515 *See* paragraph (b)(1)(iv) of proposed Rule 10; *see also* section II.B.1.d. of this release (discussing this requirement in more detail).

that resides on the systems.[516] As discussed earlier, penetration testing could be part of these measures.[517] Therefore, the existing and proposed requirements of Regulation SCI requiring penetration testing could be incorporated into and should fit within a Covered Entity's policies and procedures to address cybersecurity risks under proposed Rule 10.

Non-Covered Broker-Dealers

Non-Covered Broker-Dealers—which would be subject to Regulation S-P but not Regulation SCI—are smaller firms whose functions do not play as significant a role in the U.S. securities markets, as compared to Covered Broker-Dealers.[518] For example, Non-Covered Broker-Dealers tend to offer a more focused and limited set of services such as facilitating private placements of securities, selling mutual funds and variable contracts, underwriting securities, and participating in direct investment offerings.[519] Further, they do not hold customer securities and cash or serve as a conduit (*i.e.*, an introducing broker-dealer) for customers to access their accounts at a carrying broker-dealer that holds the customers' securities and cash. If these Non-Covered Broker-Dealers do not possess or maintain any customer information or consumer information for a business purpose in connection with the services they provide, they would not be subject to either the current or proposed requirements of Regulation S-P, including those that pertain to cybersecurity.

---

516 *See* paragraph (b)(1)(iii)(A) of proposed Rule 10.

517 *See also* section II.B.1.c. of this release. The Commission also is requesting comment above on whether proposed Rule 10 should be modified to specifically require penetration testing.

518 *See* section IV.C.2. of this release (discussing the activities of broker-dealers that would not meet the definition of "covered entity" in proposed Rule 10). As discussed below in section IV.C.2. of this release, the 1,541 broker-dealers that would meet the definition of "covered entity" in proposed Rule 10 had average total assets of $3.5 billion and average regulatory equity of $325 million; whereas the 1,969 that would not meet the definition of "covered entity" had average total assets of $4.7 million and regulatory equity of $3 million. This means that broker-dealers that would not meet the definition of "covered entity" in proposed Rule 10 accounted for about 0.2% of the total assets of all broker-dealers and 0.1% of total capital for all broker-dealers.

519 *See* section IV.C.2. of this release (discussing the activities of broker-dealers that would not meet the definition of "covered entity" in proposed Rule 10).

However, Non-Covered Broker-Dealers under proposed Rule 10 that do possess or maintain customer information or consumer information for a business purpose would be subject to the current and proposed requirements of Regulation S-P. Given their smaller size, some of these Non-Covered Broker-Dealers may store and dispose of the information in paper form and, therefore, under the existing and proposed requirements of Regulation S-P would need to address the physical security aspects of storing and disposing of this information. These paper records would not be subject to proposed Rule 10.

Some Non-Covered Broker-Dealers likely would store customer information and consumer information for a business purpose electronically on an information system. Under the existing and proposed requirements of Regulation S-P, these Non-Covered Broker-Dealers would need to address the cybersecurity risks of storing this information on an information system. These Non-Covered Broker-Dealers would be subject the requirements of proposed Rule 10 to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks taking into account the size, business, and operations of the firm.[520] Under proposed Rule 10, they also would be required to review and assess the design and effectiveness of their cybersecurity policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review. This means the Non-Covered Broker-Dealer would need to comprehensively address all of its cybersecurity risks. The policies and procedures to address cybersecurity risks required under proposed Rule 10 would need to address cybersecurity risks involving information systems on which customer information and consumer information is stored. Therefore, complying with this requirement of proposed Rule 10 would be consistent

---

[520] *See* paragraph (e) of proposed Rule 10 (setting forth the policies and procedures requirements for Market Entities that are not broker-dealers). *See also* section II.C. of this release (discussing these proposed requirements in more detail).

with complying with the existing and proposed requirements of Regulation S-P that relate to cybersecurity.

As discussed above, Regulation S-P (currently and as it would be amended) sets forth certain specific requirements that pertain to cybersecurity risk; whereas the requirements of proposed Rule 10 applicable to Non-Covered Broker-Dealers more generally require the firm to establish, maintain, and enforce written policies and procedures that are reasonably designed to address its cybersecurity risks taking into account the size, business, and operations of the firm. As explained above, those more specific existing and proposed requirements of Regulation S-P are consistent with certain of the elements—which are based on industry standards for addressing cybersecurity risk—that Covered Entities would be required to include in their policies and procedures under proposed Rule 10.[521] Further, proposed Rule 10 would require a Non-Covered Broker-Dealer to take into account its size, business, and operations when designing its policies and procedures to address its cybersecurity risks. Storing customer information and consumer information on an information system is the type of operation a Non-Covered Broker-Dealer would need to take into account. Consequently, the specific existing and proposed requirements of Regulation S-P should fit within and be consistent with a Non-Covered Broker-Dealer's reasonably designed policies and procedures to address its cybersecurity risks under proposed Rule 10, including the risks associated with storing customer information and consumer information on an information system.

iii. Regulation ATS and Regulation S-ID

Certain broker-dealers that operate an ATS are subject to Regulation ATS and certain broker-dealers that offer and maintain certain types of accounts for customers are subject to

---

521 *See* section II.B.1. of this release (discussing the policies and procedures requirements for Covered Entities).

requirements of Regulation S-ID to establish an identity theft program.[522] Additionally, SBS Entities and transfer agents could be subject to Regulation S-ID if they are "financial institutions" or "creditors."[523] As discussed below, Regulation ATS and Regulation S-ID are more narrowly focused on certain cybersecurity risks as compared to proposed Rule 10, which focuses on all cybersecurity risks of a Market Entity. In addition, the current requirements of Regulation ATS and Regulation S-ID should fit within and be consistent with the broader policies and procedures required under proposed Rule 10 to address all cybersecurity risks.

Regulation ATS requires certain broker-dealers that operate an ATS to review the vulnerability of its systems and data center computer operations to internal and external threats, physical hazards, and natural disasters if during at least four of the preceding six calendar months, such ATS had: (1) with respect to municipal securities, 20 percent or more of the average daily volume traded in the United States; or (2) with respect to corporate debt securities, 20 percent or more of the average daily volume traded in the United States.[524] Therefore, in addition to other potential systems issues, the broker-dealer would need to address cybersecurity risk of relating to its ATS system. Further, this requirement applies to systems that support order entry, order handling, execution, order routing, transaction reporting, and trade comparison in the particular security.[525] Therefore, it has a narrower focus than proposed Rule 10.

Regulation ATS also requires all broker-dealers that operate an ATS to establish adequate written safeguards and written procedures to protect subscribers' confidential trading

---

522 *See* 17 CFR 242.301 through 304 (conditions to the Regulation ATS exemption); 17 CFR 248.201 and 202 (Regulation S-ID identity theft program requirements).

523 *See* 17 CFR 248.201 and 202. The scope of Regulation S-ID includes any financial institution or creditor, as defined in the Fair Credit Reporting Act (15 U.S.C. 1681) that is required to be "registered under the Securities Exchange Act of 1934." *See* 17 CFR 248.201(a).

524 *See* 17 CFR 242.301(b)(6). Currently, no ATS has crossed the either of the volume-based thresholds and, therefore, no ATS is subject to the requirements pertaining, in part, to cybersecurity. *See also* Amendments Regarding the Definition of "Exchange" and ATSs Release, 87 FR 15496.

525 *See Regulation of Exchanges and Alternative Trading Systems*, Exchange Act Release No. 40760 (Dec. 8, 1998) [63 FR 70844, 70876 (Dec. 22, 1998)].

information.[526] The written safeguards and procedures must include, among other things, limiting access to the confidential trading information of subscribers to those employees of the alternative trading system who are operating the system or responsible for its compliance with these or any other applicable rules.[527] These requirements apply to all broker-dealers that operate an ATS and, as indicated, apply to a narrow set of information stored on their information systems: the confidential trading information of the subscribers to the ATS.

As discussed above, Covered Entities under proposed Rule 10—which would include broker-dealers that operate as an ATS—would be required to establish, maintain, and enforce written policies and procedures that are reasonably designed to address the Covered Entity's cybersecurity risks. In addition, Covered Entities would be required to include the following elements in their policies and procedures: (1) periodic assessments of cybersecurity risks associated with the Covered Entity's information systems and written documentation of the risk assessments; (2) controls designed to minimize user-related risks and prevent unauthorized access to the Covered Entity's information systems; (3) measures designed to monitor the Covered Entity's information systems and protect the Covered Entity's information from unauthorized access or use, and oversight of service providers that receive, maintain, or process information, or are otherwise permitted to access the Covered Entity's information systems; (4) measures to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the Covered Entity's information systems; and (5) measures to detect, respond to, and recover from a cybersecurity incident and written documentation. Consequently, a broker-dealer operates an ATS and that implements reasonably designed policies and procedures in compliance with the requirements of proposed Rule 10 should generally satisfy the current requirements of Regulation ATS to review the vulnerability of its systems and data center

---

526 *See* 17 CFR 242.301(b)(10).

527 *See* 17 CFR 242.301(b)(10)(i)(A).

computer operations to internal and external threats and to protect subscribers' confidential trading information to the extent these requirements pertain to cybersecurity.

Regulation S-ID requires—among other things—a financial institution or creditor within the scope of the regulation that offers or maintains one or more covered accounts to develop and implement a written identity theft prevention program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a *covered account* or any existing *covered account*.[528] Regulation S-ID defines the term "covered account"—in pertinent part—as an account that the financial institution or creditor maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a brokerage account with a broker-dealer, and any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.[529] Therefore, Regulation S-ID is narrowly focused on one cybersecurity risk—identity theft. Identity theft—as discussed earlier—is one of the tactics threat actors use to cause harm after obtaining unauthorized access to personal information.[530] As a cybersecurity risk, Market Entities would need to address it as part of their policies and procedures under proposed Rule 10. Consequently, the requirement of Regulation S-ID should fit within and be consistent with a Market Entity's reasonably designed policies and procedures to address its cybersecurity risks under proposed Rule 10, including the risks associated with identity theft.

d. Notification and Reporting to the Commission

Regulation SCI (currently and as it would be amended) provides the framework for notifying the Commission of SCI events including, among other things, to: immediately notify

---

528 *See* 17 CFR 248.201(d)(1).

529 *See* 17 CFR 248.201(b)(3).

530 *See* section I.A. of this release.

the Commission of the event; provide a written notification on Form SCI within 24 hours that includes a description of the SCI event and the system(s) affected, with other information required to the extent available at the time; provide regular updates regarding the SCI event until the event is resolved; and submit a final detailed written report regarding the SCI event.[531] If proposed Rule 10 is adopted as proposed, it would require Market Entities that are Covered Entities to provide the Commission (and other regulators, if applicable) with immediate written electronic notice of a significant cybersecurity incident affecting the Covered Entity and, thereafter, report and update information about the significant cybersecurity incident by filing Part I of proposed Form SCIR with the Commission (and other regulators, if applicable).[532] Part I of proposed of Form SCIR would elicit information about the significant cybersecurity incident and the Covered Entity's efforts to respond to, and recover from, the incident.

Consequently, a Covered Entity that is also an SCI entity that experiences a significant cybersecurity incident under proposed Rule 10 that also is an SCI event would be required to make two filings for the single incident: one on Part I of proposed Form SCIR and the other on Form SCI. The Covered Entity also would be required to make additional filings on Forms SCIR and SCI pertaining to the significant cybersecurity incident (*i.e.*, to provide updates and final reports). The approach of having two separate notification and reporting programs—one

---

[531] *See* 17 CFR 242.1002(b). An "SCI event" is an event at an SCI entity that is: (1) a "systems disruption," which is an event in an SCI entity's SCI systems that disrupts, or significantly degrades, the normal operation of an SCI system; (2) a "systems intrusion," which is any unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity; or (3) a "systems compliance issue," which is an event at an SCI entity that has caused any SCI system of such entity to operate in a manner that does not comply with the Exchange Act and the rules and regulations thereunder or the entity's rules or governing documents, as applicable. *See* 17 CFR 242.1000 (defining the terms "systems disruption," "system intrusion," and "system compliance issue" and including those terms in the definition of "SCI event"). The amendments to Regulation SCI would broaden the definition of "system intrusion" to include a cybersecurity event that disrupts, or significantly degrades, the normal operation of an SCI system, as well as a material attempted unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity. Regulation SCI 2023 Proposing Release.

[532] *See* paragraphs (c)(1) and (2) of proposed Rule 10 (requiring Covered Entities to provide immediate written notice and subsequent reporting on Part I of proposed Form SCIR of significant cybersecurity incidents); sections II.B.2. and II.B.4. of this release (discussing the requirements of paragraphs (c)(1) and (2) of proposed Rule 10 and Part I of Form SCIR in more detail). Non-Covered Broker-Dealers also would be subject to an immediate written electronic notice requirement under paragraph (e)(2) of proposed Rule 10. However, as discussed above, a Non-Covered Broker-Dealer likely would not be an SCI Entity.

under proposed Rule 10 and the other under Regulation SCI—would be appropriate for the following reasons.

As discussed earlier, certain broker-dealers and all transfer agents would not be SCI entities under the current and proposed requirements of Regulation SCI.[533] Certain of the broker-dealers that are not SCI entities (currently and as it would be amended) would be Covered Entities and all transfer agents would be Covered Entities.[534] In addition, the current and proposed reporting requirements of Regulation SCI are or would be triggered by events impacting SCI systems and indirect SCI systems. The Covered Entities that are or would be SCI entities use and rely on information systems that are not SCI systems or indirect SCI systems under the current and proposed amendments to Regulation SCI. For these reasons, Covered Entities could be impacted by significant cybersecurity incidents that do not trigger the current and proposed notification requirements of Regulation SCI either because they do not meet the current or proposed definitions of "SCI entity" or the significant cybersecurity incident does not meet the current or proposed definitions of "SCI event."

As discussed earlier, the objective of the notification and reporting requirements of proposed Rule 10 is to improve the Commission's ability to monitor and evaluate the effects of a significant cybersecurity incident on Covered Entities and their customers, counterparties, members, registrants, or users, as well as assess the potential risks affecting financial markets more broadly.[535] For this reason, Part I of proposed Form SCIR is tailored to elicit information relating specifically to cybersecurity, such as information relating to the threat actor, and the

---

533 *See* section II.F.1.b. of this release. Currently, broker-dealers that operate as ATSs and trade certain stocks exceeding specific volume thresholds are SCI entities. The proposed amendments to Regulation SCI would expand the definition of "SCI entity" to include broker-dealers that exceed an asset-based size threshold or a volume-based trading threshold in NMS stocks, exchange-listed options, agency securities, or U.S. treasury securities. *See* Regulation SCI 2023 Proposing Release.

534 *See* paragraphs (a)(1)(i)(A) and (F) proposed Rule 10 (defining the categories of broker-dealers that would be Covered Entities); paragraph (a)(1)(ix) proposed Rule 10 (defining transfer agents as "covered entities")

535 *See* section II.B.2.a. of this release.

impact of the incident on any data or personal information that may have been accessed.[536] The Commission and its staff could use the information reported on Part I of Form SCIR to monitor the U.S. securities markets and the Covered Entities that support those markets broadly from a cybersecurity perspective, including identifying cybersecurity threats and trends from a market-wide view. By requiring all Covered Entities to report information about a significant cybersecurity incident on a common form, the information obtained from these filings over time would create a comprehensive set of data of all significant cybersecurity incidents impacting Covered Entities that is based on these entities responding to the same check boxes and questions on the form. This would facilitate analysis of the data, including analysis across different Covered Entities and significant cybersecurity incidents. Eventually, this set of data and the ability to analyze it by searching and sorting how different Covered Entities responded to the same questions on the form could be used to spot common trending risks and vulnerabilities as well as best practices employed by Covered Entities to respond to and recover from significant cybersecurity incidents.

The current and proposed definitions of "SCI event" include events that are not related to significant cybersecurity incidents.[537] For example, under the current and proposed requirements of Regulation SCI, the definition of "SCI event" includes an event in an SCI entity's SCI systems that disrupts, or significantly degrades, the normal operation of an SCI system.[538] Therefore, the definitions are not limited to events in an SCI entity's SCI systems that disrupt, or significantly degrade, the normal operation of an SCI system caused by a significant cybersecurity incident. The information elicited in Form SCI reflects the broader scope of the reporting requirements of Regulation SCI (as compared to the narrower focus of proposed Rule 10 on reporting about

---

536 *See* section II.B.2.b. of this release.

537 *See* 17 CFR 242.1000 (defining the term "SCI event"); Regulation SCI 2023 Proposing Release.

538 *See* 17 CFR 242.1000 (defining the term "system disruption" and including that term in the definition of "SCI event"); Regulation SCI 2023 Proposing Release.

significant cybersecurity incidents). For example, the form requires the SCI entity to identify the type of SCI event: systems compliance issue, systems disruption, and/or systems intrusion. In addition, Form SCI is tailored to elicit information specifically about SCI systems. For example, the form requires the SCI entity to indicate whether the type of SCI system impacted by the SCI event directly supports: (1) trading; (2) clearance and settlement; (3) order routing; (4) market data; (5) market regulation; and/or (6) market surveillance. If the impacted system is a critical SCI system, the SCI entity must indicate whether it directly supports functionality relating to: (1) clearance and settlement systems of clearing agencies; (2) openings, reopenings, and closings on the primary listing market; (3) trading halts; (4) initial public offerings; (5) the provision of consolidated market data; and/or (6) exclusively-listed securities. The form also requires the SCI entity to indicate if the systems that provide functionality to the securities markets for which the availability of alternatives is significantly limited or nonexistent and without which there would be a material impact on fair and orderly markets.

e. Disclosure

Proposed Rule 10 and the existing and proposed requirements of Regulation SCI and the proposed requirements of Regulation S-P also have similar, but distinct, requirements related to notification about certain cybersecurity incidents. Regulation SCI requires that SCI entities disseminate information to their members, participants, or customers (as applicable) regarding SCI events.[539] The proposed amendments to Regulation S-P would require broker-dealers and transfer agents to notify affected individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization.[540] Proposed Rule 10 would require a Covered Entity to make two types of public disclosures relating to cybersecurity

---

539 *See* 17 CFR 242.1002(c).

540 *See* Regulation S-P 2023 Proposing Release. The proposed amendments to Regulation S-P would define "sensitive customer information" to mean any component of customer information alone or in conjunction with any other information, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information. *Id.* The proposed amendments would provide example of sensitive customer information. *Id.*

on Part II of proposed Form SCIR.[541] Covered Entities would be required to make the disclosures by filing Part II of proposed Form SCIR on EDGAR and posting a copy of the filing on their business Internet websites.[542] In addition, a Covered Entity that is either a carrying or introducing broker-dealer would be required to provide a copy of the most recently filed Part II of Form SCIR to a customer as part of the account opening process. Thereafter, the carrying or introducing broker-dealer would need to provide the customer with the most recently filed form annually. The copies of the form would need to be provided to the customer using the same means that the customer elects to receive account statements (*e.g.*, by email or through the postal service). Finally, a Covered Entity would be required to promptly make updated disclosures through each of the methods described above (as applicable) if the information required to be disclosed about cybersecurity risk or significant cybersecurity incidents materially changes, including, in the case of the disclosure about significant cybersecurity incidents, after the occurrence of a new significant cybersecurity incident or when information about a previously disclosed significant cybersecurity incident materially changes.

Consequently, a Covered Entity would—if it experiences a "significant cybersecurity incident"—be required to make updated disclosures under proposed Rule 10 by filing Part II of proposed Form SCIR on EDGAR, posting a copy of the form on its business Internet website, and, in the case of a carrying or introducing broker-dealer, by sending the disclosure to its customers using the same means that the customer elects to receive account statements. Moreover, if Covered Entity is an SCI entity and the significant cybersecurity incident is or would be an SCI event under the current or proposed requirements of Regulation SCI, the Covered Entity also could be required to disseminate certain information about the SCI event to certain of its members, participants, or customers (as applicable). Further, if the Covered Entity

---

541 *See* paragraph (d)(1) of proposed Rule 10.

542 *See* section II.B.3.b. of this release (discussing these proposed requirements in more detail).

is a broker-dealer or transfer agent and, therefore, subject to Regulation S-P (as it is proposed to be amended), the broker-dealer or transfer agent also could be required to notify individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization.

However, despite these similarities, there are distinct differences. First, proposed Rule 10, Regulation SCI, and Regulation S-P (as proposed to be amended) require different types of information to be disclosed. Second, the disclosures, for the most part, would be made to different persons: (1) the public at large in the case of proposed Rule 10;[543] (2) affected members, participants, or customers (as applicable) of the SCI entity in the case of Regulation SCI;[544] and (3) affected individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization or, in some cases, all individuals whose information resides in the customer information system that was accessed or used without authorization in the case of Regulation S-P (as proposed to be amended).

Additionally, the disclosure or notification provided about certain cybersecurity incidents is different under proposed Rule 10 and the existing and/or proposed requirements of Regulation SCI and Regulation S-P, given their distinct goals. For example, the requirement to disclose summary descriptions of certain cybersecurity incidents from the current or previous calendar year publicly on EDGAR, among other methods, under proposed Rule 10 serves a different purpose than: (1) the member, participant, or customer (as applicable) dissemination of information regarding SCI events under Regulation SCI; and (2) the customer notification obligation under the proposed amendments to Regulation S-P, which would provide more

---

543 A carrying broker-dealer would be required to make the disclosures to its customers as well through the means by which they receive account statements.

544 Information regarding major SCI events is and would be required to be disseminated by an SCI entity to all of its members, participants, or customers (as applicable) under the existing and proposed requirements of Regulation SCI. *See* Regulation SCI 2023 Proposing Release.

specific information to individuals affected by a security compromise involving their sensitive customer information, so that those individuals may take remedial actions if they so choose.

2. Request for Comment

The Commission requests comment on the potential duplication or overlap between the requirements of proposed Rule 10, Regulation SCI (as it currently exists and as it is proposed to be amended), and Regulation S-P (as it currently exists and as it is proposed to be amended). In addition, the Commission is requesting comment on the following matters:

91. Should the policies and procedures requirements of proposed Rule 10 be modified to address Market Entities that also would be subject to the existing and proposed requirements of Regulation SCI and/or Regulation S-P? For example, would it be particularly costly or create practical implementation difficulties to apply the requirements of proposed Rule 10 (if it is adopted) to have policies and procedures to address cybersecurity risks to Market Entities even if they also would be subject to requirements to have policies and procedures under Regulation SCI and/or Regulation S P that address certain cybersecurity risks (currently and as they would be amended)? If so, explain why. If not, explain why not. Are there ways the policies and procedures requirements of proposed Rule 10 could be modified to minimize these potential impacts while achieving the separate goals of this proposal to protect participants in the U.S. securities markets and the markets themselves from cybersecurity risks? If so, explain how and suggest specific modifications.

92. Would it be appropriate to modify proposed Rule 10 to exempt SCI systems or indirect SCI systems from its policies and procedures requirements and instead rely on the policies and procedures requirements of Regulation SCI to address cybersecurity risks to these information systems of Covered Entities? If so, explain why. If not, explain why not. What would be the costs and benefits of

this approach? For example, if one set of policies and procedures generally would satisfy the requirements of both rules, would this approach result in incremental costs or benefits? Please explain. Would this approach achieve the objectives of this rulemaking to address cybersecurity risks to Covered Entities, given that Rule 10 is specifically designed to address cybersecurity risks and Regulation SCI is designed to address a broader range of risks to certain information systems? Please explain. Would this approach create practical implementation and compliance complexities insomuch as one set of the Covered Entity's systems would be subject to Regulation SCI (*i.e.*, SCI systems and indirect SCI systems) and the other set would be subject to Rule 10? Please explain. If it would create practical implementation and compliance difficulties, would Covered Entities nonetheless apply separate policies and procedures requirements to their information systems based on whether they are or are not SCI systems and indirect SCI Systems or would they develop a single set of policies and procedures that comprehensively addresses the requirements of Regulation SCI and Rule 10? Please explain. Would a comprehensive set of policies and procedures result in stronger measures to protect SCI systems and indirect SCI systems from cybersecurity risks? Please explain. If so, would this be appropriate given the nature of SCI systems and indirect SCI systems and the roles these systems play in the U.S. securities markets? Please explain.

93. Should the policies and procedures requirements of proposed Rule 10 be modified to address Market Entities that also would be subject to the requirements of Regulation ATS? If so, explain why. If not, explain why not.

94. Should the immediate notification and reporting requirements of proposed Rule 10 be modified to address Covered Entities that also would be subject to the existing and proposed requirements of Regulation SCI? For example, would it be

particularly costly or create practical implementation difficulties to apply the immediate notification and subsequent reporting requirements of proposed Rule 10 and Part I of proposed Form SCIR (if they are adopted) to Covered Entities even if they also would be subject to immediate notification and subsequent reporting requirements under Regulation SCI (as it currently exists and would be amended)? If so, explain why. If not, explain why not. Are there ways the notification and reporting requirements of proposed Rule 10 and Part I of proposed Form SCIR could be modified to minimize these potential impacts while achieving the separate goals of this proposal to protect participants in the U.S. securities markets and the markets themselves from cybersecurity risks? If so, explain how and suggest specific modifications. For example, should Part I of proposed Form SCIR be modified to include a section that incorporates the check boxes and questions of Form SCI so that a single form could be filed to meet the reporting requirements of proposed Rule 10 and Regulation SCI? If so, explain why. If not, explain why not. Are there other ways Part I of proposed Form SCIR could be modified to combine the elements of Form SCI? If so, explain how. Should Rule 10 be modified to require that the initial Part I of Form SCIR must be filed within 24 hours (instead of promptly but not later than 48 hours) to align the filing timeframe with Regulation SCI? If so, explain why. If not, explain why not.

95. Should the public disclosure requirements of proposed Rule 10 be modified to address Covered Entities that also would be subject to the existing and proposed requirements of Regulation SCI and/or Regulation S-P? For example, would it be particularly costly or create practical implementation difficulties to apply the public disclosure requirements of proposed Rule 10 and Part II of proposed form SCIR (if they are adopted) to Covered Entities even if they also would be subject

to the current and proposed disclosure requirements of Regulation SCI and Regulation S-P? If so, explain why. If not, explain why not. Are there ways the public disclosure requirements of proposed Rule 10 could be modified to minimize these potential impacts while achieving the separate goals of this proposal to protect participants in the U.S. securities markets and the markets themselves from cybersecurity risks? If so, explain how and suggest specific modifications. For example, should proposed Rule 10 be modified to permit the customer notification that would be required under the amendments to Regulation S-P to satisfy the requirement of proposed Rule 10 that a Covered Entity that is a carrying broker-dealer or introducing broker-dealer send a copy of an updated Part II of proposed Form SCIR to its customers? If so, explain why. If not, explain why not. Would sending the notification required by proposed Rule 10 and the notification required by the proposed amendments to Regulation S-P to the same customer be confusing to the customer? If so, explain why. If not, explain why not.

G. Cybersecurity Risk Related to Crypto Assets

The creation, distribution, custody, and transfer of crypto assets depends almost exclusively on the operations of information systems.[545] Crypto assets, therefore, are exposed to

---

[545] The term "digital asset" or "crypto asset" refers to an asset that is issued and/or transferred using distributed ledger or blockchain technology ("distributed ledger technology"), including, but not limited to, so-called "virtual currencies," "coins," and "tokens." *See Custody of Digital Asset Securities by Special Purpose Broker-Dealers*, Exchange Act Release No. 90788 (Dec. 23, 2020) [86 FR 11627, 11627, n.1 (Feb. 26, 2021)]. To the extent digital assets rely on cryptographic protocols, these types of assets are commonly referred to as "crypto assets." A crypto asset may or may not meet the definition of a "security" under the federal securities laws. *See*, *e.g.*, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*, Securities Exchange Act Release No. 81207 (July 25, 2017), *available at* https://www.sec.gov/litigation/investreport/34-81207.pdf. *See also* SEC v. W.J. Howey Co., 328 U.S. 293 (1946). "Digital asset securities" can be referred to as "crypto asset securities" and for purposes of this release, the Commission does not distinguish between the terms "digital asset securities" and "crypto asset securities."

cybersecurity risks.[546] Further, crypto assets are attractive targets for threat actors.[547] Therefore, information systems that involve crypto assets may be subject to heightened cybersecurity risks. If Market Entities engage in business activities involving crypto assets, they could be exposed to these heighted cybersecurity risks.[548]

Crypto assets are an attractive target for unlawful activity due, in large part, to the unique nature of distributed ledger technology. Possession or control of crypto assets on a distributed ledger is based on ownership or knowledge of public and private cryptographic key pairings. These key pairings are somewhat analogous to user names and passwords and consist of strings of letters and numbers used to sign transactions on a distributed ledger and to prove ownership of a blockchain address, which is commonly known as a "digital wallet."[549] Digital wallets, in turn, generally require the use of internet-connected hardware and software to receive and transmit information about crypto asset holdings.

A digital wallet can be obtained by anyone, including a potential threat actor. If a victim's digital wallet is connected to the internet, and a threat actor obtains access to the victim's private key, the threat actor can transfer the contents of the wallet to another blockchain address (such as the threat actor's own digital wallet) without authorization from the true owner. It may be difficult to subsequently track down the identity of the threat actor because the owner of a digital wallet can remain anonymous (absent additional attribution information) and because intermediaries involved in the transfer of crypto assets, such as trading platforms, may not

---

546 *See* KPMG, *Assessing crypto and digital asset risks (*May 2022*), available at* https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2022/assessing-crypto-and-digital-asset-risks.pdf ("Properly securing digital assets[] is typically viewed as the biggest risk that companies must address.").

547 *See* U.S. Department of Treasury, *Crypto-Assets: Implications for Consumers, Investors, and Businesses* (Sept. 2022), *available at* https://home.treasury.gov/system/files/136/CryptoAsset_EO5.pdf ("Treasury Crypto Report") ("Moreover, the crypto-asset ecosystem has unique features that make it an increasingly attractive target for unlawful activity, including the ongoing evolution of the underlying technology, pseudonymity, irreversibility of transactions, and the current asymmetry of information between issuers of crypto-assets and consumers and investors.").

548 Moreover, if the Market Entity's activities involving crypto asset securities involve its information systems, the requirements being proposed in this release would be implicated.

549 *See, e.g.*, NIST Glossary (defining "private key").

comply with or may actively claim not to be subject to applicable "know your customer" or related diligence requirements.[550]

The current state of distributed ledger technology may present other challenges to defending against cybercriminal activity. First, there is no centralized information technology ("IT") infrastructure that can dynamically detect and prevent cyberattacks on wallets or prevent the transfer of illegitimately obtained crypto assets by threat actors.[551] This is unlike traditional infrastructures, such as those used by banks and broker-dealers, where behavioral and historic transaction patterns can be used to detect and prevent account takeovers in real-time. Furthermore, distributed ledger technology often makes it difficult or impossible to reverse erroneous or fraudulent crypto asset transactions, whereas processes and protocols exist to reverse erroneous or fraudulent transactions when trading more traditional assets.[552] In addition, certain code that governs the operation of a blockchain and that governs so-called "smart contracts" are often transparent to the public. This provides threat actors with visibility into potential vulnerabilities associated with the code, though developers may have limited ability to

---

550 *See, e.g.*, Treasury Crypto Report ("Compared to registered financial market intermediaries – which are subject to rules and laws that promote market integrity and govern risks and business conduct, including identifying, disclosing, and mitigating conflicts of interest and adhering to AML/CFT requirements – many crypto-asset platforms may either not yet be in compliance with, or may actively claim not to be subject to, existing applicable U.S. laws and regulations, including registration requirements . . . . When the onboarding process used by platforms is limited or opaque, the risk that the platform may be used for illegal activities increases.").

551 *See* CipherTrace, *Cryptocurrency crime and anti-money laundering report* (June 2022), *available at* https://4345106.fs1.hubspotusercontent-na1.net/hubfs/4345106/CAML%20Reports/CipherTrace%20Cryptocurrency%20Crime%20and%20Anti-Money%20Laundering%20Report%2c%20June%202022.pdf?__hstc=56248308.2ea6daf13b00f00afe4d9acf0886eddf.1667865330143.1667865330143.1667917991763.2&__hssc=56248308.1.1667917991763&__hsfp=247897319 ("CipherTrace 2022 Report").

552 For example, this is the case with Bitcoin and Ether, the two crypto assets with the largest market values. *See* CoinMarketCap, *Today's Cryptocurrency Prices by Market Cap*, *available at* https://coinmarketcap.com/ ("Crypto Asset Market Value Chart"). *See also, e.g.*, Kaili Wang, Qinchen Wang, and Dan Boneh, *ERC-20R and ERC-721R: Reversible Transactions on Ethereum* (Oct. 11, 2022), *available at* https://arxiv.org/pdf/2208.00543.pdf#page=16&zoom=100,96,233 (Stanford University proposal discussing the immutability of Ethereum-based tokens, and proposing that reversible Ethereum transactions may facilitate more wide-spread adoption of these crypto assets). With respect to securities, the clearance and settlement of securities that are not crypto assets are characterized by infrastructure whereby intermediaries such as clearing agencies and securities depositories serve as key participants in the process. The clearance and settlement of crypto asset securities, on the other hand, may rely on fewer, if any, intermediaries and remain evolving areas of practices and procedures.

patch those vulnerabilities.[553] These characteristics of distributed ledger technology, and others, present cybersecurity vulnerabilities that, if taken advantage of by a threat actor, could lead to financial harm without meaningful recourse to reverse fraudulent transactions, recover or replace lost crypto assets, or correct errors.

The amount of crypto assets stolen by threat actors annually continues to increase.[554] Threat actors looking to exploit the vulnerabilities associated with crypto assets often employ social engineering techniques, such as phishing to acquire a user's cryptographic key pairing information. Phishing tactics that have been employed to reach and trick crypto asset users into disclosing their private keys include: (1) monitoring social media for users reaching out to wallet software support, intervening with direct messages, and impersonating legitimate support staff who need the user's private key to fix the problem; (2) distributing new crypto assets at no cost to a set of wallets in an "airdrop," and then failing transactions on those assets with an error message to redirect the owner to a phishing website or a website that installs plug-in software and steals the user's credentials from a local device; and (3) impersonating a wallet software provider and stealing private keys directly from the user.[555] To the extent that the activities of Market Entities involve crypto assets, these types of phishing tactics could be used against their employees.

---

553 *See* Treasury Crypto Report ("Smart contracts, which are widely used by many permissionless blockchains, also present risks as they combine the features of generally being immutable and publicly viewable. Taken together, these attributes pose several vulnerabilities that may be exploited by illicit actors to steal customer funds: once an attacker finds a bug in a smart contract and exploits it, immutable smart contract protocols limit developers' ability to patch the exploited vulnerability, giving attackers more time to exploit the vulnerability and steal assets.").

554 *See* Treasury Crypto Report (noting that of the total amount of crypto asset based crime in 2021, theft rose by over 500% year-over-year to $3.2 billion in total); Chainalysis, *The 2022 Crypto Crime Report* (Feb. 2022), *available at* https://go.chainalysis.com/2022-Crypto-Crime-Report.html ("Chainalysis 2022 Report") (predicting that illicit transaction activity will reach an all-time high in terms of value in 2022, and noting that crypto asset based crime hit a new all-time high in 2021, with illicit addresses receiving $14 billion over the course of the year, up from $7.8 billion in 2020).

555 *See* Microsoft 365 Defender Research Team, *'Ice Phishing' on the Blockchain* (Feb. 16, 2022), *available at* https://www.microsoft.com/security/blog/2022/02/16/ice-phishing-on-the-blockchain/.

Another related variation of a social engineering attack that is similar to phishing, but does not involve stealing private keys directly, is called "ice phishing." In this scheme, the threat actor tricks the user into signing a digital transaction that delegates approval and control of the user's wallet to the attacker, allowing the threat actor to become the so-called "spender" of the wallet. Once the threat actor obtains control over the user's wallet, the threat actor can transfer all of the crypto assets to a new wallet controlled by the threat actor.[556]

Threat actors also target private keys and crypto assets through other means, such as installing key logging software,[557] exploiting vulnerabilities in code used in connection with crypto assets (such as smart contracts), and deploying flash loan attacks.[558] Installing key logging software, in particular, is an example of malware that threat actors looking to exploit the vulnerabilities associated with crypto assets often employ. Other common types of crypto asset-focused malware techniques include info stealers, clippers, and cryptojackers.[559]

---

556 *See* CipherTrace June 2022 Report. Delegating authority to another user reportedly is a common transaction on decentralized finance ("DeFi") platforms, as the user may need to provide the DeFi platform with approval to conduct transactions with the user's tokens. In an "ice phishing" attack, the attacker modifies the spender address to the attacker's address. Once the approval transaction has been signed, submitted, and mined, the spender can access the funds. The attacker can accumulate approvals over a period of time and then drain the victim's wallets quickly.

557 Key logging can involve a threat actor deploying a software program designed to record which keys are pressed on a computer keyboard to obtain passwords or other encryption keys, therefore bypassing certain security measures. *See* NIST Glossary (defining "key logger"). Key logging software can be installed, for example, when the victim clicks a link or downloads an attachment in a phishing email, downloads a Trojan virus that is disguised as a legitimate file or application, or is directed to a phony website.

558 *See* Treasury Crypto Report ("In an innovation unique to DeFi lending, some protocols may support 'flash loans,' which enable users to borrow, use, and repay crypto assets in a single transaction that is recorded on the blockchain in the same data block. Because there is no default risk associated with flash loans, users can borrow without posting collateral and without risk of being liquidated. A 'flash loan attack' can occur when the temporary surge of funds obtained in a flash loan is used to manipulate prices of crypto-assets, often through the interaction of multiple DeFi services, enabling attackers to take over the governance of a protocol, change the code, and drain the treasury."). In 2021, code exploits and flash loan attacks accounted for 49.8% of all crypto asset value stolen across all crypto asset services. *See* Chainalysis 2022 Report.

559 Specifically, "info stealers" collect saved credentials, files, autocomplete history, and crypto asset wallets from compromised computers. "Clippers" can insert new text into the victim's clipboard, replacing text the user has copied. Hackers can use clippers to replace crypto asset addresses copied into the clipboard with their own, allowing them to reroute planned transactions to their own wallets. "Cryptojackers" make unauthorized use of the computing power of a victim's device to mine crypto assets. *See* Chainalysis 2022 Report.

The size and growth of the crypto asset markets, along with the fact that many participants in these markets (such as issuers, intermediaries, trading platforms, and service providers) may be acting in noncompliance with applicable law, continue to make them an attractive target for threat actors looking for quick financial gain. The crypto asset ecosystem has exhibited rapid growth in the past few years. For example, industry reports have suggested that the total crypto asset market value increased from approximately $135 billion on January 1, 2019 to just under $2.1 trillion on March 31, 2022.[560] According to these reports, the crypto asset market value peaked at almost $3 trillion in November 2021.[561] Various sources also report that the market value remains over $1 trillion today.[562]

III. GENERAL REQUEST FOR COMMENT

In addition to the specific requests for comment above, the Commission is requesting comments from all members of the public on all aspects of the proposed rule and amendments. Commenters are requested to provide empirical data in support of any arguments or analyses. With respect to any comments, the Commission notes that they are of the greatest assistance to this rulemaking initiative if accompanied by supporting data and analysis of the issues addressed in those comments and by alternatives to the Commission's proposals where appropriate.

IV. ECONOMIC ANALYSIS

A. Introduction

The Commission is mindful of the economic effects, including the costs and benefits, of: (1) proposed Rule 10; (2) Parts I and II of proposed Form SCIR; (3) the proposed amendments to Rules 17a-4, 17ad-7, and 18a-6; (4) the proposed amendments to existing orders that exempt certain clearing agencies from registering with the Commission; and (5) the proposed

---

560 *See* CipherTrace June 2022 Report. The amount of total activity in the crypto asset markets has increased as well. According to the CipherTrace June 2022 Report, while the total activity in 2020 was around $4.3 trillion, there was approximately $16 trillion of total activity in the first half of 2021 alone. *See id*.

561 *See id*.

562 *See* Crypto Asset Market Value Chart; *see also* Treasury Crypto Report.

amendments to paragraph (d)(1) of Rule 3a71-6 to add proposed Rule 10 and Form SCIR to the list of Commission requirements eligible for a substituted compliance determination. Section 3(f) of the Exchange Act provides that when engaging in rulemaking that requires the Commission to consider or determine whether an action is necessary or appropriate in the public interest, to also consider, in addition to the protection of investors, whether the action will promote efficiency, competition, and capital formation.[563] Section 23(a)(2) of the Exchange Act also requires the Commission to consider the effect that the rules and rule amendments would have on competition, and it prohibits the Commission from adopting any rule that would impose a burden on competition not necessary or appropriate in furtherance of the Exchange Act.[564] The analysis below addresses the likely economic effects of the proposed rule and form, the proposed rule amendments, and the proposed amendments to the exemptive orders, including the anticipated and estimated benefits and costs of these proposals and their likely effects on efficiency, competition, and capital formation. The Commission also discusses the potential economic effects of certain alternatives to the approaches taken with respect to these proposals.

As discussed above, Market Entities rely on information systems to perform functions that support the fair, orderly, and efficient operation of the U.S. securities markets.[565] This exposes them and the U.S. securities markets to cybersecurity risk. According to the Bank for International Settlements, the financial sector has the second-largest share of COVID-19-related cybersecurity events between the end of February and June 2020.[566] As is the case with other risks (*e.g.*, market, credit, or liquidity risk), cybersecurity risk can be addressed through policies and procedures that are reasonably designed to manage the risk. A second means to address cybersecurity risk to the U.S. securities markets is through the Commission gathering and

---

563 *See* 15 U.S.C. 78c(f).

564 *See* 15 U.S.C. 78w(a)(2).

565 *See* section I.A. of this release (discussing cybersecurity risks and the use of information systems by Market Entities).

566 *Id*. The health sector is ranked first in term of the cyberattacks.

sharing information about significant cybersecurity incidents. This risk also can be addressed through greater transparency.[567] For these reasons (and the reasons discussed throughout the release), the Commission is proposing Rule 10 and Form SCIR to require that Market Entities address cybersecurity risks, to improve the Commission's ability to obtain information about significant cybersecurity incidents impacting Covered Entities and to require Covered Entities to disclose publicly summary descriptions of their cybersecurity risks and significant cybersecurity incidents (if applicable).

It is important to note that the Market Entities serve different functions in the U.S. securities markets and are subject to different regulatory regimes. As a result, Market Entities today have varying approaches to cybersecurity protections and would have different costs and benefits associated with complying with proposed Rule 10 and for Covered Entities to file Parts I and II of proposed Form SCIR. In addition, Market Entities may have different costs and benefits depending on the size and complexity of their businesses. For example, because Non-Covered Broker-Dealers likely are materially smaller in size than Covered Entities, use fewer and less complex information systems, and have less data stored on information systems, the obligations of Non-Covered Broker-Dealers under proposed Rule 10 are more limited, and likely would have lower compliance costs. This could be the case even though Non-Covered Broker-Dealers may still need to invest in hardware and software, employ legal and compliance personnel, or contract with a third party. Furthermore, in addition to the direct benefits and costs realized by Market Entities, other market participants, such as investors and third-party service providers would realize indirect benefits and costs from the adoption of the proposed rule. The

---

567 "The Council recommends that regulators and market participants continue to work together to improve the coverage, quality, and accessibility of financial data, as well as improve data sharing among relevant agencies." FSOC 2021 Annual Report, at 16.

direct and indirect benefits and costs realized by each type of Market Entity and market participants are discussed below.[568]

Many of the benefits and costs discussed below are difficult to quantify. For example, the effectiveness of cybersecurity strengthening measures taken as a result of proposed Rule 10 depends on the extent to which they reduce the likelihood of a cybersecurity incident and on the expected cost of such an incident, including remediation costs in the event that a cybersecurity incident causes harm. As a result, the effectiveness of cybersecurity strengthening is subject to numerous assumptions and unknowns, and thus is difficult to quantify. Effectively, because cybersecurity infrastructure as well as policies and procedures help to prevent successful cybersecurity intrusions, the benefit of cybersecurity protection can be measured as the expected loss from a cybersecurity incident. In 2020, the average loss in the financial services industry was $18.3 million, per company per incident. The average cost of a financial services data breach was $5.85 million.[569] Thus, those values would represent the benefit of avoiding a cybersecurity incident.

The Commission has limited information on cybersecurity incidents impacting Market Entities. For example, as discussed above, certain Market Entities are SCI entities subject to the requirements of Regulation SCI.[570] SCI entities must report SCI events to the Commission on Form SCI, which could include cybersecurity incidents.[571] However, only certain Market Entities are SCI entities and the reporting requirements of Regulation SCI are limited to SCI systems and indirect SCI systems, which are a subset of the information systems used by SCI entities. To the extent that a cybersecurity incident at a Market Entity that is also a SCI entity is an SCI event, the Market Entity would be required to file Form SCI. However, only certain SCI events are

---

568 *See* section IV.D. of this release (discussing these benefits and costs).

569 Jennifer Rose Hale, *The Soaring Risks of Financial Services Cybercrime: By the Numbers*, Diligent (Apr. 9, 2021), *available at* https://www.diligent.com/insights/financial-services/cybersecurity/#.

570 *See* section II.F.1.b. of this release (discussing the Covered Entities that are subject to Regulation SCI).

571 *See* section II.F.1.d. of this release (discussing the reporting requirements of Regulation SCI).

also considered to be cybersecurity incidents. Consequently, the Commission currently has only partial knowledge of the cybersecurity incidents that occur at Market Entities. The Commission believes using the benefit and cost values related to SCI Entities as a basis to estimate the benefits and costs of the proposed rule for Covered Entities would be instructive but may be under inclusive.

Similarly, the Commission has access to information contained in confidential anti-money laundering (AML) suspicious activity reports ("SARs") that broker-dealers file with the Department of the Treasury's Financial Crime Enforcement Network ("FinCEN"), which includes known or suspected cybersecurity incidents.[572] However, the SARs filed by broker-dealers with FinCEN do not necessarily include all of the details associated with an incident, such as whether the incident was confirmed, the extent of the impact, and how the breach was remediated. Furthermore, the SAR filing may not be timely, as a broker-dealer has up to 30 days to file the SAR if a suspect is identified, or up to 60 days if a suspect is not identified. Issues that require immediate attention—such as terrorist financing or ongoing money laundering schemes—must be reported to law enforcement.[573] If reporting is not otherwise required by the Commission or an SRO, a broker-dealer "may also, but is not required to" contact the Commission.[574] Broker-dealers must make the supporting documentation available to the Commission and registered SROs (as well as to FinCEN, law enforcement agencies, and Federal regulatory authorities that examine for Bank Secrecy Act compliance) upon request.[575] The benefits and costs of filing SARs with FinCEN can serve as a basis to approximate the cost of filing Part I of proposed Form SCIR. However, the proposed rule would require a quicker

---

572 *See, e.g.,* Fergus Shiel and Ben Hallman, International Consortium of Investigative Journalists*, Suspicious Activity Reports, Explained* (Sept. 20, 2020), *available at* https://www.icij.org/investigations/fincen-files/suspicious-activity-reports-explained/ (stating that approximately 85% of SARs are filed by a few large banks to report money laundering).

573 *See* 31 CFR 1023.320(b)(3).

574 *See* 31 CFR 1023.320(a)(1), (b)(3).

575 *See* 31 CFR 1023.320(d).

reporting timeline, more information to be provided, and multiple updates with regard to a given significant cybersecurity event. Thus, the costs related to complying with SAR filings serves as a floor for Covered Entities complying with the proposed rule.

While the Commission has attempted to quantify economic effects where possible, some of the discussion of economic effects is qualitative in nature. The Commission seeks comment on all aspects of the economic analysis, especially any data or information that would enable the Commission to quantify the proposal's economic effects more accurately.

B. Broad Economic Considerations

Market Entities generally have financial incentives to maintain some level of cybersecurity protection because failure to safeguard their operations from attacks on their information systems and protect information about their customers, counterparties, members, registrants, or users as well as their funds and assets could lead to losses of funds, assets, and customer information, as well as damage the Market Entity's reputation. As a result, Market Entities generally have an incentive to invest some amount of money to address cybersecurity risk.

Market Entities' reputational motives generally should encourage them to invest in measures to protect their information systems from cybersecurity risk.[576] Moreover, the damage caused by a significant cybersecurity incident, including the associated remediation costs, may exceed that of implementing cybersecurity policies and procedures that may have prevented the incident and its harmful impacts. As a result, significant losses arising from a potential significant cybersecurity incident can encourage Market Entities to invest in cybersecurity protections today. However, such investments in cybersecurity protections may not be sufficient. The Investment Company Institute notes that the remediation costs of $252 million

---

576 *See* Marc Dupuis and Karen Renaud, *Scoping the Ethical Principles of Cybersecurity Fear Appeals*, 23 Ethics and Info. Tech. 265 (2021), *available at* https://doi.org/10.1007/s10676-020-09560-0.

associated with the 2013 data breach experienced by Target Brands, Inc. ("Target") far exceeded the cost of the cybersecurity insurance the company purchased ($90 million), resulting in an out-of-pocket loss for Target of $162 million.[577] PCH Technologies states that in 2020, small companies (1-49 employees) lost an average of $24,000 per cybersecurity incident. That loss increased to $50,000 per incident for medium-sized companies (50-249 employees). Large companies (250-999 employees) and enterprise-level firms (1,000 employees or more) lost an average of $133,000 and $504,000 per cybersecurity incident, respectively.[578]

Having an annual penetration testing requirement can help Market Entities reduce the likelihood of costly data breaches. For instance, according to one industry source, RSI Security, a penetration test "can measure [the entity's] system's strengths and weaknesses in a controlled environment before [the entity has] to pay the cost of an extremely damaging data breach."[579] For example, RSI Security explains that penetration testing "can cost anywhere from $4,000-$100,000," and "[o]n average, a high quality, professional [penetration testing] can cost from $10,000-$30,000."[580] RSI Security, however, was clear that the magnitudes of these costs can vary with size, complexity, scope, methodology, types, experience, and remediation measures.[581] On the other hand, the same article cited IBM's 2019 Cost of a Data Breach Study, which reported that the average cost of a data breach is $3.92 million with an average loss of 25,575

---

577 *See* National Law Review, *Target Data Breach Price Tag: $252 Million and Counting* (Feb. 26, 2015), *available at* https://www.natlawreview.com/article/target-data-breach-price-tag-252-million-and-counting.

578 Timothy Guim, *Cost of Cyber Attacks vs. Cost of Cyber Security in 2021*, PCH Technologies (July 7, 2021), *available at* https://pchtechnologies.com/cost-of-cyber-attacks-vs-cost-of-cyber-security-in-2021/#:~:text=1%20Large%20businesses%3A%20Between%20%242%20million%20and%20%245,%24500%2C000%20or%20less%20spent%20on%20cybersecurity%20per%20year.

579 RSI Security, *What is the Average Cost of Penetration Testing?,* RSI Security Blog (posted Mar. 5,2020), *available at* https://blog.rsisecurity.com/what-is-the-average-cost-of-penetration-testing/#:~:text=Penetration%20testing%20can%20cost%20anywhere,that%20of%20a%20large%20company.

580 *See* RSI Security, *What is the Average Cost of Penetration Testing?,* RSI Security Blog (posted Mar. 5, 2020), *available at* https://blog.rsisecurity.com/what-is-the-average-cost-of-penetration-testing/#:~:text=Penetration%20testing%20can%20cost%20anywhere,that%20of%20a%20large%20company.

581 *See id.*

records,[582] which would more than justify "the average $10,000-$30,000 bill from a professional, rigorous [penetration testing]."[583] Another source estimates a "high-quality, professional [penetration testing to cost] between $15,000-$30,000," while emphasizing that "cost varies quite a bit based on a set of variables."[584] This is in line with a third source, which states that "[a] true penetration test will likely cost a minimum of $25,000."[585] It is the Commission's understanding that multi-cloud architecture could introduce more complexity and accordingly, cybersecurity risks into Market Entities back-up systems, to the extent they have them.[586]

Large Market Entities that have economies of scale are able to implement cybersecurity policies and procedures in a more cost-effective manner. Smaller Market Entities, on the other hand, generally do not enjoy the same economies of scale or scope. The marginal cost for smaller Market Entities when implementing cybersecurity policies and procedures that are just as robust as those that would be needed by large Market Entities likely would be relatively high for smaller Market Entities. As a result, investment costs in cybersecurity protection at small broker-dealers, for example, (most of which would be Non-Covered Broker-Dealers under proposed Rule 10) likely will account for a larger proportion of their revenue than at relatively large broker-dealers (which likely would be Covered Entities that realize economies of scale).

Having policies and procedures in place to address cybersecurity risk would benefit the customers, counterparties, members, registrants, or users with whom Market Entities interact.

---

582 *See* IBM, *Cost of a Data Breach Report* (2019), *available at* https://www.ibm.com/downloads/cas/RDEQK07R ("2019 Cost of Data Breach Report").

583 *See* RSI Security, *What is the Average Cost of Penetration Testing?,* RSI Security Blog (posted Mar. 5, 2020), *available at* https://blog.rsisecurity.com/what-is-the-average-cost-of-penetration-testing/#:~:text=Penetration%20testing%20can%20cost%20anywhere,that%20of%20a%20large%20company.

584 Gary Glover, *How Much Does a Pentest Cost?*, Securitymetrics Blog (Nov. 15, 2022, 8:36 a.m.), *available at* https://www.securitymetrics.com/blog/how-much-does-pentest-cost.

585 Mitnick Security, *What Should You Budget for a Penetration Test? The True Cost*, Mitnick Security Blog, (posted Jan. 29, 2021, 5:13 a.m.), *available at* https://www.mitnicksecurity.com/blog/what-should-you-budget-for-a-penetration-test-the-true-cost.

586 For example, security breach possibilities could increase because of the interconnection of Market Entities through their multi cloud providers.

However, a cybersecurity budget likely is tempered, in part, such that the total sum spent to address cybersecurity risk provides some, but possibly not complete, protection against cyberattacks.[587] Ultimately, those costs to address cybersecurity risks will be passed on, to the extent possible, to the persons with whom the Market Entities do business.[588]

The level of cybersecurity protection instituted by Market Entities may be inadequate from the perspective of overall economic efficiency.[589] In other words, the chosen level of cybersecurity protection may, in fact, represent an underinvestment relative to the optimal level of cybersecurity protection that should be maintained by Market Entities from an overall economic perspective. Levels of cybersecurity protection that are not optimal may exacerbate the occurrence of harmful cybersecurity incidents. Cybersecurity events have grown in both number and sophistication.[590] These developments in the market have significantly increased the negative externalities that may flow from systems failures.

Underinvestment in cybersecurity may occur because a Market Entity is aware that it would not bear the full cost of a cybersecurity incident (*i.e.*, some negative externalities may be borne by its customers, counterparties, members, registrants, or users). As a result, the Market

---

587 *See* Martijn Wessels, Puck van den Brink, Thijmen Verburgh, Beatrice Cadet, and Theo van Ruijven, *Understanding Incentives for Cybersecurity Investments: Development and Application of a Typology*, 1 Digit. Bus. 1-7 (Oct. 2021), *available at* https://doi.org/10.1016/j.digbus.2021.100014; Scott Dynes, Eric Goetz, and Michael Freeman, *Cyber Security: Are Economic Incentives Adequate?* (Intern. Conf. on Critical Infrastructure Protection, Conference Paper, 2007), *available at* https://doi.org/10.1007/978-0-387-75462-8_2; Brent R. Rowe and Michael P. Gallaher, *Private Sector Cyber Security Investment Strategies: An Empirical Analysis*, The Fifth Workshop on the Economics of Information Security (Mar. 2006), *available at* http://www.infosecon.net/workshop/downloads/2006/pdf/18.pdf ("Private Sector Cyber Security Investment Strategies Analysis"); Nicole van der Meulen, RAND Europe, *Investing in Cybersecurity* (Aug. 2015), *available at* https://repository.wodc.nl/bitstream/handle/20.500.12832/2173/2551-full-text_tcm28-73946.pdf?sequence=4&isAllowed=y.

588 *See* Derek Mohammed, *Cybersecurity Compliance in the Financial Sector*, J. Internet Banking and Com. (2015), *available at* https://www.icommercecentral.com/open-access/cybersecurity-compliance-in-the-financial-sector.php?aid=50498.

589 Low levels of investment in cybersecurity protection, which are different from underinvestment in cybersecurity protection, can be a function of a number of issues, such as firm budget, available solutions, knowledge of the threat actors' capabilities, and the performance of in-house or contracted information technology teams.

590 *See, e.g.*, Chuck Brooks, *Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know* (June 3, 2022), *available at* https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=2429c57e7864.

Entity does not have to internalize the complete cost of cybersecurity protection when deciding upon its level of investment. This underinvestment by the Market Entity is considered to be a moral hazard problem, because other market participants are harmed by a significant cybersecurity incident and are forced to bear those costs that spill over to them. At the same time, even though Market Entities may not bear the full cost of a cybersecurity failure (*e.g.,* loss of the personal information or the assets of their customers, members, registrants, or users), they likely would incur some costs themselves and therefore have incentives to avoid cybersecurity failures. These incentives could cause them to implement policies and procedures to address cybersecurity risk, which would likely result in benefits that accrue in large part to their customers, counterparties, members, registrants, or users. Market Entities could do this in order to avoid the harms that could be caused by a significant cybersecurity incident (*e.g.*, loss of funds, assets, or personal, confidential, or proprietary information; damage to or the holding hostage of their information systems; or reputational damage). As a result, Market Entities have a potential incentive to rely overly on reactive solutions to cybersecurity threats and attacks instead of proactive ones.[591] .

1. In the context of cybersecurity, negative externalities arising from the moral hazard problem can have significant negative repercussions on the financial system more broadly, particularly due to the interconnectedness of Market Entities.[592] Borg notes that the level of interconnectedness and complexity can have an influence on the degree of damage that cybersecurity incidents impose on Market Entities as well as their customers, counterparties, members, registrants, and users.[593] As for the availability of substitutes the negative effect of a cybersecurity incident could be

---

591 *See* Private Sector Cyber Security Investment Strategies Analysis.

592 *See* Anil K. Kashyap and Anne Wetherilt, *Some Principles for Regulating Cyber Risk*, 109 Amer. Econ. Assoc. Papers and Proc. 482 (May 2019).

593 *See* Scott Borg, *Economically Complex Cyberattacks*, IEEE Computer Society (2005), *available at* https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1556539.

lessened to the extent that there is one or more competing firms that can complete the task, such as another broker-dealer or national securities exchange. On the flip side, significant cybersecurity incidents may be the most damaging when there are no substitutes available to execute the required task.

In addition to other firms being negatively affected by a cybersecurity incident, investors can be negatively affected. For example, a significant cybersecurity incident at a national securities exchange could affect its ability to execute trades, causing orders to go unfilled. Depending on how long it takes the national securities exchange to resolve the issue, the prices of securities traded on the exchange may be different from when the orders were originally placed.[594] A loss of confidence in an exchange due to a cybersecurity incident could result in a longer-term reallocation of trading volume to competing exchanges or other trading venues.[595] A significant cybersecurity incident could produce negative effects that spill over and affect market participants outside of the national securities exchange itself. It also may adversely affect market confidence, and curtail economic activity through a reduction in securities trading among market participants.[596]

While the negative externalities that arise from the moral hazard problem are usually depicted as being absorbed by other market participants, the losses to other parties may be potentially covered in part or in full by insurance policies.[597] An even stronger incentive to underinvest is the possibility that an outside party can make whole or at least mitigate some of the losses incurred by the various market participants. Market Entities may underinvest in their

---

594 National securities exchanges currently are subject to certain obligations under Regulation SCI.

595 National securities exchanges may be required to meet certain regulatory obligations in such circumstances.

596 *See* Electra Ferriello, *Prof. Robert Shiller's U.S. Crash Confidence Index*, Yale School of Management, Intern. Ctr. for Fin. (Nov. 3, 2020), *available at* https://som.yale.edu/blog/prof-robert-shillers-us-crash-confidence-index; Gregg E. Berman, Senior Advisor to the Director, Division of Trading and Markets, Commission, Speech by SEC Staff: Market Participants and the May 6 Flash Crash (Oct. 2010), *available at* https://www.sec.gov/news/speech/2010/spch101310geb.htm.

597 *See* Marsh, *Underinvestment in Cyber Insurance Can Leave Organizations Vulnerable* (2022), *available at* https://www.marsh.com/pr/en/services/cyber-risk/insights/underinvestment-in-cyber-insurance.html.

cybersecurity measures due to the moral hazard that results from expectations of government support.[598] Most threat actors primarily have a monetary incentive, and there is a large monetary incentive to breach cybersecurity protections in the financial sector. As a result, Covered Entities—such as clearing agencies, large national securities exchanges, and large carrying broker-dealers—may be attractive targets to sophisticated threat actors aiming to compromise or disrupt the U.S. financial system because of the services they perform to support the functioning of the U.S. securities markets; the protection of confidential, proprietary, or personal information they store; or the financial assets they hold. Protection against "advanced persistent threats"[599] from sophisticated threat actors, whatever their motives, is costly.[600] The belief—no matter how misplaced—that a widespread and crippling cybersecurity attack would be met with government support, such as direct payments for recovery and immediate cybersecurity investments, could lead to moral hazard where certain Covered Entities underinvest in defenses aimed at countering that threat.[601]

Suboptimal spending on cybersecurity also can be the result of asymmetric information among Market Entities and market participants. A Market Entity may not know what its optimal

---

598 It has long been noted that it is difficult for governments to commit credibly to not providing support to entities that are seen as critical to the functioning of the financial system, resulting in problems of moral hazard. *See, e.g.*, Walter Bagehot, *Lombard Street: A Description of the Money Market* (Henry S. King & Co., 1873). Historically, banking entities seen as "too big to fail" or "too interconnected to fail" have been the principal recipients of such government support. Since the financial crisis of 2007-2009, non-bank financial institutions (such as investment banks), money market funds, and insurance companies, as well as specific markets such as the repurchase market have also benefited. *See, e.g.*, Gary B. Gorton, *Slapped by the Invisible Hand: The Panic of 2007*, Oxford Univ. Press (2010); *see also* Viral V. Acharya, Deniz Anginer, and A. Joseph Warburton, *The End of Market Discipline? Investor Expectations of Implicit Government Guarantees*, SSRN Scholarly Paper, Rochester, NY: Social Science Research Network (May 1, 2016).

599 "Advanced persistent threat" refers to sophisticated cyberattacks by hostile organizations with the goal of: gaining access to defense, financial, and other targeted information from governments, corporations and individuals; maintaining a foothold in these environments to enable future use and control; and modifying data to disrupt performance in their targets. *See* Michael K. Daly, *The Advanced Persistent Threat (or Informationized Force Operations)*, Raytheon (Nov. 4, 2009), *available at* https://www.usenix.org/legacy/event/lisa09/tech/slides/daly.pdf.

600 *See* Nikos Virvilis and Dimitris Gritzalis, *The Big Four - What We Did Wrong in Advanced Persistent Threat Detection?*, 2013 Int'l Conf. on Availability, Reliability and Security 248 (2013).

601 *See* Lawrence A. Gordon, Martin P. Loeb, and William Lucyshyn, *Cybersecurity Investments in the Private Sector: The Role of Governments*, 15 Geo. J. Int'l Aff. 79 (2014).

cybersecurity expenditures should be because the nature and scope of future attacks are unknown. In addition, a Market Entity may not know what its competitors do in terms of cybersecurity planning, whether they have been subject to unsuccessful cyberattacks, or have been a victim of one or more significant cybersecurity incidents. Market Entities also may not be able to signal credibly to their customers, counterparties, members, registrants, or users that they are better at addressing cybersecurity risks than their peers, thus reducing their incentive to bear such cybersecurity investment costs.[602] Lastly, Market Entities' customers, counterparties, members, registrants, or users typically do not have information about the Market Entities' cybersecurity spending, the efficacy of the cybersecurity investments made, or their policies and procedures. Therefore, those market participants cannot make judgments about Market Entities' cybersecurity preparedness. Because of this information asymmetry, Market Entities may not have as strong of an incentive to have robust cybersecurity measures compared to a scenario in which customers, counterparties, members, registrants, or users had perfect information about the Market Entities' cybersecurity practices and the risks that they face.

Underinvestment in cybersecurity also may stem from the principal-agent problem of divergent goals in economic theory. The relationship between a Market Entity (*i.e.*, the agent) and the principals (*i.e.*, its customers, counterparties, members, registrants, or users) can be affected if the principal relies on the agent to perform services on the principal's behalf.[603] Because principals and their agents may not have perfectly aligned preferences and goals, agents may take actions that increase their well-being at the expense of principals, thereby imposing "agency costs" on the principals.[604] Although private contracts between principals and agents may aim to

---

602 *See* Sanford J. Grossman, *The Informational Role of Warranties and Private Disclosure about Product Quality*, 24 J. L. Econ. 461 (Dec. 1981); *see also* Michael Spence, *Competitive and Optimal Responses to Signals*: *An Analysis of Efficiency and Distribution*, 7 J. Econ. Theory 296 (Mar. 1, 1974); George. A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q. J. Econ. 488 (Aug. 1970).

603 *See* Michael C. Jensen and William H. Meckling, *Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure*, 3 J. Fin. Econ. 305 (1976).

604 *Id*.

minimize such costs, they are limited in their ability to do so in that agents can decide not enter into such agreements and ultimately not provide the particular services to the principals. Furthermore, agents can charge much higher fees that the principals choose not to bear. These limitations provides one rationale for regulatory intervention.[605] Market-based incentives alone are unlikely to result in optimal provision of cybersecurity protection. In this context, having plans and procedures in place to prepare for and respond to cybersecurity incidents,[606] and the rule would help ensure that the infrastructure of the U.S. securities markets remains robust, resilient, and secure. A well-functioning financial system is a public good.

Beyond reputational damage to the affected agent (Market Entity), the principals (the Market Entity's customers, counterparties, members, registrants, or users) can be negatively affected by a cybersecurity breach as a result of loss in personal information and/or funds and assets. Thus the principals and the agents may have different reasons for needing cybersecurity protocols. Furthermore, the negative effects of a cybersecurity incident also can spread among Market Entities due to their interconnectedness.[607] Those other Market Entities prefer that the principals employ strong cybersecurity practices that reduce the chances of a successful breach and its negative cascading effects throughout the financial sector. All of the preceding negative externalities are arguments for proposed Rule 10.

---

605 Such limitations can arise from un-observability or un-verifiability of actions, transactions costs associated with including numerous contingencies in contracts, or bounded rationality in the design of contracts. *See, e.g.*, Jean Tirole, *Cognition and Incomplete Contracts*, 99 Am. Econ. Rev. 265 (Mar. 2009) (discussing a relatively modern treatment of these issues).

606 For example, according to an IBM report, in the context of system issues arising from cybersecurity events, having an incident response plan and "testing that plan regularly can help [each firm] proactively identify weaknesses in [its] cybersecurity and shore up [its] defenses" and "save millions in data breach costs." *See* 2019 Cost of Data Breach Report; *see also* Alex Asen et al., *Are You Spending Enough on Cybersecurity* (Feb. 19, 2020), *available at* https://www.bcg.com/publications/2019/are-you-spending-enough-cybersecurity (noting "[a]s the world becomes ever more reliant on technology, and as cybercriminals refine and intensify their attacks, organizations will need to spend more on cybersecurity").

607 *See* sections I.A.1. and I.A.2. of this release (discussing how the interconnectedness of Market Entities creates cybersecurity risk).

In the production of cybersecurity defenses and controls, the main input is information. In particular, information about prior attacks and their degree of success, as well as prior human errors and their degree of harm, is valuable in mounting effective countermeasures and controls.[608] However, Market Entities may be naturally reluctant to share such information, as doing so could assist future attackers as well as lead to loss of customers, reputational harm, litigation, or regulatory scrutiny, which would be costs associated with public disclosure.[609] On the other hand, disclosure of such information creates a positive information externality—the benefits of which accrue to society at large and are not fully captured by the Market Entity making the disclosure. This situation can occur because the disclosure informs the Market Entity's customers, counterparties, members, registrants, or users—as well as the Market Entity's competitors—about the cybersecurity incidents experienced by the Market Entity. As a result, information disclosures intended to close the information asymmetry gap can have both positive and negative consequences.

As discussed earlier, sources of market failure in cybersecurity come from information asymmetries at two different levels: (1) between Market Entities and their customers, counterparties, members, registrants, or users; and (2) between Market Entities and threat actors. These two failures, in turn, create distinct consequences for each of these stakeholders.

At the first level, a Market Entity's customers, counterparties, members, registrants, or users have incomplete information about their own cybersecurity risks due to incomplete information about the Market Entity's actual cybersecurity policies and procedures. To exacerbate the first level of information asymmetry, Market Entities typically interact with other market participants. For example, investors do business with broker-dealers, introducing broker-dealers work with carrying broker-dealers, FINRA supervises broker-dealers, broker-dealers

---

608 *See* Peter W. Singer and Allan Friedman, *Cybersecurity: What Everyone Needs to Know 222* (Oxford Univ. Press, 2014).

609 *See, e.g.,* FTC Equifax Civil Action.

interact with national securities exchanges, and national securities exchanges work with clearing agencies.

When utilizing the services of a Market Entity, other market participants may not have full information regarding the Market Entity's exposure to material harm as a result of a cybersecurity incident. A cybersecurity incident that harms a Market Entity can harm its customers, counterparties, members, registrants, or users. Disclosure of information regarding significant cybersecurity incidents by Market Entities could be used by their customers, counterparties, members, registrants, or users to manage their own cybersecurity risk by investing in additional cybersecurity protection, and, to the extent they have a choice, selecting a different Market Entity with satisfactory cybersecurity protection with whom to transact or otherwise conduct business.[610] That is, a Market Entity with strong cybersecurity policies and procedures and a clean record in terms of past significant cybersecurity incidents may be perceived by these market participants as more desirable to interact with, or obtain services from, than Market Entities of the same type that do not fit that profile. Even general details about the cybersecurity incidents, as well as the number of significant cybersecurity incidents during the current or previous calendar year, could allow customers, counterparties, members, registrants, and users to compare Market Entities.

---

[610] As discussed earlier, the public disclosure requirements of proposed Rule 10 would apply to Market Entities that meet the proposed rule's definition of "covered entity." *See* paragraph (d) of proposed Rule 10; section II.B.3. of this release (discussing the public disclosure requirements of proposed Rule 10).

As a result, information from the disclosure may permit customers, counterparties, members, registrants, and users to gauge the riskiness of doing business with a certain Market Entity when they would not have been able to without that knowledge, and the disclosures may encourage those market participants to move their business to competing Market Entities that would have to disclose information under proposed Rule 10 and are perceived to be more prepared for cybersecurity attacks.[611] The information disclosed by competitors also can incentivize Market Entities to increase their investment in cybersecurity protections and allow them to adjust their defenses when they would not have done so otherwise, thus increasing overall market stability by further limiting harmful cybersecurity incidents.

At the second level, there are differences in the capabilities of threat actors that are external to Market Entities and the assumed level of cybersecurity preparations needed by Market Entities to protect against significant cybersecurity incidents. Specifically, Market Entities cannot fully anticipate the type, method, and complexity of all types of cyberattacks that may materialize. Moreover, cyberattacks evolve over time, becoming more complex and using new avenues to circumvent Market Entities' cybersecurity protections.[612] Furthermore, Market Entities cannot predict the timing or the target of a given cyberattack. Though this information asymmetry is impossible to eradicate fully given the inherent secretive nature of threat actors, regulation may help to prevent an expansion of information asymmetry by requiring Market Entities to gather and assess information about cybersecurity risks and vulnerabilities more often. Doing so would not only help to contain the negative effects of successful cybersecurity attacks on any one Market Entity going forward, but it also would aid in minimizing the growth in

---

611 The firms making the disclosure may be incentivized to invest more in cybersecurity protection, potentially to the point of overinvestment in order not to lose customers, counterparties, members, registrants, and users.

612 *See*, *e.g.*, Verizon DBIR.

negative externalities as the effects of successful cyberattacks spillover to other Market Entities as well as to their customers, counterparties, members, registrants, or users.

Cybersecurity defenses must constantly evolve in order to keep up with the threat actors who are exogenous to the Market Entity, and its ability to anticipate specific attacks on itself is difficult at best. Within the reasonable scenario of an interconnected market with multiple points of entry for a potential threat actor, it may be more costly for Market Entities that are the victims of cascading cybersecurity breaches than for the initial target itself, as the other Market Entities within the network ultimately would need to prepare for a multitude of attacks originating from many different initial targets.[613] A strong cybersecurity program can also help Market Entities to protect themselves from cybersecurity attacks that could possibly come from one of multiple entry points. Having comprehensive cybersecurity policies and procedures will aid Market Entities identifying the source of a breach, which can result in lower detection costs and the identification of the threat actor in a more expeditious manner.

C. Baseline

Each type of Market Entity that would be subject to proposed Rule 10 has a distinct business model and role in the U.S. financial markets. As a result, the risks and practices, regulation, and market structure for each Market Entity will form the baseline for the economic analysis.

1. Cybersecurity Risks and Current Relevant Regulations

a. Cybersecurity Risks

With the widespread adoption of internet-based products and services over the last two decades, all businesses have had to address cybersecurity issues.[614] For financial services firms, the stakes are particularly high because they transact, hold custody of, and maintain ownership

---

613 *See* Cybersecurity and its Cascading Effect on Societal Systems.

614 *See* section I.A.1. of this release (discussing cybersecurity risks to the U.S. securities markets).

records of wealth in the form of cash, securities, or other liquid assets that cyber threat actors might strive to obtain illegally. Such entities also represent attack vectors for threat actors. In addition, Market Entities have linkages with each other as a result of the business they conduct together. A breach at one Market Entity may be exploited and serve as a means of compromising other Market Entities. Cybersecurity threat intelligence surveys consistently find the financial sector to be one of the most—if not the most—attacked industries,[615] and remediation costs for an incident can be substantial.[616] As a result, firms in the financial sector need to invest in cybersecurity to protect their business operations along with the accompanying assets and data stored on information systems.

Further, as discussed earlier, the custody and transfer of crypto assets depends almost exclusively on the operations of information systems.[617] Crypto assets, therefore, are exposed to cybersecurity risks and they are attractive targets for threat actors. Information systems that involve crypto assets may be subject to heightened cybersecurity risks. To the extent that Market Entities engage in business activities involving crypto assets, they could be exposed to these heighted cybersecurity risks.

The ubiquity and rising costs of cybercrime,[618] along with financial services firms' increasingly costly efforts to prevent it,[619] have been the motivation behind the growth in the cybersecurity industry.[620] Many Market Entities cite the NIST Framework as the main standard

---

615 *See, e.g.*, IBM, *X-Force Threat Intelligence Index 2022* (2022), *available at* https://www.ibm.com/security/data-breach/threat-intelligence.

616 *See, e.g.*, 2019 Cost of Data Breach Report (noting the average cost of a data breach in the financial industry in the United States is $5.97 million).

617 *See* section II.G. of this release (discussing cybersecurity risks related to crypto assets).

618 *See* FBI Internet Crime Report (noting that cybercrime victims lost approximately $6.9 billion in 2021).

619 *See* Office of Financial Research, *Annual Report to Congress 2021*, *available at* https://www.financialresearch.gov/annual-reports/files/OFR-Annual-Report-2021.pdf.

620 Sage Lazzaro, *The Cybersecurity Industry Is Burning — But VCs Don't Care*, VentureBeat (Sept. 2, 2021), *available at* https://venturebeat.com/2021/09/02/the-cybersecurity-industry-is-burning-and-vcs-dont-care/ ("VentureBeat").

for implementing strong cybersecurity measures.[621] The focus that has been placed on cybersecurity also has led to the development of numerous technologies and standards by private sector firms aimed at mitigating cybersecurity threats. Many of these developments, such as multi-factor authentication, secure hypertext transfer protocol,[622] and user-access control, are now commonplace. Practitioners—chief technology officers ("CTOs"), chief compliance officers ("CCOs"), chief information officers ("CIOs"), chief information security officers ("CISOs"), and their staffs— frequently utilize industry standard frameworks[623] and similar offerings from cybersecurity consultants and product vendors to assess and address institutional cybersecurity preparedness. Such frameworks include information technology asset management, controls, change management, vulnerability management, incident management, continuity of operations, risk management, dependencies on third parties, training, and information sharing. In recent years, companies' boards of directors and executive management teams have focused on these areas.

Unaddressed cybersecurity risks, particularly at Market Entities, impose negative externalities on the broader financial system. Actions taken to implement, maintain, and upgrade cybersecurity protections likely reduce overall risk in the economy. In addition, due to the potential for large-scale losses with respect to funds, securities, and customer information, Market Entities have a vested interest in installing, maintaining, and upgrading cybersecurity-related software and hardware. Based on staff discussions with market participants, cybersecurity-related activities can be performed in-house or contracted out to third parties with

---

621 FCI, *Top 5 Ways the Financial Services Industry Can Leverage NIST for Cybersecurity Compliance*, *available at* https://fcicyber.com/top-5-ways-the-financial-services-industry-can-leverage-nist-for-cybersecurity-compliance/.

622 Hypertext transfer protocol, HTTP, is the primary set of rules that allow a web browser to communicate with (*i.e.*, send data to) a website.

623 CISA, *Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide* (Apr. 2020), *available at* https://www.cisa.gov/sites/default/files/publications/2_CRR%204.0_Self-Assessment_User_Guide_April_2020.pdf.

expertise in those areas. Financial services firms may employ a mix of in-house and outsourced staff and resources to meet their cybersecurity needs and goals.

b. Current Relevant Regulations

i. Broker-Dealers

Broker-dealers are subject to Regulation S-P[624] and Regulation S-ID.[625] In addition, ATSs that trade certain stocks exceeding specific volume thresholds are subject to Regulation SCI.[626] Further, an ATS is subject to Regulation ATS.[627] As discussed earlier, Regulation SCI, Regulation S-P, Regulation ATS, and Regulation S-ID have provisions requiring policies and procedures to address certain types of cybersecurity risks.[628] Regulation SCI also requires immediate written or telephonic notice and subsequent reporting to the Commission on Form SCI of certain types of incidents.[629] Finally, Regulation SCI has provisions requiring disclosures to persons affected by certain incidents.[630]

Broker-dealers are also subject to the Commission's financial responsibility rules. Rule 15c3-1requires broker-dealers to maintain minimum amounts of net capital, ensuring that the broker-dealer at all times has enough liquid assets to promptly satisfy all creditor claims if the broker-dealer were to go out of business.[631] Rule 15c3-3 under the Exchange Act imposes requirements relating to safeguarding customer funds and securities.[632] These rules provide

---

624 *See* 17 CFR 248.1 through 248.30.

625 *See* 17 CFR 248.201 and 202.

626 *See* 17 CFR 242.1000 through 1007.

627 *See* 17 CFR 242.301 through 304.

628 *See* section II.F.1.c. of this release (discussing in more detail the existing requirements of Regulation SCI, Regulation S-P, Regulation ATS, and Regulation S-ID to have policies and procedures to address certain cybersecurity risks).

629 *See* section II.F.1.d. of this release (discussing in more detail the existing immediate notification and subsequent reporting requirements of Regulation SCI).

630 *See* section II.F.1.e. of this release (discussing in more detail the existing disclosure requirements of Regulation SCI).

631 *See* 17 CFR 240.15c3-1.

632 *See* 17 CFR 240.15c3-3.

protections for broker-dealer counterparties and customers and can help to mitigate the risks to, and impact on, customers and other market participants by protecting them from the consequences of financial failure that may occur because of a systems issue at a broker-dealer.

Under Exchange Act Rule 15c3-4, OTC derivatives dealers must establish, document, and maintain a system of internal risk management controls to assist it in managing the risks associated with its business activities, including market, credit, leverage, liquidity, legal, and operational risks.[633] The required risk management system must include, among other things: a risk control unit that reports directly to senior management, periodic reviews which may be performed by internal audit staff, and annual reviews which must be conducted by independent certified public accountants.[634] Management must periodically review the entity's business activities for consistency with risk management guidelines, including that the data necessary to conduct the risk monitoring and risk management function as well as the valuation process over the entity's portfolio of products is accessible on a timely basis and information systems are available to capture, monitor, analyze, and report relevant data.[635]

Exchange Act Rules 17a-3 and 17a-4 require broker-dealers to make and keep current records detailing, among other things, securities transactions, money balances, and securities positions.[636] Further, a broker-dealer that fails to make and keep current the records required by Rule 17a-3 must give notice to the Commission of this fact on the same day and, thereafter, within 48 hours transmit a report to the Commission stating what the broker-dealer has done or is doing to correct the situation.[637]

---

633 *See* 17 CFR 240.15c3-4(a).

634 *See* 17 CFR 240.15c3-4(c).

635 *Id.*

636 *See* 17 CFR 240.17a-3; 17 CFR 240.17a-4.

637 *See* 17 CFR 240.17a-11.

Moreover, with certain exceptions, broker-dealers must file confidential SARs with FinCEN to report any suspicious transaction relevant to a possible violation of law or regulation.[638] The SARs include information regarding who is conducting the suspicious activity, what instruments or mechanisms are being used, when and where the suspicious activity took place, and why the filer thinks the activity is suspicious. Broker-dealers must make the records available to FinCEN as well as to other appropriate law enforcement agencies, federal or state securities regulators, and SROs registered with the Commission.

Broker-dealers are generally required to register with the Commission and join a national securities association or national securities exchange.[639] As SROs, national securities associations and national securities exchanges are required to enforce their members' compliance with the Exchange Act, the rules and regulations thereunder, and the SRO's own rules. The vast majority of brokers and dealers join FINRA. Broker-dealers that are members of FINRA are subject FINRA Rules 3110, 3120, and 4530(b) (among other FINRA rules).[640] FINRA Rule 3110 requires broker-dealer members to have in place a system to supervise its activities so that they are in compliance with applicable rules and regulations. FINRA Rule 3120 requires broker-dealer members to test and verify that the supervisory procedures are reasonably designed with respect to the activities of the member and its associated persons, as well as to achieve compliance with applicable securities laws and regulations and with applicable FINRA rules. In addition, broker-dealer members must create additional or amended supervisory procedures where a need is identified by such testing and verification. The designated individual(s) must submit to the broker-dealer member's senior management no less than annually a report detailing

---

638 *See* 31 CFR 1023.320; section IV.A. of this release (discussing the requirements to file SARs in more detail).

639 *See* 15 U.S.C. 78o(a)(1) and 15 U.S.C. 78o(b)(8).

640 Broker-dealers that are members of national securities exchanges are also subject to the rules of the national securities exchanges regarding membership, registration, operation, and business conduct, among other exchange regulations.

each member's system of supervisory controls, the summary of the test results and significant identified exceptions, and any additional or amended supervisory procedures created in response to the test results. FINRA Rule 4530(b) states that each broker-dealer member shall promptly report to FINRA, but not later than 30 calendar days after the member has concluded or reasonably should have concluded, that an associated person of the member or the member itself has violated any securities-, insurance-, commodities-, financial- or investment-related laws, rules, regulations, or standards of conduct of any domestic regulatory body, foreign regulatory body, or SRO. Furthermore, Commission staff has issued statements[641] and FINRA has issued

---

641 *See, e.g.* EXAMS, Risk Alert, *Safeguarding Client Accounts*; EXAMS, Risk Alert, *Select COVID-19 Compliance Risks and Considerations for Broker-Dealers and Investment Advisers* (Aug. 12, 2020), *available at* https://www.sec.gov/files/Risk%20Alert%20-%20COVID-19%20Compliance.pdf; EXAMS,Risk Alert, *Ransomeware*; EXAMS, *Report on OCIE Cybersecurity and Resiliency Observations* (Jan. 27, 2020), *available at* https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf ("EXAMS Cybersecurity and Resiliency Observations"); EXAMS, *Safeguarding Customer Records and Information in Network Storage—Use of Third Party Security Features* (May 23, 2019), *available at* https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Network%20Storage.pdf; EXAMS, *Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P— Privacy Notices and Safeguard Policies* (Apr. 16, 2019), *available at* https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf; EXAMS, *Observations from Cybersecurity Examinations* (Aug. 7, 2017), *available at* https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf ("EXAMS Observations from Cybersecurity Examinations"); EXAMS, *Cybersecurity: Ransomware Alert* (May 17, 2017), *available at* https://www.sec.gov/files/risk-alert-cybersecurity-ransomware-alert.pdf; EXAMS, *OCIE's 2015 Cybersecurity Examination Initiative* (Sept. 15, 2015), *available at* https://www.sec.gov/files/ocie-2015-cybersecurity-examination-initiative.pdf; EXAMS, *Cybersecurity Examination Sweep Summary* (Feb. 3, 2015), *available at* https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf ("Cybersecurity Examination Sweep Summary"); EXAMS, *OCIE's 2014 Cybersecurity Initiative* (Apr. 15, 2014), *available at* https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf.

guidance[642] in the area of cybersecurity.[643] The statements and FINRA guidance with respect to these rules identify common elements of reasonably designed cybersecurity policies and procedures including risk assessment, user security and access, information protection, incident response,[644] and training.[645]

Consistent with these rules, nearly all broker-dealers that participated in two Commission exam sweeps in 2015 and 2017 reported[646] maintaining some cybersecurity policies and

---

642 *See* FINRA, *Core Cybersecurity Threats and Effective Controls for Small Firms* (May 2022), *available at* https://www.finra.org/sites/default/files/2022-05/Core_Cybersecurity_Threats_and_Effective_Controls-Small_Firms.pdf; FINRA, *Cloud Computing in the Securities Industry* (Aug. 16, 2021), *available at* https://www.finra.org/sites/default/files/2021-08/2021-cloud-computing-in-the-securities-industry.pdf; FINRA, *2021 Report on FINRA's Examination and Risk Monitoring Program* (Feb. 1, 2021), *available at* https://www.finra.org/sites/default/files/2021-02/2021-report-finras-examination-risk-monitoring-program.pdf ("FINRA 2021 Report on Examination and Risk Monitoring Program"); FINRA, *2019 Report on FINRA Examination Findings and Observations* (Oct. 16, 2019), *available at* https://www.finra.org/sites/default/files/2019-10/2019-exam-findings-and-observations.pdf; FINRA Common Cybersecurity Threats; FINRA, *Report on Selected Cybersecurity Practices – 2018* (Dec. 1, 2018), *available at* https://www.finra.org/sites/default/files/Cybersecurity_Report_2018.pdf "(FINRA Report on Selected Cybersecurity Practices"); FINRA, *Report on FINRA Examination Findings* (Dec. 6, 2017), *available at* https://www.finra.org/sites/default/files/2017-Report-FINRA-Examination-Findings.pdf;; FINRA, *Small Firm Cybersecurity Checklist* (May 23, 2016), *available at* https://www.finra.org/compliance-tools/small-firm-cybersecurity-checklist.

643 Cybersecurity has also been a regular theme of FINRA's Regulatory and Examination Priorities Letter since 2008 often with reference to Regulation S-P. Similarly, while risks related to data compromises were highlighted in the Commission staff's exam priorities, an official focus on "cyber" began in 2014 after the SEC sponsored a Cybersecurity Roundtable and the Division of Examination conducted cybersecurity initiative I and II to assess industry practices and legal and compliance issues associated with broker-dealer and investment adviser cybersecurity preparedness. Cybersecurity initiatives I and II were each separate series of examinations of cybersecurity practices conducted by EXAMS, concluding in 2014 and 2017. The examinations covered broker-dealers, investment advisers, and funds. EXAMS released a summary report for each initiative.

644 *See* FINRA 2021 Report on Examination and Risk Monitoring Program (noting that FINRA recommended among effective practices with respect to incident response: (1) establishing and regularly testing -often using tabletop exercises- a written formal incident response plan that outlines procedures for responding to cybersecurity and information security incidents; and (2) developing frameworks to identify, classify, prioritize, track and close cybersecurity-related incidents).

645 These categories vary somewhat in terms of nomenclature and the specific categories themselves across different Commission and FINRA publications.

646 *See* Cybersecurity Examination Sweep Summary (noting that of 57 examined broker-dealers, the vast majority adopted written information security policies, conducted periodic audits to determine compliance with these information security policies and procedures, conducted risk assessments and reported considering such risk assessments in establishing their cybersecurity policies and procedures, and that with respect to vendors, the majority of the broker-dealers required cybersecurity risk assessments of vendors with access to their firms' networks and had at least some specific policies and procedures relating to vendors). *See also* EXAMS Observations from Cybersecurity Examinations (noting that nearly all firms surveyed had incident response plans).

procedures; conducting some periodic risk assessments to identify threats and vulnerabilities,[647] conducting firm-wide systems inventorying or cataloguing, ensuring regular system maintenance including the installation of software patches to address security vulnerabilities, performing some penetration testing.[648] A separate staff statement observed that at least some firms implemented capabilities that are able to control, monitor, and inspect all incoming and outgoing network traffic to prevent unauthorized or harmful traffic and implemented capabilities that are able to detect threats on endpoints.[649] In the two Commission exam sweeps, many firms indicated that policies and procedures were vetted and approved by senior management and that firms provided annual cybersecurity reports to the board while some also provided ad hoc reports in the event of major cybersecurity events.[650] Broadly, many broker-dealers reported relying on industry standards with respect to cybersecurity[651] typically by adhering to a specific industry standard or combination of industry standards or by using industry standards as guidance in designing policies and procedures.

With respect to broker-dealer reporting to their boards regarding cybersecurity policies and procedures and cybersecurity incidents, the board reporting frequency ranged from quarterly

---

647 *See* FINRA Report on Selected Cybersecurity Practices. This report noted that FINRA has conducted a voluntary Risk Control Assessment ("RCA") Survey with all active member firms for a number of years. According to the 2018 RCA, 94% of higher revenue firms and 70% of mid-level revenue firms use a risk assessment as part of their cybersecurity program.

648 *Id*. According to FINRA's 2018 RCA, 100% of higher revenue firms include penetration testing as a component in their overall cybersecurity program.

649 *See* EXAMS Cybersecurity and Resiliency Observations.

650 *See* FINRA, *Report on Cybersecurity Practices* (Feb. 2015), *available at* https://www.finra.org/sites/default/files/2020-07/2015-report-on-cybersecurity-practices.pdf ("FINRA Report on Cybersecurity Practices").

651 *Id.* Among the firms that were part of the sweep, nearly 90% used one or more of the NIST, International Organization for Standardization ("ISO") or Information Systems Audit and Control Association ("ISACA") frameworks or standards. More specifically, 65% of the respondents reported that they use the ISO 27001/27002 standard while 25% use the Control Objectives for Information and Related Technologies ("COBIT") framework created by ISACA. Some firms use combinations of these standards for various parts of their cybersecurity programs. While the report focused on firm utilization of cybersecurity frameworks specifically, in many cases, the referenced frameworks were broader IT frameworks.

to ad-hoc among the firms FINRA reviewed.[652] Approximately two-thirds of the broker-dealers (68%) examined in a 2015 survey had an individual explicitly assigned as the firm's CISO which might suggest extensive executive leadership engagement.

There are no current Commission or FINRA requirements for broker-dealers to disseminate notifications of breaches to members or clients although many firms do so[653] pursuant to various state data breach laws.[654] Broker-dealers are subject to state laws known as "Blue Sky Laws," which generally are regulations established as safeguards for investors against securities fraud.[655] All 50 states have enacted laws in recent years requiring firms to notify individuals of data breaches. These laws differ by state, with some states imposing heightened notification requirements relative to other states.[656]

ii. SROs

National securities exchanges, registered clearing agencies, FINRA, and the MSRB are all SROs and are all considered to be SCI Entities, which requires them to comply with Regulation SCI.[657] As discussed earlier, Regulation SCI has provisions requiring policies and

---

652 *See* FINRA Report on Cybersecurity Practices. At a number of firms, the board received annual cybersecurity-related reporting while other firms report on a quarterly basis. A number of firms also provide ad hoc reporting to the board in the event of major cybersecurity events.

653 *See* Cybersecurity Examination Sweep Summary. Based on a small sample of firms, the vast majority of broker-dealers maintained plans for data breach incidents and most had plans for notifying customers of material events.

654 *See* Digital Guardian, *The Definitive Guide to U.S. State Data Breach Laws* (Nov. 15, 2022), *available at* https://info.digitalguardian.com/rs/768-OQW-145/images/the-definitive-guide-to-us-state-data-breach-laws.pdf.

655 *See, e.g.*, Office of Investor Education and Advocacy, Commission, *Blue Sky Laws*, *available at* https://www.investor.gov/introduction-investing/investing-basics/glossary/blue-sky-laws.

656 For example, some states may require a firm to notify individuals when a data breach includes biometric information, while others do not. *Compare* Cal. Civil Code § 1798.29 (stating that notice to California residents of a data breach is generally required when a resident's personal information was or is reasonably believed to have been acquired by an unauthorized person and that "personal information" is defined to mean an individual's first or last name in combination with one of a list of specified elements, which includes certain unique biometric data), *with* Ala. Stat. §§ 8-38-2, 8-38-4, 8-38-5 (stating that notice of a data breach to Alabama residents is generally required when sensitive personally identifying information has been acquired by an unauthorized person and is reasonably likely to cause substantial harm to the resident to whom the information relates and that "sensitive personally identifying information" is defined as the resident's first or last name in combination with one of a list of specified elements, which does not include biometric information).

657 *See* 17 CFR 242.1000 through 1007.

procedures to address certain types of cybersecurity risks.[658] Regulation SCI also requires immediate written or telephonic notice and subsequent reporting to the Commission on Form SCI of certain types of incidents.[659] Finally, Regulation SCI has provisions requiring disclosures to persons affected by certain incidents.[660]

In addition, as described above, Rule 613 of Regulation NMS requires the Participants to jointly develop and submit to the Commission a CAT NMS Plan.[661] The Participants conduct the activities of the CAT through a jointly owned limited liability company, Consolidated Audit Trail, LLC. The CAT is intended to function as a modernized audit trail system that provides regulators with more timely access to a comprehensive set of trading data, thus enabling regulators to more efficiently and effectively reconstruct market events, monitor market behavior, and investigate misconduct. The CAT System accepts data that are submitted by the Participants and broker-dealers, as well as data from certain market data feeds like SIP and OPRA.[662]

FINRA CAT, LLC – a wholly-owned subsidiary of FINRA – has entered into an agreement with the Company to act as the Plan Processor and, as such, is responsible for building, operating and maintaining the CAT. However, because the CAT System is owned and operated by FINRA CAT, LLC on behalf of the national securities exchanges and FINRA, the Participants remain ultimately responsible for the performance of the CAT and its compliance with statutes, rules, and regulations.

---

658 *See* section II.F.1.c. of this release (discussing in more detail the existing requirements of Regulation SCI to have policies and procedures to address certain cybersecurity risks).

659 *See* section II.F.1.d. of this release (discussing in more detail the existing immediate notification and subsequent reporting requirements of Regulation SCI).

660 *See* section II.F.1.e. of this release (discussing in more detail the existing disclosure requirements of Regulation SCI).

661 *See* 17 CFR 242.613*; see also* section II.F.1.c. of this release (discussing the CAT NMS Plan in general and describing the roles of the Participants and Plan Processor).

662 CAT data is not public, although some information in the CAT may be available through public sources (*e.g.*, market data feeds like the SIP or proprietary exchange feeds).

Under the Commission approved CAT NMS Plan, the Plan Processor must develop various policies and procedures related to data security, including a comprehensive information security program that includes, among other things, requirements related to: (1) connectivity and data transfer, (2) data encryption, (3) data storage, (4) data access, (5) breach management, including requirements related to the development of a cyber incident response plan and documentation of all information relevant to breaches, and (6) personally identifiable information data management.[663] As part of this requirement, the Plan Processor is required to create and enforce policies, procedures, and control structures to monitor and address CAT data security, including reviews of industry standards[664] and periodic penetration testing.[665] Under the CAT NMS Plan the comprehensive information security program must be updated by the Plan Processor at least annually.[666] Furthermore, both the Participants and the Plan Processor must also implement various data confidentiality measures that include safeguards to secure access and use of the CAT.[667] The Plan Processor must also review Participant information security policies and procedures related to the CAT to ensure that such policies and procedures are comparable to those of the CAT System.[668] In addition to these policies and procedures

---

663 *See* CAT NMS Plan, appendix D, sections 4 and 6.12.

664 The Company is subject to certain industry standards with respect to its comprehensive information security program, including but not limited to: NIST 800-23 (Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Test/Evaluated Products), NIST 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations), NIST 800-115 (Technical Guide to Information Security Testing and Assessment), and, to the extent not otherwise specified, all other provisions of the NIST cyber security framework. *See* CAT NMS Plan, Appendix D, section 4.2.

665 *Id*. at section 6.2(b)(v); Appendix D, sections 4 and 6.12.

666 *See* CAT NMS Plan at Appendix D, section 4.1.

667 Specifically, the measures implemented by the Plan Processor must include, among other things: (1) restrictions on the acceptable uses of CAT Data; (2) role-based access controls; (3) authentication of individual users; (4) MFA and password controls; (5) implementation of information barriers to prevent unauthorized staff from accessing CAT Data; (6) separate storage of sensitive personal information and controls on transmission of data; (7) security-driven monitoring and logging; (8) escalation of non-compliance events or security monitoring; and (9) remote access controls. *Id*. at Appendix D, sections 4.1, 5.3, 8.1.1, and 8.2.2; section 6.2(a)(v)(J)-(L); section 6.2(b)(vii); section 6.5(c)(i); section 6.5(f).

668 CAT NMS Plan at section 6.2(b)(vii).

requirements,[669] the CAT NMS Plan requires several forms of periodic review of CAT, including an annual written assessment,[670] regular reports,[671] and an annual audit.[672]

iii. SBS Entities

Section 15F(j)(2) of the Exchange Act, among other things, requires each SBS Entity to establish robust and professional risk management systems adequate for managing its day-to-day business.[673] Additionally, certain SBS Entities must comply with specified provisions of Rule 15c3-4 and, therefore, establish, document, and maintain a system of internal risk management controls to assist in managing the risks associated with their business activities.[674] Further, SBS Entities could be subject to Regulation S-ID if they are "financial institutions" or "creditors."[675]

---

669 In August 2020, the Commission proposed certain amendments to the CAT NMS Plan that are designed to enhance the security of the CAT. *See* https://www.sec.gov/rules/proposed/2020/34-89632.pdf.

670 The Participants are required to provide the Commission with an annual written assessment of the Plan Processor's performance, which must include, among other things, an evaluation of potential technology upgrades and an evaluation of the CAT information security program. *Id*. at section 6.6(b); section 6.2(a)(v)(G).

671 The Plan Processor is required to provide the operating committee with regular reports on various topics, including data security issues and the Plan Processor. *Id*. at section 6.1(o); section 6.2(b)(vi); section 6.2(a)(v)(E); and section 4.12(b)(i).

672 The Plan Processor is required to create and implement an annual audit plan that includes a review of all Plan Processor policies, procedures, control structures, and tools that monitor and address data security, in addition to other types of auditing practices. *Id*. at section 6.2(a)(v)(B)-(C); Appendix D, section 4.1.3; Appendix D, section 5.3.

673 15 U.S.C. 78o-10(j). The Commission also requires that specified SBS Entity trading relationship documentation include the process for determining the value of each security-based swap for purposes of complying with, among other things, the risk management requirements of section 15F(j) of the Exchange Act and paragraph (h)(2)(iii)(I) of Rule 15Fh-3, and any subsequent regulations promulgated pursuant to section 15F(j). *See* 17 CFR 140.15Fi-5(b)(4). The documentation must include *either:* (1) alternative methods for determining the value of the security-based swap in the event of the unavailability or other failure of any input required to value the security-based swap for such purposes; or (2) a valuation dispute resolution process by which the value of the security-based swap shall be determined for the purposes of complying with the rule. *See* 17 CFR 140.15Fi-5(b)(4)(ii). Further, SBS Entities must engage in portfolio reconciliation to resolve discrepancies, among other things. *See* 17 CFR 240.15Fi-3(a) and (b). Such discrepancies include those resulting from a cybersecurity incident.

674 *See* 17 CFR 240.15c3-1(a)(7)(iii) (applies to broker-dealers authorized to use models, including broker-dealers dually registered as an SBSD); 17 CFR 240.15c3-1(a)(10)(ii) (applies to broker-dealers not authorized to use models that are dually registered as an SBSD); 17 CFR 240.18a-1(f) (applies to SBSDs that are not registered as a broker-dealer, other than an OTC derivatives dealer, and that do not have a prudential regulator); 17 CFR 240.18a-2(c) (applies to MSBSPs); *see also* 17 CFR 240.15c3-4*; see* section IV.C.1.b.i. of this section (discussing requirements of Rule 15c3-4).

675 *See* 17 CFR 248.201 and 202. The scope of Regulation S-ID includes any financial institution or creditor, as defined in the Fair Credit Reporting Act (15 U.S.C. 1681) that is required to be "registered under the

SBS Entities are subject to additional Commission rules to have risk management policies and procedures, to review policies and procedures, to report information about compliance to the Commission, and to disclose certain risks to their counterparties. For example, paragraph (h) of Rule 15Fh-3 requires, among other things, that an SBSD or MSBSP establish, maintain, and enforce written policies and procedures regarding the supervision of the types of security-based swap business in which it is engaged and the activities of its associated persons that are reasonably designed to prevent violations of applicable federal securities laws and the rules and regulations thereunder.[676] The policies and procedures must include, among other things: (1) procedures for a periodic review, at least annually, of the security-based swap business in which the SBS Entity engages and (2) procedures reasonably designed to comply with duties set forth in section 15F(j) of the Exchange Act, such as risk management duties set forth in section 15F(j)(2).[677]

Paragraph (b) of Rule 15Fk-1 requires each SBS Entity's CCO to, among other things, report directly to the board of directors or to the senior officer of the SBS Entity and to take reasonable steps to ensure that the SBS Entity establishes, maintains, and reviews written policies and procedures reasonably designed to achieve compliance with the Exchange Act and the rules and regulations thereunder relating to its business as an SBS Entity by: (1) reviewing its compliance with respect to the requirements described in section 15F of the Act and the rules and regulations thereunder, where the review involves preparing the an annual assessment of its written policies and procedures reasonably designed to achieve compliance with section 15F of the Act and the rules and regulations thereunder; (2) taking reasonable steps to ensure that the

---

Securities Exchange Act of 1934." *See* 17 CFR 248.201(a). Because SBS Entities are required to be so registered, an SBS Entity that is a "financial institution" or "creditor" as defined in the Fair Credit Reporting Act is within the scope of Regulation S-ID.

676 *See* 17 CFR 240.15Fh-3(h). An SBS Entity must amend its written supervisory procedures, as appropriate, when material changes occur in its business or supervisory system. Material amendments to the SBS Entity's supervisory procedures must be communicated to all associated persons to whom such amendments are relevant based on their activities and responsibilities. *See* 17 CFR 240.15Fh-3(h)(4).

677 *See* 17 CFR 240.15Fh-3(h)(2)(iii).

SBS Entity establishes, maintains, and reviews policies and procedures reasonably designed to remediate non-compliance issues identified by the chief compliance officer through any means; and (3) taking reasonable steps to ensure that the SBS Entity establishes and follows procedures reasonably designed for the handling, management response, remediation, retesting, and resolution of non-compliance issues.[678]

Paragraph (c) of Rule 15Fk-1 requires an SBS Entity to submit an annual compliance report containing, among other things, a description of: (1) its assessment of the effectiveness of its policies and procedures relating to its business as an SBS Entity; (2) any material changes to the SBS Entity's policies and procedures since the date of the preceding compliance report; (3) any areas for improvement, and recommended potential or prospective changes or improvements to its compliance program and resources devoted to compliance; (4) any material non-compliance matters identified; and (5) the financial, managerial, operational, and staffing resources set aside for compliance with the Exchange Act and the rules and regulations thereunder relating to its business as a SBSD or MSBSP, including any material deficiencies in such resources.[679] The compliance report must be submitted to the Commission within 30 days following the deadline for filing the SBS Entity's annual financial report.[680]

SBS Entities' operations also are governed, in part, by paragraph (b) of Rule 15Fh-3 in that they must, at a reasonably sufficient time prior to entering into a security-based swap, disclose to a counterparty (other than a SBSD, MSBSP, swap dealer, or major swap participant) material information concerning the security-based swap in a manner reasonably designed to allow the counterparty to assess material risks and characteristics as well as material incentives

---

678 *See* 17 CFR 240.15Fk-1(b)(2). The CCO also must administer each policy and procedure that is required to be established pursuant to section 15F of the Exchange Act and the rules and regulations thereunder. *See* 17 CFR 240.15Fk-1(b)(4).

679 *See* 17 CFR 240.15Fk-1(c)(2).

680 *Id.*

or conflicts of interest.[681] Relevant risks may include market, credit, liquidity, foreign currency, legal, operational, and any other applicable risks.[682] Further, SBSDs must establish, maintain, and enforce written policies and procedures reasonably designed to obtain and retain a record of the essential facts concerning each counterparty whose identity is known to the SBSD that are necessary for conducting business with such counterparty.[683] Among other things, the essential facts regarding the counterparty are facts required to implement the SBSD's operational risk management policies in connection with transactions entered into with such counterparty.[684]

iv. SBSDRs

Section 13(n) of the Exchange Act specifies the requirements and core principles with which SBSDRs are required to comply. The Commission adopted rules that cover the receiving and maintenance of security-based swap data, how entities can access such information, and the maintaining the continued privacy of confidential information. Security-based swap data repositories must have written policies and procedures reasonably designed to review any prohibition or limitation of any person with respect to access to services offered, directly or indirectly, or data maintained by the SBSDR.[685]

The SBSDRs must enforce written policies and procedures reasonably designed to protect the privacy of security-based swap transaction information.[686] As a result, they must establish and maintain safeguards, policies, and procedures reasonably designed to prevent the misappropriation or misuse, directly or indirectly, of confidential information, including, but not limited to, trade data; position data; and any nonpublic personal information about a market participant or any of its customers, material, nonpublic information, and/or intellectual property,

---

681 *See* 17 CFR 240.15Fh-3(b).

682 *See* 17 CFR 240.15Fh-3(b)(1).

683 *See* 17 CFR 240.15Fh-3(e).

684 *See* 17 CFR 240.15Fh-3(e)(2).

685 17 CFR 240.13n-4(c)(1)(iv).

686 17 CFR 240.13n-9(b)(1).

such as trading strategies or portfolio positions, by the SBSDR or any person associated with the SBSDR for personal benefit or for the benefit of others. Such safeguards, policies, and procedures must address, without limitation: (1) limiting access to such confidential information, material, nonpublic information, and intellectual property; (2) standards pertaining to trading by persons associated with the SBSDR for their personal benefit or for the benefit of others; and (3) adequate oversight to ensure compliance with these safeguards. These rules cover potential unauthorized access from within or outside of the SBSDR, which could include a cybersecurity breach.[687]

Additionally, a SBSDR must furnish to a market participant, prior to accepting its securities-based swap data, a disclosure document that contains information from which the market participant can identify and evaluate accurately the risks and costs associated with using the services of the SBSDR.[688] Key points include, among other things, the criteria for providing others with access to services offered and data maintained by the SBSDR; criteria for those seeking to connect to or link with the SBSDR; policies and procedures regarding the SBDR's safeguarding of data and operational reliability, as described in Rule 13n-6; policies and procedures reasonably designed to protect the privacy of any and all security-based swap transaction information that the SBSDR receives from a SBSD, counterparty, or any registered entity, as described in Rule 13n-9(b)(1); policies and procedures regarding its non-commercial and/or commercial use of the security-based swap transaction information that it receives from a market participant, any registered entity, or any other person; dispute resolution procedures involving market participants, as described in Rule 13n-5(b)(6); and governance arrangements of the swap-based security data repository.[689]

v. Transfer Agents

---

687 17 CFR 240.13n-9(b)(2).

688 *See* 17 CFR 240.13n-10.

689 *See* 17 CFR 240.13n-10(b).

Transfer agents registered with the Commission (but not transfer agents registered with another appropriate regulatory agency) are subject to the Regulation S-P Disposal Rule.[690] Transfer agents also may be subject to Regulation S-ID if they are "financial institutions" or "creditors."[691] As discussed earlier, the Regulation S-P Disposal Rule and Regulation S-ID have provisions requiring policies and procedures to address certain types of cybersecurity risks.[692]

Rule 17Ad-12 requires transfer agents to ensure that all securities are held in safekeeping and are handled, in light of all facts and circumstances, in a manner that is reasonably free from risk of theft, loss, or destruction. In addition, the transfer agent must ensure that funds are protected, in light of all facts and circumstances, against misuse. In evaluating which particular safeguards and procedures must be employed, the cost of the various safeguards and procedures as well as the nature and degree of potential financial exposure are two relevant factors.[693]

Transfer agents are subject indirectly to state corporation law when acting as agents of corporate issuers, and they are directly subject to state commercial law, principal-agent law, and other laws, many of which are focused on corporate governance and the rights and obligations of issuers and securityholders.[694] The transfer of investment securities is primarily governed by UCC Article 8, which has been adopted by the legislatures of all 50 states,[695] the District of Columbia, Puerto Rico, and the Virgin Islands. Transfer agents may also be subject to the laws

---

690 *See* 17 CFR 248.30(b)(2).

691 *See* 17 CFR 248.201 and 202. The scope of Regulation S-ID includes any financial institution or creditor, as defined in the Fair Credit Reporting Act (15 U.S.C. 1681) that is required to be "registered under the Securities Exchange Act of 1934." *See* 17 CFR 248.201(a).

692 *See* section II.F.1.c. of this release (discussing in more detail the existing requirements of the Regulation S-P Disposal Rule and Regulation S-ID to have policies and procedures to address certain cybersecurity risks).

693 17 CFR 240.17Ad-12(a).

694 *See, e.g.,* Del. Code Ann. tit. 8 (Delaware General Corporation Law), Del. Code Ann. tit. 6, art. 8 (Investment Securities), Restatement (Third) of Agency (2006).

695 Louisiana has enacted the provisions of Article 8 into the body of its law, among others, but has not adopted the UCC as a whole.

of the states of incorporation for both issuers and their securityholders that apply to specific services provided by the transfer agent, such as data privacy.[696]

c. Market Entities Subject to CFTC Regulations

Certain types of Market Entities are dually registered with the Commission and the CFTC. For example, some clearing agencies are registered with the CFTC as derivative clearing organizations ("DCOs") and some SBSDRs are registered with the CFTC as swap data repositories ("SDRs"). In addition, some broker-dealers are registered with the CFTC as futures commission merchants ("FCMs") or swap dealers. Most currently registered SBSDs are also registered with the CFTC as swap dealers. As CFTC registrants, these Market Entities are subject to requirements that pertain to cybersecurity or are otherwise relevant to the proposals in this release.

i. Requirements for DCOs

DCOs are subject to a CFTC systems safeguards rule.[697] This rule requires them—among other things—to establish and maintain: (1) a program of risk analysis and oversight with respect to their operations and automated systems to identify and minimize sources of operational risk; and (2) a business continuity and disaster recovery plan, emergency procedures, and physical, technological, and personnel resources sufficient to enable the timely recovery and resumption of operations and the fulfillment of each obligation and responsibility of the DCO, including, but not limited to, the daily processing, clearing, and settlement of transactions, following any disruption of its operations.[698] The safeguards rule also requires vulnerability and

---

696 For example, California's privacy statute which became effective in 2003, was the first significant effort by a state to assert substantive regulation of privacy of customer data. *See* Cal. Civ. Code §§ 1798.80-1798.84. While state regulations vary across jurisdictions, other states have followed suit with similar regulatory initiatives. *See, e.g.,* Minn. Stat. § 325E.61, Neb. Rev. Stat. §§ 87-801-807.

697 *See* 17 CFR 39.18.

698 *See* 17 CFR 39.18(b) and (c). The program of risk analysis and oversight must include—among other elements—information security, including, but not limited to, controls relating to: access to systems and data (including, least privilege, separation of duties, account monitoring and control); user and device

penetration testing (among other things).[699] Further, it requires notice to the CFTC staff if the DCO experiences certain exceptional events.[700]

ii. Requirements for SDRs

SDRs are subject to a CFTC systems safeguards rule.[701] This rule requires them—among other things—to: (1) establish and maintain a program of risk analysis and oversight to identify and minimize sources of operational risk through the development of appropriate controls and procedures and the development of automated systems that are reliable, secure, and have adequate scalable capacity; (2) establish and maintain emergency procedures, backup facilities, and a business continuity-disaster recovery plan that allow for the timely recovery and resumption of operations and the fulfillment of their duties and obligations as an SDR; and (3) periodically conduct tests to verify that backup resources are sufficient to ensure continued fulfillment of all their duties under the Commodity Exchange Act and the CFTC's regulations.[702] The program of risk analysis and oversight required by the SDR safeguards rule—among other things—must address: (1) information security; and (2) business continuity-disaster recovery planning and resources.[703] The safeguards rule also requires the SDR to notify the CFTC

---

identification and authentication; security awareness training; audit log maintenance, monitoring, and analysis; media protection; personnel security and screening; automated system and communications protection (including, network port control, boundary defenses, encryption); system and information integrity (including, malware defenses, software integrity monitoring); vulnerability management; penetration testing; security incident response and management; and any other elements of information security included in generally accepted best practices. *See* 17 CFR 39.18(b)(2)(i).

699 *See* 17 CFR 39.18(e).

700 *See* 17 CFR 39.18(g).

701 *See* 17 CFR 49.24.

702 *See* 17 CFR 49.24(a).

703 *See* 17 CFR 49.24(b)(2) and (3). For the purposes of the SDR safeguards rule, information security includes, but is not limited to, controls relating to: access to systems and data (including least privilege, separation of duties, account monitoring and control); user and device identification and authentication; security awareness training; audit log maintenance, monitoring, and analysis; media protection; personnel security and screening; automated system and communications protection (including network port control, boundary defenses, encryption); system and information integrity (including malware defenses, software integrity monitoring); vulnerability management; penetration testing; security incident response and management; and any other elements of information security included in generally accepted best practices. *See* 17 CFR 49.24(b)(2).

promptly of—among other events—all cyber security incidents or targeted threats that actually or potentially jeopardize automated systems operation, reliability, security, or capacity.[704]

iii. Requirements for FCMs and Swap Dealers

The CFTC does not have a cybersecurity regime for FCMs and swap dealers comparable to that being proposed in this release.[705] However, FCMs and swap dealers are currently subject to information security requirements by virtue of their membership with the National Futures Association (NFA).[706] Specifically, NFA examines swap dealers and FCMs for compliance with NFA Interpretive Notice 9070, which establishes general requirements for NFA members relating to their information systems security programs (ISSPs).[707] The notice requires members to adopt and enforce a written ISSP reasonably designed to provide safeguards to protect against security threats or hazards to their technology systems. The safeguards must be appropriate to the member's size, complexity of operations, type of customers and counterparties, the sensitivity of the data accessible within its systems, and its electronic interconnectivity with other entities. The notice further provides guidance on how to meet this requirement, including that members should document and describe the safeguards in the ISSP, identify significant internal

---

704 *See* 17 CFR 49.24(g)(2).

705 Current CFTC requirements relating to information security for FCMs and swap dealers are more general in nature or limited in application. *See*, *e.g.*, 17 CFR 23.600(c)(4)(vi) (providing that swap dealer's risk management program policies and procedures shall take into account, among other things, secure and reliable operating and information systems with adequate, scalable capacity, and independence from the business trading unit; safeguards to detect, identify, and promptly correct deficiencies in operating and information systems; and reconciliation of all data and information in operating and information systems); 162.21, 160.30 (requiring FCMs and swap dealers to adopt written policies and procedures addressing administrative, technical, and physical safeguards with respect to the information of consumers). The current CFTC Chairman has, however, announced support for developing cybersecurity requirements for FCMs and swap dealers. *See* CFTC, Address of Chairman Rostin Behnam at the ABA Business Law Section Derivatives & Futures Law Committee Winter Meeting (Feb. 3, 2023), *available at* https://www.cftc.gov/PressRoom/SpeechesTestimony/opabehnam31.

706 *See* NFA, *Interpretive Notice 9070—NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs* (Sept. 30, 2019), *available at* https://www.nfa.futures.org/rulebooksql/rules.aspx?RuleID=9070&Section=9. NFA has also issued guidance relating to the oversight of third-party service providers. *See* NFA, *Interpretive Notice 9079 - NFA Compliance Rules 2-9 and 2-36: Members' Use of Third-Party Service Providers* (Sept. 30, 2021), *available at* https://www.nfa.futures.org/rulebooksql/rules.aspx?Section=9&RuleID=9079.

707 *Id.*

and external threats and vulnerabilities, create an incident response plan, and monitor and regularly review their ISSPs for effectiveness, among other things. Members should also have procedures to promptly notify NFA in the form and manner required of a cybersecurity incident related to the member's commodity interest business and that results in: 1) any loss of customer or counterparty funds; 2) any loss of a member's own capital; or 3) in the member providing notice to customers or counterparties under state or federal law.

The CFTC does require swap dealers to establish and maintain a business continuity and disaster recovery plan that outlines the procedures to be followed in the event of an emergency or other disruption of their normal business activities.[708] The business continuity and disaster recovery plan must be designed to enable the swap dealer to continue or to resume any operations by the next business day with minimal disturbance to its counterparties and the market, and to recover all documentation and data required to be maintained by applicable law and regulation.[709] The business continuity and disaster recovery plan must—among other requirements—be tested annually by qualified, independent internal personnel or a qualified third party service.[710] The date the testing was performed must be documented, together with the

---

[708] *See* 17 CFR 23.603. The business continuity and disaster recovery plan must include: (1) the identification of the documents, data, facilities, infrastructure, personnel and competencies essential to the continued operations of the swap dealer and to fulfill its obligations; (2) the identification of the supervisory personnel responsible for implementing each aspect of the business continuity and disaster recovery plan and the emergency contacts required to be provided; (3) a plan to communicate with specific persons the in the event of an emergency or other disruption, to the extent applicable to the operations of the swap dealer; (4) procedures for, and the maintenance of, back-up facilities, systems, infrastructure, alternative staffing and other resources to achieve the timely recovery of data and documentation and to resume operations as soon as reasonably possible and generally within the next business day; (5) maintenance of back-up facilities, systems, infrastructure and alternative staffing arrangements in one or more areas that are geographically separate from the swap dealer's primary facilities, systems, infrastructure and personnel (which may include contractual arrangements for the use of facilities, systems and infrastructure provided by third parties); (6) back-up or copying, with sufficient frequency, of documents and data essential to the operations of the swap dealer or to fulfill the regulatory obligations of the swap dealer and storing the information off-site in either hard-copy or electronic format; and (7) the identification of potential business interruptions encountered by third parties that are necessary to the continued operations of the swap dealer and a plan to minimize the impact of such disruptions. *See* 17 CFR 23.603(b).

[709] *See* 17 CFR 23.603(a).

[710] *See* 17 CFR 23.603(g).

nature and scope of the testing, any deficiencies found, any corrective action taken, and the date that corrective action was taken.[711]

d. Market Entities Subject to Federal Banking Regulations

Broker-dealers affiliated with a banking organization[712] and some SBS Entities and transfer agents that are banking organizations are subject to the requirements of prudential regulators such as the FDIC, Federal Reserve Board, and the OCC. These prudential regulators have rules requiring banking organizations to notify them no later than 36 hours after learning of a "computer-security incident," which is defined "as an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits."

The rule also requires a bank service provider to notify at least one bank-designated point of contact at each affected customer bank as soon as possible when it determines it has experienced a computer-security incident that has materially disrupted or degraded, or is reasonably likely to disrupt or degrade, covered services provided to the bank for four or more hours. If the bank has not previously provided a designated point of contact, the notification must be made to the bank's chief executive officer ("CEO") and CIO or to two individuals of comparable responsibilities."[713] Prudential regulators have also published guidance for banking organizations relating to cybersecurity.[714]

---

711 *Id.*

712 In the simplification of the Volcker Rule, effective Jan. 21, 2020, Commission staff estimated that there were 202 broker-dealers that were affiliated with banking organizations.

713 *See* 12 CFR 53.1 through 53.4 (OCC); 12 CFR 225.300 through 225.303 (Federal Reserve Board); 12 CFR 304.21 through 24 (FDIC).

714 *See, e.g.*, *SR 21-14: Authentication and Access to Financial Institution Services and Systems* (Aug. 11, 2021), *available at* https://www.federalreserve.gov/supervisionreg/srletters/sr2114.htm; *SR 15-9: FFIEC Cybersecurity Assessment Tool for Chief Executive Officers and Boards of Directors* (July 2, 2015), *available at* https://www.federalreserve.gov/supervisionreg/srletters/sr1509.htm; *SR 05-23 / CA 05-10: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (Dec. 1, 2005), *available at* https://www.federalreserve.gov/boarddocs/srletters/2005/SR0523.htm.

e. Information Sharing

Information sharing is an important part of cybersecurity. Alerts that are issued by the Commission or by the securities industry make Market Entities aware of trends in cybersecurity incidents and potential threats. This advanced warning can help Market Entities to prepare for future cybersecurity attacks by testing and upgrading their cybersecurity infrastructure.

The value of such information sharing has long been recognized. In 1998, Presidential Decision Directive 63 established industry-based information sharing and analysis centers ("ISACs") to promote the disclosure and sharing of cybersecurity information among firms.[715] The FS-ISAC provides financial firms with such a forum.[716] However, observers have questioned the efficacy of these information-sharing partnerships.[717] Although the Commission does not have data on the extent of Market Entities' use of such forums or their efficacy, surveys of securities firms conducted by FINRA suggest that there is considerable variation in firms' willingness to share information about cybersecurity threats on a voluntary basis, with larger firms being more likely to do so.[718] Similarly, a recent survey of financial firms found that while recognition of the value of information-sharing arrangements is widespread, the majority of firms report hesitance to participate due to regulatory restrictions or privacy concerns.[719]

---

715 *See President Decision Directive/NSC-63, Critical Infrastructure Protection* (May 22, 1998); *Presidential Decision Directive 63, Critical Infrastructure Protection: Sector Coordinators*, 98 FR 41804 (Aug. 5, 1998) (notice and request for expressions of interest); *see also* National Council of ISACs, *available at* https://www.nationalisacs.org.

716 Information about FS-ISAC is *available at* https://www.fsisac.com.

717 *See* James A. Lewis and Denise E. Zheng, *Cyber Threat Information Sharing*, 2015 Cre. for Strategic and Int'l Stud. 62 (Mar. 2015) (stating that the "benefits of information sharing, when done correctly, are numerous" but that [p]rogrammatic, technical, and legal challenges, as well as lack of buy-in from the stakeholder community, are the key impediments" to effective information-sharing partnerships).

718 *See* FINRA Report on Cybersecurity Practices. Survey respondents included large investment banks, clearing firms, online brokerages, high-frequency traders, and independent dealers.

719 *See* Julie Bernard, Mark Nicholson, and Deborah Golden, *Reshaping the Cybersecurity Landscape*, Deloitte (Jul. 24, 2020), *available at* https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html ("Reshaping the Cybersecurity Landscape"). Survey respondents consisted of CISOs (or equivalent) of 53 members of the FS-ISAC. Of the respondents, 24 reported being in the retail/corporate banking sector, 20 reported being in the consumer/financial services (non-banking) sector, and 17 reported being in the insurance sector. Other respondents included IT service providers, financial utilities, trade associations, and credit unions. Some respondents reported being in multiple sectors.

Market surveillance and regulatory activities—such as enforcement by SROs—can result in information sharing with—and referrals to—the Commission and other federal agencies, particularly if the issues being investigated are cybersecurity related.

f. Adequacy of Current Cybersecurity Policies and Procedures

While spending on cybersecurity measures in the financial services industry is considerable, and the growing risk of cybersecurity events has led many corporate executives to significantly increase their cybersecurity budget,[720] the budget levels themselves are not the most important facet of a cybersecurity program.[721] In a recent survey of 20 consumer/financial (non-banking) services firms, respondents ranked cybersecurity budget levels lower than other facets of cybersecurity maintenance.[722] For example, financial companies' boards and management teams indicated that overall cybersecurity strategy, the identification threats and cybersecurity risks, the firm's susceptibility to breaches when other financial institutions are successfully attacked, and the results of cybersecurity testing all ranked higher than security budgets themselves.[723] Surveys of financial services firms indicate that 10.5% of their information technology budgets are spent on cybersecurity, and the per-employee expenditure is approximately $2,348 annually as of 2020.[724] This per-employee value can be used to estimate the cybersecurity expenditures at each of the Market Entities that would be affected by the proposed rule.[725]

2. Market Structure

---

720 For example, according to one source, as of 2020, "55% of enterprise executives [were planning] to increase their cybersecurity budgets in 2021 and 51% are adding full-time cyber staff in 2021." Louis Columbus, *The Best Cybersecurity Predictions for 2021 Roundup*, Forbes.com (Dec. 15, 2020), *available at* https://www.forbes.com/sites/louiscolumbus/2020/12/15/the-best-cybersecurity-predictions-for-2021-roundup/?sh=6d6db8b65e8c.

721 *See* Reshaping the Cybersecurity Landscape.

722 *Id.*

723 *Id*.

724 *Id*.

725 The per-employee expenditure can be multiplied by the Market Entity's employee head count on a full-time equivalent basis to estimate its spending on cybersecurity protection.

a. Broker-Dealers

The operations and functions of broker-dealers are discussed earlier in this release.[726] The following broker-dealers would be Covered Entities: (1) broker-dealers that maintain custody of securities and cash for customers or other broker-dealers (*i.e.*, carrying broker-dealers); (2) broker-dealers that introduce their customer accounts to a carrying broker-dealer on a fully disclosed basis (*i.e.*, introducing broker-dealers); (3) broker-dealers with regulatory capital equal to or exceeding $50 million; (4) broker-dealers with total assets equal to or exceeding $1 billion; (5) broker-dealers that operate as market makers; and (6) broker-dealers that operate an ATS.[727] Broker-dealers that do not fall into one of those six categories would not be Covered Entities (*i.e.*, they would be Non-Covered Broker-Dealers). As discussed above, broker-dealers that are Covered Entities would be subject to additional policies and procedures, reporting, and disclosure requirements under proposed Rule 10.[728] These additional requirements would not apply to broker-dealers that are not Covered Entities.[729]

Table 1 presents a breakdown of all broker-dealers registered with the Commission as of the third quarter of 2022. Based on 2022 FOCUS Part II/IIA data, there were 3,510 registered broker-dealers with average total assets of $1.5 billion and average regulatory capital of $144 million. Of those broker-dealers, 1,541 would be classified as Covered Entities with average total assets of $3.5 billion and average regulatory capital of $325 million. Meanwhile, the 1,969 brokers that would be classified as Non-Covered Broker-Dealers were generally much smaller than broker-dealers that would be classified as Covered Entities, having an average total asset level of $4.7 million and regulatory capital of $3 million. In other words, Non-Covered Broker-

---

726 *See* section I.A.2.b. of this release.

727 *See* paragraphs (a)(1)(i)(A) through (F) of proposed Rule 10.

728 *See* paragraph (b) through (d) of proposed Rule 10 (setting forth the requirements for Market Entities that meet the definition of "covered entity").

729 *See* paragraph (e) of proposed Rule 10 (setting forth the requirements for Market Entities that do not meet the definition of "covered entity").

Dealers accounted for only about 0.2 percent of total asset value and only 0.1 percent of total regulatory capital in the third quarter of 2022.

The majority of small broker-dealers, as defined by Rule 0-10[730] were classified as Non-Covered Broker-Dealers (74%) compared to a minority of small broker-dealers that were classified as Covered Entities (26%), which means that most small broker-dealers would be subject to the less stringent regulatory requirements under the proposed Rule 10 for Non-Covered Broker-Dealers. The small broker-dealers that qualified as Covered Entities and would be subject to additional requirements of proposed Rule 10 generally were broker-dealers that introduce their customer accounts to carrying broker-dealers on a fully disclosed basis.

Table 1—Broker-Dealers as Covered Entities as of September 2022
[Average broker-dealer total assets and regulatory equity]

Categories of Covered BDs	Total number of BDs	Number of small BDs Included	Number of Retail BDs	Average total assets (millions)	Average regulatory equity (millions)
Carrying	162	0	145	$28,250.9	$2,528.7
Introducing	1219	195	1106	$103.0	$44.3
Market making	19	0	1	$179.2	$17.4
ATS	36	0	21	$4.1	$3.1
>$50 Mil-lion Regulatory Equity and/or > $1 billion total assets	105	0	44	$6,891.6	$351.5
Covered	1541	195	1317	$3,523.3	$325.1
Non-Covered	1969	569	1115	$4.7	$3.0
Total	3510	764	2432	$1,549.9	$144.4

Covered Broker-Dealers provide a broad spectrum of services to their clients, including, for example: trade execution, clearing, market making, margin and securities lending, sale of

730 *See* 17 CFR 240.0-10 ("Rule 0-10") for definition of small entities including small broker-dealers under the Exchange Act for purposes of the Regulatory Flexibility Act ("RFA"). This definition is for the economic analysis only. *See also* section VI of this release (setting forth the Commission's RFA analysis).

investment company shares, research services, underwriting and selling, retail sales of corporate securities, private placements, and government and Series K securities sales and trading. In contrast, Non-Covered Broker-Dealers tend to offer a more focused and limited set of services.

In terms of specific services offered, as presented in Table 2 below, while the majority of broker-dealers that are Covered Entities have lines of business devoted to broker and dealer services across a broad spectrum of financial instruments, Non-Covered Broker-Dealers as a whole focus on private placements. In addition, a significant minority of Non-Covered Broker-Dealers also engages in mutual fund sales and underwriting, variable contract sales, corporate securities underwriting, and direct investment offerings.

Table 2—Lines of Business at Broker-Dealers as of September 2022*

[Percent of Covered Entity and Non-Covered Broker-Dealers engaged in each line of business]

Line of Business	Percent of Covered Broker-Dealers	Percent of Non-Covered Broker-Dealers
Retailing Corporate Equity Securities Over The Counter	76.4%	8.1%
Corporate Debt Securities	69.6%	7.9%
Mutual Funds	62.2%	19.5%
Private Placements	58.1%	72.1%
Options	58.1%	3.7%
US Government Securities Broker	56.2%	3.9%
Municipal Debt/Bonds - Broker	53.1%	6.4%
Other Securities Business	52.0%	65.1%
Underwriter - Corporate Securities	45.0%	11.5%
Trading Via Floor Broker	43.4%	5.7%
Variable Contracts	42.4%	16.3%
Proprietary Trading	40.4%	3.8%
Investment Advisory Services	25.8%	4.6%
Municipal Debt/Bonds - Dealer	25.4%	1.5%
Direct investments – Primary	21.2%	13.2%
US Government Securities Dealer	20.7%	0.9%
Other Non-Securities Business	18.1%	11.2%
Time Deposits	16.5%	1.2%
Commodities	12.5%	1.1%
Market Making	12.3%	0.6%

Mortgage or Asset Backed Securities	11.9%	1.3%
Bank Networking/Kiosk Relationship	11.0%	0.4%
Internet/Online Trading Accounts	10.8%	0.5%
Exchange Non-Floor Activities	10.6%	0.9%
Direct investments – Secondary	8.2%	2.0%
Oil and Gas Interests	7.9%	3.1%
Underwriter - Mutual Funds	6.4%	7.8%
Exchange Floor Activities	5.9%	1.2%
Executing Broker	5.5%	0.6%
Day Trading Accounts	4.8%	0.3%
Insurance Networking/Kiosk Relationship	4.7%	0.6%
Non Profit Securities	4.2%	0.4%
Real Estate Syndication	2.8%	2.8%
Prime Broker	1.6%	0.0%
Issuer Affiliated Broker	1.2%	1.1%
Clearing Broker in a Prime Broker Arrangement	1.2%	0.0%
Crowdfunding FINRA Rule 4518 (a)	0.7%	1.1%
Funding Portal	0.2%	0.3%
Crowdfunding FINRA Rule 4518 (b)	0.1%	0.3%
Capital Acquisition Broker	0.1%	1.2%

* This information is derived from Form BD, Question 12.

As of November 2022, there were 33 NMS Stock ATSs with an effective Form ATS-N on file with the Commission[731] and 68 non-NMS Stock ATSs with a Form ATS on file with the Commission.[732] Most broker-dealer ATS operators operate a single ATS.

b. Clearing Agencies

The operations and functions of clearing agencies are discussed earlier in this release.[733] A clearing agency (whether registered with the Commission or exempt) would be considered a Covered Entity under proposed Rule 10.[734] There are a total of 16 clearing agencies that would meet the definition of a Covered Entity under proposed Rule 10. There are seven registered and active clearing agencies: DTC, FICC, NSCC, ICC, ICEEU, the Options Clearing Corp., and

---

731 *See* Form ATS-N Filings and Information, *available at* https://www.sec.gov/divisions/marketreg/form-ats-n-filings.htm.

732 *See* the current list of registered ATSs on the Commission's website, *available at* https://www.sec.gov/foia/docs/atslist.

733 *See* section I.A.2.c. of this release.

734 *See* paragraph (a)(1)(iii). of proposed Rule 10.

LCH SA. Two clearing agencies are registered with the Commission but are inactive and currently do not provide clearing and settlement activities. Those clearing agencies are the BSECC and SCCP.[735] In addition, there are five clearing agencies that are exempt from registering with the Commission. Those exempt clearing agencies are DTCC ITP Matching U.S. LLC, Bloomberg STP LLC, and SS&C Technologies, Inc., which provide matching services; and Clearstream Banking, S.A. and Euroclear Bank SA/NV, which provide clearing agency services with respect to transactions involving U.S. government and agency securities for U.S. participants.[736]

Of the seven operating registered clearing agencies, six provide CCP clearing services and one provides CSD services. In addition, NSCC, FICC, and DTC are all registered clearing agencies that are subsidiaries of the Depository Trust and Clearing Corporation. Together, this subset of registered clearing agencies offer clearing and settlement services for equities, corporate, and municipal bonds, government and mortgage-backed securities, derivatives, money market instruments, syndicated loans, mutual funds, and alternative investment products in the United States. ICC and ICEEU are both registered clearing agencies for credit default swaps ("CDS") and are both subsidiaries of ICE. LCH SA, a France-based subsidiary of LCH Group Holdings Ltd, is a registered clearing agency that also offers clearing for CDS. The seventh registered clearing agency, the Options Clearing Corp., offers clearing services for exchange-traded U.S. equity options.

---

735 BSECC and SCCP have not provided clearing services in over a decade. *See* BSECC Notice (stating that BSECC "returned all clearing funds to its members by September 30, 2010, and [] no longer maintains clearing members or has any other clearing operations as of that date . . . . BSECC [] maintain[s] its registration as a clearing agency with the Commission for possible active operations in the future"); SCCP Notice (noting that SCCP "returned all clearing fund deposits by September 30, 2009; [and] as of that date SCCP no longer maintains clearing members or has any other clearing operations . . . . SCCP [] maintain[s] its registration as a clearing agency for possible active operations in the future."). BSECC and SCCP are included in the economic baseline and must be considered in the benefits and costs analysis due to their registration with the Commission. They also are included in the PRA for purposes of the PRA estimate. *See* section V of this release (setting forth the Commission's PRA analysis).

736 In addition to the 14 clearing agencies discussed above, the Commission's expects that two entities may apply to register or to seek an exemption from registration as a clearing agency in the next three years. As a result, they were included in the PRA in section V.

c. The MSRB

The operations and functions of the MSRB are discussed earlier in this release.[737] The MSRB would be considered a Covered Entity under proposed Rule 10.[738] As an SRO registered with the Commission, the MSRB protects municipal securities investors, municipal entities, obligated persons, and the public interest. While the MSRB used to only regulate the activities of broker-dealers and banks that buy, sell, and underwrite municipal securities, it regulates certain activities of municipal advisors.

d. National Securities Associations

The operations and functions of national securities association are discussed earlier in this release.[739] A national securities association would be considered a Covered Entity under proposed Rule 10.[740] FINRA currently is the only national securities association registered with the Commission and is a not-for-profit organization with 3,700 employees that oversees broker-dealers, including their branch offices, and registered representatives through examinations, enforcement, and surveillance.

FINRA, among other things, provides a forum for securities arbitration and mediation; conducts market regulation, including by contract for a majority of the national securities exchanges; regulates its broker-dealer members; administers testing and licensing of registered persons; collects and stores regulatory filings;[741] and operates industry utilities such as Trade Reporting Facilities.[742] Through the collection of regulatory filings submitted by broker-dealers

---

737 *See* section I.A.2.d. of this release.

738 *See* paragraph (a)(1)(iv) of proposed Rule 10.

739 *See* section I.A.2.e. of this release.

740 *See* paragraph (a)(1)(i)(v) of proposed Rule 10.

741 Some of the filings collected include FOCUS reports; Form OBS; Form SSOI; Form Custody; firm clearing arrangements filings; Blue Sheets; customer margin balance reporting; short interest reporting; Form PF; Form 211; public offering and private placement related filings; FINRA Rules 4311 and 4530 reporting; subordination agreements; and Regulations M, T, and NMS.

742 These include Trade Reporting and Compliance Engine (TRACE), OTC ATS and Non-ATS data, Over-the-Counter Reporting Facility (ORF), Trade Reporting Facility (TRF), Alternative Display Facility (ADF), and Order Audit Trail System (OATS) (phased out as of 2021).

as well as stock options and fixed-income quote, order, and trade data, FINRA maintains certain confidential information – not only its own but of other SROs.

e. National Securities Exchanges

The operations and functions of the national securities exchanges are discussed earlier in this release.[743] A national securities exchange would be considered a Covered Entity under proposed Rule 10.[744] There are 24 national securities exchanges[745] currently registered with the Commission that would meet the definition of a Covered Entity under proposed Rule 10(a)(1): BOX Exchange LLC; Cboe BYX Exchange, Inc.; Cboe BZX Exchange, Inc.; Cboe C2 Exchange, Inc.; Cboe EDGA Exchange, Inc.; Cboe EDGX Exchange, Inc.; Cboe Exchange, Inc.; Investors Exchange LLC; Long-Term Stock Exchange, Inc.; MEMX, LLC; Miami International Securities Exchange; MIAX Emerald, LLC; MIAX PEARL, LLC; Nasdaq BX, Inc.; Nasdaq GEMX, LLC; Nasdaq ISE, LLC; Nasdaq MRX, LLC; Nasdaq PHLX LLC; The Nasdaq Stock Market; New York Stock Exchange LLC; NYSE Arca, Inc.; NYSE Chicago, Inc.; NYSE American, LLC; and NYSE National, Inc.[746]

f. SBS Entities and SBSDRs

Operations and functions of SBS Entities and SBSDRs are discussed earlier in this release.[747] An SBS Entity and an SBSDR would be considered a Covered Entity under proposed Rule 10.[748] As of January 4, 2023, there were 50 registered SBSDs that would meet the

---

743 *See* section I.A.2.f. of this release.

744 *See* paragraph (a)(1)(vi) of proposed Rule 10.

745 Exempt securities exchanges governed by section 5 of the Act are not considered to be national securities exchanges.

746 Two exchanges, The Island Futures Exchange, LLC, and NQLX LLC, were formerly registered with the Commission as national securities exchanges.

747 *See* sections I.A.2.g. and I.A.2.h. of this release.

748 *See* paragraphs (a)(1)(iii), (vii), and (viii) of proposed Rule 10 (defining, respectively, MSBSPs, SBSDRs, and SBSDs as "covered entities").

definition of a Covered Entity under proposed Rule 10(a)(1).[749] There were no MSBSPs as of January 4, 2023.

There are three SBSDRs that would meet the definition of a Covered Entity under proposed Rule 10(a)(1). The Commission has two registered security-based swap data repositories (ICE Trade Vault, LLC and DTCC Data Repository (U.S.), LLC). GTR North America provides transaction reporting services for derivatives in the United States through the legal entity DTCC Data Repository (U.S.) LLC. DTCC Data Repository (U.S.), LLC enables firms to meet their reporting obligations under the Dodd-Frank Act and accepts trade submissions directly from reporting firms as well as through third-party service providers.[750] In addition to the two registered SBSDRs, the Commission expects that an additional entity may apply to be a registered SBSDR in the next three years.

g. Transfer Agents

The operations and functions of transfer agents are discussed earlier in this release.[751] Transfer agents would be Covered Entities under proposed Rule 10.[752] Transfer agents generally work for issuers of securities. Among other functions, they may: (1) track, record, and maintain on behalf of issuers the official record of ownership of each issuer's securities; (2) cancel old certificates, issue new ones, and perform other processing and recordkeeping functions that facilitate the issuance, cancellation, and transfer of securities; (3) facilitate communications between issuers and registered securityholders; and (4) make dividend, principal, interest, and other distributions to securityholders.[753] Transfer agents are required to be registered with the

---

749 *See List of Registered Security-Based Swap Dealers and Major Security-Based Swap Participants* (Jan. 4, 2023), *available at* https://www.sec.gov/tm/List-of-SBS-Dealers-and-Major-SBS-Participants.

750 *See* DTCC, *GTR North America*, *available at* https://www.dtcc.com/repository-and-derivatives-services/repository-services/gtr-north-america.

751 *See* section I.A.2.i. of this release.

752 *See* paragraph (a)(1)(ix) of proposed Rule 10.

753 *See Transfer Agent Regulations*, Exchange Act Release No. 76743 (Dec. 22, 2015), 80 FR 81948, 81949 (Dec. 31, 2015).

Commission, or if the transfer agent is a bank, then with a bank regulatory agency. As of December 31, 2022, there were 353 registered transfer agents.[754]

h. Service Providers

Many Market Entities utilize service providers to perform some or all of their cybersecurity functions. Market Entities that are large—relative to other Market Entities—in terms of their total assets, number of clients or members, or daily transactions processed are likely to have significant information technology, their own information technology departments and dedicated staff such that some functions are performed in-house. Other services may be contracted out to service providers that cater to Market Entities. Smaller Market Entities that do not have large technology budgets may rely more heavily (or completely) on third parties for their cybersecurity needs. According to a voluntary survey, financial services firms spend approximately 0.3 percent of revenue or 10% of their information technology budgets on cybersecurity, highlighting the fact that identifying vulnerabilities and having cybersecurity policies and procedures in place are more important than the actual cybersecurity budget itself, particularly with respect to expensive hardware and software.[755]

In performing their contracted duties, specialized service providers may receive, maintain, or process confidential information from Market Entities, or are otherwise permitted to access Market Entities' information systems and the information residing on those systems. Market Entities work with service providers that provide certain critical functions, such as process payment providers, regulatory services consultants, data providers, custodians, and valuation services. However, Market Entities also employ general service providers, such as email providers, relationship management systems, cloud applications, and other technology vendors.

---

754 *See* Commission, *Transfer Agent Data Sets* (Dec. 31, 2022), *available at* https://www.sec.gov/dera/data/transfer-agent-data-sets.

755 *See* Reshaping the Cybersecurity Landscape.

Regardless of their size, Market Entities typically enter into contracts with service providers to perform a specific function for a given time frame at a set price. At the conclusion of a contract, it may be renewed if both parties are satisfied. Because prices typically increase over time, there may be some need to negotiate a new fee for continued service. Negotiations also occur if additional services are requested from a given third-party provider. In the instance where additional services are required mid-contract, for example, due to increased regulatory requirements, the service provider may be able to bill for the extra work that it must incur separately to provide the additional service, particularly if that party is in a highly concentrated market for that service and can wield market power. This may be the case because that condition is specified in the contract with the Market Entity.

Service providers that cater to the securities industry with specialized services are likely to have economies of scale that allow them to more easily handle requests from Market Entities for additional services.[756] Some service providers, however, may not have the technical expertise to provide a requested additional service or may refuse to do so for other reasons. In this case, the Market Entity would need to find another service provider. The costs associated with service provider contracts, including those of renegotiating them or tacking on of supplemental fees, are passed on to the Market Entity's customers, counterparties, members, participants, or users to the extent that the Market Entities are able to do so.

D. Benefits and Costs of Proposed Rule 10, Form SCIR, and Rule Amendments

In this section, the Commission considers the benefits and costs of the rule, form, and amendments being proposed in this release.[757] As discussed earlier, proposed Rule 10 would

---

[756] *See* Bharath Aiyer et al., *New Survey Reveals $2 Trillion Market Opportunity for Cybersecurity Technology and Service Providers* (2022), *available at* https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers.

[757] Throughout the following, the Commission also considers benefits and costs related to potential effects on economic efficiency, competition, and capital formation. The Commission summarizes these effects in section IV.E. of this release.

require all Market Entities (Covered Entities and non-Covered Entities) to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks.[758] All Market Entities also, at least annually, would be required to review and assess the design and effectiveness of their cybersecurity policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review.[759] They also would be required to prepare a report (in the case of Covered Entities) or a record (in the case of non-Covered Entities) with respect to the annual review.[760] Finally, all Market Entities would need to give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring.[761]

Market Entities that meet the definition of "covered entity" would be subject to certain additional requirements under proposed Rule 10.[762] First, their cybersecurity risk management policies and procedures would need to include the following elements:

- Periodic assessments of cybersecurity risks associated with the Covered Entity's information systems and written documentation of the risk assessments;
- Controls designed to minimize user-related risks and prevent unauthorized access to the Covered Entity's information systems;
- Measures designed to monitor the Covered Entity's information systems and protect the Covered Entity's information from unauthorized access or use, and oversight of service providers that receive, maintain, or process information, or are otherwise permitted to access the Covered Entity's information systems;

---

758 *See* paragraphs (b) through (d) of proposed Rule 10 (setting forth the requirements for Market Entities that meet the definition of "covered entity"); paragraph (e)(1) of proposed Rule 10; *see also* sections II.B.1. and II.C. of this release (discussing these proposed requirements in more detail).

759 *See* paragraph (b)(2) of proposed Rule 10; paragraph (e)(1) of proposed Rule 10; *see also* sections II.B.1.f. and II.C. of this release (discussing these proposed requirements in more detail).

760 *See* paragraph (b)(2) of proposed Rule 10; paragraph (e)(1) of proposed Rule 10; *see also* sections II.B.1.f. and II.C. of this release (discussing these proposed requirements in more detail).

761 *See* paragraph (c)(1) of proposed Rule 10; paragraph (e)(2) of proposed Rule 10; *see also* sections II.B.2.a. and II.C. of this release (discussing these proposed requirements in more detail).

762 *See* paragraph (b) through (d) of proposed Rule 10 (setting forth the requirements for Market Entities that meet the definition of "covered entity"); paragraph (e) of proposed Rule 10 (setting forth the requirements for Market Entities that do not meet the definition of "covered entity").

- Measures to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the Covered Entity's information systems; and

- Measures to detect, respond to, and recover from a cybersecurity incident and written documentation of any cybersecurity incident and the response to and recovery from the incident.[763]

Second, Covered Entities would need to make certain records pursuant to the policies and procedures required under proposed Rule 10. In particular, Covered Entities would be required to document in writing periodic assessments of cybersecurity risks associated with the Covered Entity's information systems and information residing on those systems.[764] Additionally, Covered Entities would be required to document in writing any cybersecurity incident, including the Covered Entity's response to and recovery from the cybersecurity incident.[765]

Third, Covered Entities—in addition to providing the Commission with immediate written electronic notice upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring—would need to report and update information about the significant cybersecurity incident by filing Part I of proposed Form SCIR with the Commission by filing it with the Commission through the EDGAR system..[766] The form would elicit information about the significant cybersecurity incident and the Covered Entity's efforts to respond to, and recover from, the incident. Covered Entities would be required to file updated versions of proposed Form SCIR when material information becomes available or previously reported information is deemed inaccurate. Lastly, a final proposed Form SCIR would need to be submitted after a significant cybersecurity incident is resolved.

---

763 *See* sections II.B.1.a. through II.B.1.e. of this release (discussing these proposed requirements in more detail). In the case of non-Covered Entities, as discussed in more detail below in Section II.C. of this release, the design of the cybersecurity risk management policies and procedures would need to take into account the size, business, and operations of the broker-dealer. *See* paragraph (e) of proposed Rule 10.

764 *See* paragraph (b)(1)(i)(B) of proposed Rule 10; *see also* section II.B.1.a. of this release (discussing this documentation requirement in more detail).

765 *See* paragraph (b)(1)(v)(B) of proposed Rule 10; *see also* section II.B.1.e. of this release (discussing this documentation requirement in more detail).

766 *See* sections II.B.2. and II.B.4. of this release (discussing these proposed requirements in more detail).

Fourth, Covered Entities would need to disclose publicly summary descriptions of their cybersecurity risks and the significant cybersecurity incidents they experienced during the current or previous calendar year on Part II of proposed Form SCIR.[767] The form would need to be filed with the Commission through the EDGAR system and posted on the Covered Entity's public-facing business Internet website and, in the case of Covered Entities that are carrying or introducing broker-dealers, provided to customers at account opening and annually thereafter.

Rules 17a-4, 17ad-7, and 18a-6—which apply to broker-dealers, transfer agents, and SBS Entities respectively—would be amended to establish preservation and maintenance requirements for the written policies and procedures, annual reports, Parts I and II of proposed Form SCIR, and records required to be made pursuant to proposed Rule 10 (*i.e.*, the Rule 10 Records).[768] The proposed amendments would specify that the Rule 10 Records must be retained for three years. In the case of the written policies and procedures to address cybersecurity risks, the record would need to be maintained until three years after the termination of the use of the policies and procedures.[769] In addition, orders exempting certain clearing agencies from registering with the Commission are proposed to be amended to establish preservation and maintenance requirements for the Rule 10 Records that would apply to the exempt clearing agencies subject to those orders.[770] The amendments would provide that the records need to be retained for five years (consistent with Rules 13n-7 and 17a-1).[771] In the case of the written

---

767 *See* sections II.B.3. and II.B.4. of this release (discussing these proposed requirements in more detail).

768 *See* sections II.B.5. and II.C. of this release (discussing these proposed amendments in more detail). Rule 17a-4 sets forth record preservation and maintenance requirements for broker-dealers, Rule 17ad-7 sets forth record preservation and maintenance requirements for transfer agents, and Rule 18a-6 sets forth record preservation and maintenance requirements for SBS Entities.

769 *See* proposed rule 17a-4(e).

770 *See* section II.B.5. of this release (discussing these proposed amendments in more detail).

771 As discussed in section II.B.5.a. of this release, the existing requirements of Rule 13n-7 (which applies to SBSDRs) and Rule 17a-1 (which applies to registered clearing agencies, the MSRB, national securities associations, and national securities exchanges) will require these Market Entities to retain the Rule 10 Records for five years and, in the case of the written policies and procedures, for five years after the termination of the use of the policies and procedures.

policies and procedures to address cybersecurity risks, the record would need to be maintained until three years after the termination of the use of the policies and procedures.

1. Benefits and Costs of the Proposal to the U.S. Securities Markets

The Commission is proposing rules to require *all* Market Entities, based on the reasons discussed throughout, to take steps to protect their information systems and the information residing on those systems from cybersecurity risk.[772] For example, as discussed above, Market Entities may not take the steps necessary to address adequately their cybersecurity risks.[773] A Market Entity that fails to do so is more vulnerable to succumbing to a significant cybersecurity incident. As discussed earlier, a significant cybersecurity incident can cause serious harm not only to the Market Entity but also to its customers, counterparties, members, registrants, or users, as well as to any other market participants (including other Market Entities) that interact with the impacted Market Entity.[774] Therefore, it is vital to the U.S. securities markets and the participants in those markets that all Market Entities address cybersecurity risk, which, as discussed above, is increasingly threatening the financial sector.[775]

a. Benefits

The Commission anticipates that an important economic benefit of the proposal would be to protect the fair, orderly, and efficient operations of the U.S. securities markets and the soundness of Market Entities better by requiring all Market Entities to establish, maintain, and enforce written policies and procedures cybersecurity policies and procedures. As noted earlier, the average loss in the financial services industry was $18.3 million, per company per cybersecurity incident. Adopting and enforcing cybersecurity policies and procedures could assist Market Entities from incurring such losses. Furthermore, the requirement to implement

---

772 *See* section I.A.1. of this release (discussing the attractiveness of the U.S. securities market to threat actors).

773 *See* section IV.B. of this release (discussing broad economic considerations).

774 *See* section I.A.2. of this release (discussing how critical operations of Market Entities are exposed to cybersecurity risk).

775 *See* section I.A.1. of this release (discussing threats to the U.S. financial sector).

cybersecurity policies and procedures could protect potential negative downstream effects that could be incurred by other participants in the U.S. securities markets, such as the Market Entity's customers, counterparties, members, registrants, and users, in the event of a cybersecurity attack. By requiring each Market Entity to implement policies and procedures to address cybersecurity risk, the proposed rule would reduce the likelihood that one Market Entity's cybersecurity incident can adversely affect other Market Entities and market participants, as well as the U.S. securities markets at large.

In addition, FSOC has stated that "[m]aintaining and improving cybersecurity resilience of the financial sector requires continuous assessment of cyber vulnerabilities and close cooperation across firms and governments within the U.S. and internationally."[776] The information provided to the Commission under the proposed reporting requirements could help in assessing potential cybersecurity risks that affect the U.S. securities markets. The reporting of significant cybersecurity incidents also could be used to address future cyberattacks. For example, these reports could assist the Commission in identifying patterns and trends across Covered Entities, including widespread cybersecurity incidents affecting multiple Covered Entities at the same time. Further, the reports could be used to evaluate the effectiveness of various approaches that are used to respond to and recover from significant cybersecurity incidents. Therefore, requiring Covered Entities to report significant cybersecurity incidents to

---

[776] FSOC, *Annual Report (2022)*, at 70, *available at* https://home.treasury.gov/system/files/261/FSOC2022AnnualReport.pdf ("FSOC 2022 Annual Report") ("By exchanging cyber threat information within a sharing community, organizations can leverage the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats the organization may face.") *See also* NIST, Special Pub. 800-150, *Guide to Cyber Threat Information Sharing* iii (2016), *available at* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf. The NIST Special Publication also notes that the use of structured data can facilitate information sharing. *Id.* at 7 ("Structured data that is expressed using open, machine-readable, standard formats can generally be more readily accessed, searched, and analyzed by a wider range of tools. Thus, the format of the information plays a significant role in determining the ease and efficiency of information use, analysis, and exchange.").

the Commission could help assist the Commission in carrying out its mission of maintaining fair, orderly, and efficient operations of the U.S. securities markets.

Similarly, requiring Covered Entities to publicly disclose summary descriptions of their cybersecurity risks and significant cybersecurity incidents would provide enhanced transparency about cybersecurity threats that could impact the U.S. securities markets. Participants in these markets could use this additional information to enhance the management of their own cybersecurity risks, which also could serve to strengthen the resilience of the U.S. securities markets to future cybersecurity threats.

b. Costs

In general, the costs associated with the proposals include the costs of developing, implementing, documenting, and reviewing cybersecurity policies and procedures. For example, a Market Entity that has only the minimal cybersecurity protection needed to meet the current regulatory requirements may incur substantial costs when implementing the policies and procedures required by proposed Rule 10. These costs could be significantly lower for a Market Entity that currently has a well-developed and documented cybersecurity program. A Market Entity that incurs costs under the proposal may attempt to pass them on to other market participants and even other Market Entities to the extent that they are able to do that. This could increase costs for the Market Entity's customers, counterparties, members, registrants, or users participate in the U.S. securities markets.

In general, compliance costs with proposed Rule 10 would vary across the various types of Market Entities. As discussed above, one factor determining costs would be the extent to which a Market Entity's existing measures to address cybersecurity risk would comply with the proposal. Other factors would be the Market Entity's particular business model, size, and unique cybersecurity risks. While the compliance costs for smaller entities, such as Non-Covered Broker-Dealers, may be relatively smaller, those costs may not be inconsequential relative to

their size. Further, Covered Entities may incur substantial compliance costs given their relatively large size.

2. Policies and Procedures and Annual Review Requirements for Covered Entities

The definition of a "covered entity" includes a wide range of Commission registrants. The different Covered Entities that would be subject to proposed Rule 10 vary based on the types of businesses they are involved in, their relative sizes, and the number of competitors they face. As a result, the benefits and costs associated with the requirements to establish, maintain, and enforce written cybersecurity policies and procedures and to review them at least annually likely will vary among the different types of Covered Entities. Because the benefits and costs are heterogeneous across the different types of Covered Entities, the costs and benefits that are common to all Covered Entities are discussed first. Next, the benefits and costs associated with each type of Covered Entity are examined separately to account for the different operations and functions they perform and the differences in how existing or proposed regulations apply to them. The estimated cost of compliance for a given Covered Entity and for all Covered Entities combined is provided in the common costs discussion.

a. Common Benefits and Costs for Covered Entities

i. Benefits

As discussed above, due to the interconnected nature of the U.S. securities market, strong policies and procedures to address cybersecurity risks are needed by Covered Entities to protect not only themselves, but also the Market Entities with whom they do business, as well as other market participants, such as the Covered Entity's customers, counterparties, members, or users. The Commission anticipates that an important economic benefit of the cybersecurity policies and procedures and annual review requirements of proposed Rule 10 would be to reduce the cybersecurity vulnerabilities of each Market Entity and enhance the preparedness of each Market Entity against cybersecurity threats to its operations. This would reduce the likelihood that the Market Entity experiences the adverse consequences of a cybersecurity incident. With written

cybersecurity policies and procedures that are maintained and enforced, as well as periodically reviewed and assessed, Market Entities can better protect themselves against cybersecurity threats; harden the security surrounding their information systems and the data, which includes the prevention of unauthorized access; minimize the damage from successful cyberattacks; and recover more quickly from significant cybersecurity incidents when they do occur. For example, the Covered Entity's risk assessment policies and procedures would need to require written documentation of these risk assessments.[777]

Relatedly, proposed Rule 10 would require that the incident response and recovery policies and procedures include written documentation of a cybersecurity incident, including the Covered Entity's response to and recovery from the incident.[778] These records could be used by the Covered Entity to assess the efficacy of, and adherence to, its incident response and recovery policies and procedures. The record of the cybersecurity incidents further could be used as a "lessons-learned" document to help the Covered Entity respond more effectively the next time it experiences a cybersecurity incident. The Commission staff also could use the records to review compliance with this aspect of proposed Rule 10.

The records discussed above generally could be used by the Covered Entity when it performs its review to analyze whether its current policies and procedures need to be updated, to inform the Covered Entity of the risks specific to it, and to support responses to cybersecurity risks by identifying cybersecurity threats to information systems that, if compromised, could result in significant cybersecurity incidents.[779] The documentation also could be used by

---

[777] *See* paragraph (b)(1)(i)(B) of proposed Rule 10.

[778] *See* paragraph (b)(1)(v)(B) of proposed Rule 10.

[779] *See* paragraph (b)(2) of proposed Rule 10 (which would require a Covered Entity to review and assess the design and effectiveness of the cybersecurity policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review). *See also* section II.B.1.f. of this release (discussing the proposed requirements in more detail).

Commission staff and internal auditors of the Covered Entity to examine for adherence to the risk assessment policies and procedures.

Moreover, the annual review requirement is designed to require the Covered Entity to evaluate whether its cybersecurity policies and procedures continue to work as designed and whether changes are needed to ensure their continued effectiveness, including oversight of any delegated responsibilities. As discussed earlier, the sophistication of the tactics, techniques, and procedures employed by threat actors is increasing.[780] .

As discussed above, it is unlikely that Covered Entities do not currently have some minimum level of cybersecurity policies and procedures in place due to their own business decisions and certain existing regulations and oversight. However, as discussed above, current Commission regulations regarding cybersecurity policies and procedures are narrower in scope. Proposed Rule 10 aims to be comprehensive in terms of mandating that Covered Entities have cybersecurity policies and procedures that address all cybersecurity incidents that may affect their information systems and the funds and securities as well as personal, confidential, and proprietary information that may be stored on those systems. The benefits of the proposed Rule 10 would be lessened to the extent that a Covered Entity already has implemented cybersecurity policies and procedures that are generally consistent with the written policies and procedures and annual review requirements under proposed Rule 10.

If a Covered Entity has to supplement its existing cybersecurity policies and procedures, amend them, or institute annual reviews and document their assessments in a report, the benefit of proposed Rule 10 for that Covered Entity would be greater. The proposal will help ensure the Covered Entity has robust procedures in place to prevent cybersecurity incidents, may enable Covered Entities to detect cybersecurity incidents earlier, and help ensure that Covered Entities

---

780 *See* section I.A.1. of this release (discussing, for example, how cybersecurity threats are evolving); *see also* Bank of England CBEST Report (stating that "[t]he threat actor community, once dominated by amateur hackers, has expanded to include a broad range of professional threat actors, all of whom are strongly motivated, organised and funded").

have a plan in place to remediate cybersecurity incidents quickly. Lastly, as a second-order effect, it could reduce the Covered Entities' risk of exposure to other Covered Entities' cybersecurity incidents stemming—for example—from the interconnectedness of Covered Entities' information systems.

The Commission currently does not have reliable data on the extent to which each Covered Entity's existing policies and procedures are consistent with the proposed Rule 10. Therefore, it is not possible to quantify the scale of the benefits arising from the proposed policies and procedures and annual review requirements. However, given the importance of the U.S. securities markets, the value of the funds and assets that are traded and held, and the current state of transactions where much of them are electronic, it seems likely that the Covered Entities that transact business digitally have a strong incentive to implement cybersecurity policies and procedures in order to protect and maintain their operations. The proposed rule will require Covered Entities to implement stronger protections that go beyond what they do based on those market incentives.

To the extent that Covered Entities engage in business activities involving crypto assets (which depend almost exclusively on the operations of information systems), developing strong cybersecurity policies and procedures would result in large benefits for them and potentially for their customers, counterparties, members, registrants or users. For example, robust cybersecurity policies and procedures would help to ensure that Covered Entities are better shielded from the theft of crypto assets by threat actors, which may be difficult or impossible to recover, given the nature of the distributed ledger technology.[781] In addition, Covered Entities would avoid negative reputational damage associated with a successful cyberattack.

ii. Costs

---

[781] *See* section II.G. of this release (noting that there is no centralized IT infrastructure that can dynamically detect and prevent cyberattacks on wallets or prevent the transfer of illegitimately obtained crypto assets by bad actors).

The costs associated with the policies and procedures and annual review requirements of proposed Rule 10 would primarily result from compliance costs borne by Covered Entities in the design, implementation, review, written assessment, and updates of the cybersecurity policies and procedures. The proposed requirement will likely change a Covered Entity's behavior toward cybersecurity risk and necessitates a certain amount of investment in cybersecurity protection.[782] In addition to the aforementioned direct compliance costs faced by Covered Entities, those Covered Entities that utilize service providers would need to take steps to oversee them under proposed Rule 10.[783] The costs of this oversight, including direct compliance costs, ultimately would likely be passed on to the Covered Entities' customers, counterparties, members, participants, or users to the extent Covered Entities are able to do so. As indicated above, the compliance costs generally may be lessened to the extent that Covered Entities' existing policies and procedures would be consistent with the requirements of proposed Rule 10. Therefore, the marginal increase in compliance costs that arise likely would be due to the extent to which a Covered Entity needs to make modifications to its existing cybersecurity policies and procedures, implement annual reviews of those policies and procedures, and/or write assessments reports.

The compliance costs associated with developing, implementing, documenting, and reviewing the cybersecurity policies and procedures for Covered Entities' activities that involve crypto assets likely would be higher than those connected with traditional services and technologies offered and used, respectively, by Covered Entities. The cost difference primarily would be due to technological features of distributed ledger technologies as well as with the

---

782 While the existing policies and procedures of Covered Entities largely could be consistent with the requirements of proposed Rule 10, without a requirement to do so, they may not conduct annual reviews and draft assessment reports. The annual review and report costs are estimated be around $1,500 and $20,000 based on the costs of obtaining a cybersecurity audit. *See How Much Does a Security Audit Cost?*, Cyber Security Advisor (Jan. 29, 2019), *available at* https://cybersecadvisor.org/blog/how-much-does-a-security-audit-cost ("Cost of Security Audit").

783 *See* paragraphs (b)(1)(i)(A)(*2*), (b)(1)(iii)(B), and (b)(2) of proposed Rule 10.

costs increasing as a Covered Entity engages in activities with additional crypto assets and blockchains.

iii. Service Providers

As indicated above, Covered Entities may use service providers to supply them with some or all of their necessary cybersecurity protection. In general, the cost of contracted cybersecurity services depends on the size of the entity, where larger firms may offer a wider range of services and thus needing more cybersecurity protection. According to a data security provider blog, "[a]mong mid-market organizations (250-999 employees), 46% spend under $250,000 on security each year and 43% spend $250,000 to $999,999. Among enterprise organizations (1,000-9,999 employees), 57% spend between $250,000 and $999,999, 23% spend less than $250,000, and 20% spend at least $1 million. Half of large enterprises (more than 10,000 employees) spend $1 million or more on security each year and 43% spend between $250,000 and $999,999."[784]

Under the proposal, Covered Entities need to identify their service providers that receive, maintain, or process information, or are otherwise permitted to access its information systems and the information residing on those systems, and then assess the cybersecurity risks associated with their use by those service providers.[785] The policies and procedures for protecting information would require oversight of the service providers that receive, maintain, or process the Covered Entities' information, or are otherwise permitted to access the Covered Entities' information systems and the data residing on those systems, through a written contractual

---

[784] *See* Desdemona Bandini, *New Security Report: The Security Bottom Line, How Much Security Is Enough?*, (Nov. 19, 2019), *available at* https://duo.com/blog/new-security-report-the-security-bottom-line-how-much-security-is-enough.

[785] *See* paragraph (b)(1)(i)(A)(*2*) of proposed Rule 10.

agreement, as specified in paragraph (b)(iii)(B) of proposed Rule 10.[786] Service providers would be required to implement and maintain, pursuant to a written contract with the Covered Entities, appropriate measures, including the practices described in paragraph (b) of proposed Rule 10.

The proposed requirements will likely impose additional costs, at least initially, on service providers catering to Covered Entities, as they would be asked to provide services not included in existing contracts. The Commission believes that most service providers providing business-critical services would likely face pressure to enhance their cybersecurity practices to satisfy demand from Covered Entities due to new regulatory requirements placed on those Covered Entities.[787] Service providers may be willing to bear additional costs in order to continue their business relationships with the Covered Entities, particularly if the parties are operating under an ongoing contract.[788] Such situations are more likely to arise with services that are considered general information technology, such as email, relationship management, website hosting, cloud applications, and other common technologies, given that the service provider does not have market power because it has many competitors offering these services. In contrast, providers of more specialized services—such as payment service providers, regulatory service providers, data providers, custodians, and providers of valuation services—may have significant market power and may be able to charge a Covered Entity separately for the additional services that would be required under proposed Rule 10. Whether passed on to Covered Entities immediately or reflected in subsequent contract renewals, the costs associated the additional services—including the associated negotiation process—would likely be passed on to the Covered Entities' customers, counterparties, members, participants, or users to the extent that they are able to do so.

---

786 *See* paragraph (b)(1)(iii)(B) of proposed Rule 10.

787 A service provider involved in any business-critical function would likely need to receive, maintain, or process information from the Covered Entities as well as the Covered Entities' customers, counterparties, members, registrants, or users.

788 *See, e.g.,* Cost of Security Audit.

In terms of the cost of additional services received from service providers, those providers that offer a specialized service and have market power may not be willing to give any price concessions in the negotiation process. The same may be true for service providers where Covered Entities make up a small proportion of their overall business. Other service providers in a more competitive environment—such as those that offer general information technology services—may be more willing to provide a discount to keep the Covered Entity as a customer.[789] Moreover, the compliance costs for service providers of common technologies may be generally larger than those realized by firms that offer specialized services because they cater to a wider variety of customers, which makes contracts with different parties more idiosyncratic.

Some Covered Entities may find that one or several of their existing service providers may not be technically able to—or may not wish to make the investment to—support the Covered Entities' compliance with the proposed rule. Similarly, some Covered Entities may find that one or several of their existing service providers may not be able to—or wish to because of significant market power—enter into written contracts where the costs are not mutually agreeable. Also, some service providers may not want to amend their contracts and take on the particular obligations even if they already have the technical abilities. In those cases, the Covered Entities would need to change service providers and bear the associated switching costs, while the service providers would suffer loss of their customer base.[790]

For service providers that do business with Covered Entities, the proposed rule may impose additional costs related to revising the service provider's cybersecurity practices to satisfy the requirements that would be imposed on the Covered Entities. Moreover, if a service

---

[789] *See* Jon Brodkin, *IT Shops Renegotiate Contracts to Get Savings Out of Vendors*, Computer World (Nov. 6, 2008), *available at* https://www.computerworld.com/article/2781173/it-shops-renegotiate-contracts-to-get-savings-out-of-vendors.html.

[790] For example, the Covered Entity has insufficient market power to affect changes in the service provider's business practices and the suite of cybersecurity technologies it currently offers to that Covered Entity.

provider is already providing services to a Covered Entity that are largely compliant with proposed Rule 10, then the resulting increase in compliance costs likely would be minor.

Even if satisfying additional client requirements would not represent a significant expense for service providers, the processes and procedures that are necessary to implement an infrequently utilized service may prevent some service providers from continuing to work with the Covered Entity.[791] That is, the provision of the service may be viewed as more burdensome than the revenue received from the Covered Entity. This consequence would serve as a disincentive to the service provider. In such cases, Covered Entities would bear costs related to finding alternative service providers while existing service providers would suffer lost revenue once the Covered Entities switch service providers.[792]

To estimate the costs associated with the proposed policies and procedures requirements and annual review requirements, the Commission considered the initial and ongoing compliance costs.[793] The internal annual costs for these requirements (which include an initial burden estimate annualized over a three year period) are estimated to be $14,631.54 per Covered Entity, and $29,102,133.06 in total. These costs include a blended rate of $462 for a compliance attorney and assistant general counsel for a total of 31.67 hours. The annual external costs for adopting and implementing the policies and procedures, as well as the annual review of the policies and procedures are estimated to be $3,472 per Covered Entity, and $6,905,808 in total. This includes the cost of using outside legal counsel at a rate of $496 per hour for a total of seven hours.

---

791 For example, the costs associated with legal review of alterations to standard contracts may not be worth bearing by the service provider if Covered Entities represent a small segment of the service provider's business.

792 At the same time, these frictions would benefit service providers that cater to customers in regulated industries.

793 *See* section V of this release (discussing these costs in more detail).

b. Broker-Dealers

i. Benefits

The benefits of the policies and procedures requirements of proposed Rule 10 for Covered Broker-Dealers likely will not be consistent across these entities, as their services vary. Covered Broker-Dealers that are larger, more interconnected with other market participants, and offer more services have a higher potential for greater losses for themselves and others in the event of a cybersecurity incident. Thus, the benefits arising from robust cybersecurity practices increases with the size and number of services offered by Covered Broker-Dealers. For example, a cybersecurity incident at a large Covered Broker-Dealer that facilitates trade executions and/or provides carrying and clearing services carries greater risk due to the larger number of services it provides as well as its interconnections with other Market Entities. For example, carrying broker-dealers may provide services to multiple introducing brokers-dealers and their customers. Commission staff determined that, as of September 2022, carrying broker-dealers have an average of 44 introducing broker-dealers on behalf of which they carry funds and securities,[794] with a median number of five broker-dealers. Furthermore, a carrying broker-dealer may intermediate the connection between one introducing broker-dealer and the final carrying broker-dealer.[795] As a result, there are potentially many avenues for infiltration, from the introducing broker-dealers to the carrying broker-dealers. Such Covered Broker-Dealers will not only hold customers' personally identifiable information and records, but also typically have control over customers' funds and assets. This makes them attractive targets for threat actors. In addition, even a brief disruption of the services offered by a carrying broker-dealer (*e.g.*, from a ransomware attack) could have large, negative downstream repercussions on the broker-dealer's customers and other Covered Entities (*e.g.*, inability to submit orders during volatile market

---

[794] Based on Form Custody, Item 4, as of 2021.

[795] *Id*.

conditions or to access funds and securities). The persons negatively impacted could include not only individuals but also institutional customers, such as introducing broker-dealers, hedge funds, and family offices. In this scenario, the Covered Broker-Dealer could incur major losses if it experienced a significant cybersecurity incident. Thus, compliance with written cybersecurity policies and procedures, along with annual reviews and a written assessment report, likely would have substantial benefits for those Covered Broker-Dealers that hold customer information, funds, and assets.

Because Covered Broker-Dealers perform a number of functions in the U.S. securities markets and those functions are increasingly performed through the use of information systems, it is important that those information systems be secure against cyberattacks. Covered Broker-Dealers use networks to connect their information systems to those of national securities exchanges, clearing agencies, and to communicate and transact with other Covered Broker-Dealers. Written policies and procedures would strengthen a Covered Broker-Dealer's cybersecurity protocols so that it would be more difficult for threat actors to disrupt market-making activities in securities or otherwise compromise the liquidity of the securities markets, an occurrence that could negatively impact the ability of investors to liquidate or purchase certain securities at favorable or predictable prices or in a timely manner.

ATSs are trading systems that meet the definition of "exchange" under federal securities laws but are not required to register as national securities exchanges if they comply with the conditions of the Regulation ATS exemption, which includes registering as a broker-dealer. ATSs have become significant venues for orders and non-firm trading interest in securities.[796] ATSs use data feeds, algorithms, and connectivity to perform their functions. ATSs rely heavily

---

[796] Exchange Act Rule 3a1-1(a)(2) exempts an ATS from the definition of exchange under section 3(a)(1) of the Exchange Act on the condition that the ATS complies with Regulation ATS. *See generally* Regulation of NMS Stock Alternative Trading Systems Release, 83 FR 38768; Amendments Regarding the Definition of "Exchange" and ATSs Release, 87 FR 15496.

on information systems to perform these functions, including to connect to other Market Entities, such as other Covered Broker-Dealers and national securities exchanges.

A significant cybersecurity incident that disrupts an ATS could negatively impact the ability of investors to liquidate or purchase certain securities at favorable or predictable prices or in a timely manner to the extent it provides liquidity to the market for those securities. Furthermore, the records stored by ATSs on their information systems consist of proprietary information about Market Entities that use their services, including confidential business information (*e.g.*, information about their trading activities). A significant cybersecurity incident at an ATS could lead to the improper use of this information to harm the Market Entities (*e.g.*, public exposure of confidential trading information) or provide the unauthorized user with an unfair advantage over other market participants (*e.g.*, trading based on confidential business information). Comprehensive cybersecurity policies and procedures, along with periodic assessments, would fortify broker-dealer ATS operations in their efforts to thwart cybersecurity attacks.

On the other hand, a small Covered Broker-Dealer could experience a cybersecurity incident that has significant negative impacts on the entity and its customers, such as a disruption to its services or the theft of a customer's personal information. These types of incidents would have profound negative effects for the small Covered Broker-Dealer and its customers, but the negative effects would likely be insignificant relative to the size of the entire U.S. securities markets. In this case, strong cybersecurity policies and procedures generally could provide substantial benefits to small Covered Broker-Dealers themselves and their customers, but likely not to other market participants.

As discussed in the baseline, Covered Broker-Dealers currently are subject to Regulations S-P, Regulation S-ID, FINRA rules, and SRO and Commission oversight, as well as Regulation

ATS applying to broker-dealer operated ATSs.[797] In addition, Covered Broker-Dealers that operate an ATS and trade certain stocks exceeding specific volume thresholds are subject to Regulation SCI.[798] As discussed above, Regulation S-P, Regulation ATS, and Regulation S-ID have requirements to establish policies and procedures that address certain cybersecurity risks.[799] Therefore, Covered Broker-Dealers subject to these other regulations have existing cybersecurity policies and procedures that address certain cybersecurity risks. However, proposed Rule 10 would require all Covered Broker-Dealers to establish, maintain, and enforce a set of cybersecurity policies and procedures that is broader and more comprehensive than is required under the existing requirements of Regulation S-P, Regulation S-ID, and Regulation ATS that pertain to cybersecurity risk. This could substantially benefit these Covered Broker-Dealers and their customers and counterparties as well as other Market Entities that provide services to them or transact with them. In particular, the failure to protect a particular information system from cybersecurity risk can create a vulnerability that a threat actor could exploit to access other information systems of the Covered Broker-Dealer. Therefore, proposed Rule 10—because it would require all information systems to be protected by policies and procedures—would result in benefits to Covered Broker-Dealers (*i.e.*, enhanced cybersecurity resiliency).

Covered Broker-Dealers that are registered as FCMs or swap dealers are subject to NFA requirements that relate to proposed Rule 10.[800] These additional requirements may bring those dually-registered Covered Broker-Dealers more in line with the requirements of the proposed

---

797 *See* section IV.C.1.b.i. of this release (discussing as part of the baseline the current relevant regulations applicable to broker-dealers); *see also* section II.F. of this release (discussing other relevant regulations applicable to Covered Broker-Dealers).

798 *Id*.

799 *See* section II.F.1.c. of this release (discussing in more detail the existing requirements of Regulation S-P, Regulation ATS, and Regulation S-ID to have policies and procedures to address certain cybersecurity risks).

800 *See* section IV.C.1.d.iii. of this release (discussing as part of the baseline current CFTC-related requirements applicable to FCMs and swap dealers).

rule[801]. As a result, the marginal benefit of compliance for them may be smaller than those that are only registered with the Commission.

ii. Costs

The compliance costs of the policies and procedures requirements of proposed Rule 10 for Covered Broker-Dealers may generally be lower, to the extent their current policies and procedures are designed to comply with Regulation SCI, Regulation S-P, Regulation ATS (if they operate an ATS), Regulation S-ID, and FINRA rules and are consistent with certain of the requirements of the proposed Rule 10.[802] However, the requirements of proposed Rule 10 are designed to address all of the Covered Broker-Dealer's cybersecurity risks; whereas the requirements of these other regulations that relate to cybersecurity are more narrowly focused. Consequently, the marginal costs associated with implementing the cybersecurity policies and procedures required under the proposed Rule 10 would depend on the extent to which broker-dealers' existing cybersecurity protections address cybersecurity risks beyond those that are required to be addressed by these other regulations.

Covered Broker-Dealers that are dually registered with the CFTC as FCMs or swap dealers are subject to NFA requirements, as noted above.[803] These additional requirements may make compliance with the proposed rule less burdensome and thus less costly, as those NFA requirements are already in place.

c. Clearing Agencies and National Securities Exchanges

i. Benefits

---

801 *See* section I.B. of this release (discussing the proposed requirements for Covered Entities, including Covered Broker-Dealers, with respect to cybersecurity policies and procedures).

802 *See* section II.F.1.c. of this release (discussing the requirements of proposed Rule 10 and how they relate to Regulation S-P, Regulation ATS, and Regulation S-ID).

803 *See* section IV.C.1.d.iii. of this release (discussing as part of the baseline current CFTC-related requirements applicable to FCMs and swap dealers).

Strong cybersecurity protocols at national securities exchanges would help maintain their critical function of matching orders of buyers and sellers. A cybersecurity incident could prevent an exchange from executing trades, therefore preventing members and their customers from buying or selling securities at the exchange. Interruptions in order flow and execution timing could lead to inefficiencies in order matching, possibly resulting in a less desirable execution price. Moreover, customer information could be stolen and trading strategies could be revealed. Lastly, a cybersecurity breach could be problematic for market surveillance staff that monitors the market for illegal trading activity. Thus, the policies and procedures requirements of proposed Rule 10 could offer significant benefits to national securities exchanges and market participants that depend on their processing of order flow and the ability of regulators to surveil the market.

Clearing agencies serve an important role in the securities markets by ensuring that executed trades are cleared and that the funds and securities are transferred to and from the appropriate accounts. A cybersecurity incident at a clearing agency could result in delays in clearing as well as in the movement of funds and assets. Such an incident also could lead to the loss or misappropriation of customer information, funds, and assets. Threat actors could also gain access to and misappropriate the clearing agency's default fund by, for example, obtaining access to the clearing agency's account in which the fund is held. Strong cybersecurity policies and procedures would assist clearing agencies in protecting the funds and securities in their control. This would benefit the clearing agency, its members, and market participants that rely on the services of its members.

As discussed in the baseline, national securities exchanges, registered clearing agencies, and certain exempt clearing agencies are subject to Regulation SCI.[804] Regulation SCI has

---

[804] *See* section IV.C.1.b.ii. of this release (discussing as part of the baseline the relevant regulations applicable to national securities exchanges and clearing agencies).

requirements for SCI entities to establish policies and procedures that address certain cybersecurity risks The proposed requirements of proposed Rule 10, in contrast, apply to all of the Covered Entity's information systems. The benefits of the policies and procedures requirements of proposed Rule 10 would depend on the extent to which the national securities exchanges' and clearing agencies' current cybersecurity policies and procedures (which include those required by Regulation SCI) are consistent with those required under the proposed rule. Major changes in cybersecurity policies and procedures could yield large benefits. However, the marginal benefit of the proposed rule likely would decline the more closely a national securities exchange's or clearing agency's cybersecurity policies and procedures are consistent with the requirements of proposed Rule 10.

Clearing agencies that are registered as DCOs are subject to additional CFTC requirements that may be related to those of proposed Rule 10.[805] As a result, the marginal benefit of proposed Rule 10 may be smaller than those that are only registered with the Commission.

ii. Costs

The incremental cost of compliance with the policies and procedures requirements of proposed Rule 10 for national exchanges and clearing agencies depends on how much their current cybersecurity policies and procedures go beyond what is required by Regulation SCI. This is because the requirements of proposed Rule 10 are designed to address all of the cybersecurity risks faced by a national securities exchange or clearing agency; in contrast, the requirements of Regulation SCI that relate to cybersecurity are more narrowly focused.[806] Therefore, national securities exchanges and clearing agencies that have policies and procedures

---

805 *See* section IV.C.1.d.i. of this release (discussing as part of the baseline the current relevant CFTC regulations applicable to DCOs).

806 *See* section II.F.1.c. of this release (discussing the requirements of proposed Rule 10 and how they relate to the requirements of Regulation SCI).

in place that only address the requirements of Regulation SCI will need to make potentially significant changes to their cybersecurity policies and procedures in order to comply with the requirements of proposed Rule 10. Alternatively, national securities exchanges and clearing agencies that currently have comprehensive cybersecurity policies and procedures may incur fewer costs to comply with proposed Rule 10. Nevertheless, assuming that they do not do so already, ensuring that those cybersecurity policies and procedures are documented and reviewed on an annual basis as required by the proposal, with an accompanying written assessment, would assist national securities exchanges and clearing agencies to withstand cybersecurity incidents and address them more effectively, thus minimizing the negative effects of such occurrences.

Clearing agencies that are dually registered with the CFTC as DCOs are subject to that agency's systems safeguards rule, as noted above.[807] Complying with the CFTC requirements may make compliance with the proposed rule less burdensome and thus less costly, to the extent that the registered DCO implements the CFTC requirements on the registered clearing agency side of its operations.

Finally, national securities exchanges and clearing agencies that are registered with the Commission but currently are not active would incur substantially higher costs relative to their active peers if they needed to come into compliance with proposed Rule 10. If they resume clearing activities and operations, they may incur significant costs to develop, document, implement, maintain, and enforce policies and procedures, including cybersecurity policies and procedures, as well as establish protocols for written annual reviews with necessary modifications and updates.

d. FINRA and the MSRB

i. Benefits

---

807 *See* section IV.C.1.c.i. of this release (discussing as part of the baseline the current relevant CFTC regulations applicable to DCOs).

FINRA is the only national securities association currently registered with the Commission. Similarly, the MSRB is the only entity (other than the Commission) established by Congress to, among other activities, propose and adopt rules with respect to transactions in municipal securities.

FINRA issues cybersecurity-related statements to members that discuss best practices for achieving adequate cybersecurity protection.[808] FINRA and MSRB members are also subject to internal oversight and external audits. Nevertheless, both FINRA and the MSRB store proprietary information about their members, including confidential business information, on their respective information systems. FINRA stores information about broker-dealers and trades. Some information and systems under FINRA's control may belong to other organizations where FINRA is simply contracted to perform data processing duties. There also may be sensitive information related to FINRA's oversight practices that is not made public, such as regulatory assessments of various broker-dealers or internal analyses regarding its examinations and examination programs. Furthermore, FINRA may keep information on cyberattacks on itself and on broker-dealers that, if made public, could compromise existing cybersecurity systems. Therefore, FINRA and the MSRB themselves require their own cybersecurity policies and procedures.

As discussed in the baseline, FINRA and the MSRB are subject to Regulation SCI.[809] Regulation SCI has requirements to establish policies and procedures that address certain cybersecurity risks.[810] Therefore, the benefits of the policies and procedures requirements of proposed Rule 10 would depend on the extent to which the FINRA's and the MSRB's current cybersecurity policies and procedures (which include those required by Regulation SCI) are

---

808 *See* FINRA, *Cybersecurity*, *available at* https://www.finra.org/rules-guidance/key-topics/cybersecurity#overview.

809 *See* section IV.C.1.b.ii. of this release (discussing as part of the baseline the current relevant regulations applicable to national securities associations and FINRA).

810 *See* section II.F.1.c. of this release (discussing in more detail the requirements of Regulation SCI).

consistent with those required under the proposed rule. This means the marginal benefit of the proposed rule may be limited depending on how closely FINRA's and the MSRB's cybersecurity policies and procedures are consistent with proposed Rule 10. Nevertheless, ensuring that those cybersecurity policies and procedures are documented and reviewed on an annual basis, with an accompanying written assessment, could assist the two entities in avoiding cybersecurity incidents and addressing them more effectively, thus minimizing the negative effects of such occurrences.

ii. Costs

As with national securities exchanges and clearing agencies, the Commission does not expect that FINRA and the MSRB will incur significant costs as a result of complying with the policies and procedures requirements of proposed Rule 10 because they are already subject to Regulation SCI and, due to their importance in the oversight and oversight of their members or registrants, as well as the storage of trade information and data owned by other parties, there are strong incentives for FINRA and the MSRB to invest in comprehensive cybersecurity programs.

e. SBS Entities

i. Benefits

As discussed in the baseline, SBS Entities must comply with section 15F(j)(2) of the Exchange Act and various Commission rules. SBS Entities that are dually registered with the CFTC are subject to that agency's rules as well as the rules of the NFA.[811] The benefits that would accrue to SBS Entities depend on the level of cybersecurity protection they currently have in place. Policies and procedures that are consistent with the policies and procedures requirements of proposed Rule 10 may only need moderate updating and adjustment. As a result the marginal benefits likely are small. There would be much greater benefits for SBS Entities

---

[811] *See* section IV.C.1.c.iii. of this release (discussing as part of the baseline current relevant regulations applicable to SBS Entities).

that must significantly revise their current policies and procedures. Further, proposed Rule 10 would require that SBS Entities have policies and procedures to respond to and recover from cybersecurity incidents, which would assist the SBS Entities in minimizing the harm caused by the incident and enhancing their ability to recover from it. Annual reviews also would help them update their policies and procedures to address emerging threats.

SBS Entities that are registered as swap dealers are subject to additional requirements of the CFTC and NFA that may be related to those of proposed Rule 10.[812] As a result, the marginal benefit of compliance for them may be smaller than those that are only registered with the Commission.

ii. Costs

Complying with the policies and procedures requirements of proposed Rule 10 may not be costly for SBS Entities. SBS Entities must comply with section 15F(j)(2) of the Exchange Act and various Commission rules. The costs that arise from compliance with proposed Rule 10 depend on how closely their current documented policies and procedures, as well as annual reviews and summary reports, are consistent with the proposed rule. SBS Entities that have very similar cybersecurity policies and procedures to those that would be required under proposed Rule 10 would have small associated costs to come into compliance with the rule. SBS Entities that need to make more substantial changes to their cybersecurity policies and procedures to comply with the proposed rule would incur higher attendant costs. Ultimately, the ability of SBS Entities to bear those additional costs depends on the competitive landscape of the security-based swap market.

---

[812] *See* section IV.C.1.c.iii. of this release (discussing as part of the baseline the current relevant CFTC regulations applicable to swap dealers).

SBS Entities that are dually registered with the CFTC as swap dealers are subject to that agency's requirements, as noted above.[813] These additional requirements may make compliance with the proposed rule less burdensome and thus less costly, as the CFTC requirements are already in effect and dually registered SBS Entities must comply with those regulations.

f. SBSDRs

i. Benefits

SBSDRs collect and maintain security-based swap transaction data so that relevant authorities can access and analyze the data from secure, central locations, thereby allowing regulators to monitor for potential market abuse and risks to financial stability.[814] SBSDRs also reduce operational risk and enhance operational efficiency in the security-based swap market, such as by maintaining transaction records that help counterparties ensure that their records reconcile.[815]

The Commission requires SBSDRs to have written documentation regarding how they keep such transaction information secure.[816] If the policies and procedures requirements of proposed Rule 10 requires an SBSDR to do additional development, documentation, implementation, and review of its cybersecurity policies and procedures, then the benefits that accrue from doing so will be large. In this circumstance, compliance with the policies and procedures requirements of proposed Rule 10 would bolster SBSDRs' cybersecurity resiliency. As a result, SBSDRs would be better prepared to identify cybersecurity vulnerabilities and

---

813 *See* section IV.C.1.c.iii. of this release (discussing as part of the baseline the current relevant CFTC regulations applicable to swap dealers).

814 *See* SBSDR Adopting Release, 80 FR at 14440 ("[SBSDRs] are required to collect and maintain accurate SBS transaction data so that relevant authorities can access and analyze the data from secure, central locations, thereby putting them in a better position to monitor for potential market abuse and risks to financial stability.").

815 *See* SBSDR Proposing Release at 77307 (stating that "[t]he enhanced transparency provided by an [SBSDR is important to help regulators and others monitor the build-up and concentration of risk exposures in the [security-based swap] market . . . . In addition, [SBSDRs] have the potential to reduce operational risk and enhance operational efficiency in the [security-based swap] market").

816 *See* section IV.C.1.b.iv. of this release (discussing as part of the baseline the current relevant regulations applicable to SBSDRs).

prevent significant cybersecurity incidents, thereby safeguarding the security-based swap trade data that they receive and maintain. Further, proposed Rule 10 would require that SBSDRs have policies and procedures to respond to and recover from a significant cybersecurity incident, which would assist SBSDRs in minimizing the harm caused by the incident and enhancing their ability to recover from it. Annual reviews also would help them update their policies and procedures to address emerging threats.

SBSDRs that are dually registered with the CFTC as SDRs must comply with that agency's systems safeguards rule, applicable to information systems for data under the CFTC's jurisdiction.[817] These additional requirements may bring those dually-registered SBSDRs more in line with the requirements of the proposed rule, to the extent that the registered entity applies the CFTC's systems safeguard requirements to the SBSDR operations. As a result, the marginal benefit of compliance for them may be smaller than those that are only registered with the Commission.

ii. Costs

The costs that arise from compliance with the policies and procedures requirements of proposed Rule 10 depend on how closely the current documented policies and procedures of SBSDRs are consistent with the proposed rule. SBSDRs that have very similar cybersecurity policies and procedures to those that would be required under proposed Rule 10 would face small costs to amend their cybersecurity policies and procedures. SBSDRs that need to make more substantial changes to their cybersecurity policies and procedures to comply with the proposed rule would realize greater marginal benefits from attaining compliance, while incurring higher attendant costs.

---

[817] *See* section IV.C.1.d.ii. of this release (discussing as part of the baseline the current relevant CFTC regulations applicable to SDRs).

SBSDRs that are dually registered with the CFTC as SDRs are subject to that agency's system safeguards rule, as noted above.[818] These additional requirements may make compliance with the proposed rule less burdensome and thus less costly, to the extent the registered entity applies the CFTC's system safeguard requirements to its SBSDR operations.

g. Transfer Agents

i. Benefits

The benefits of the policies and procedures requirements of proposed Rule 10 likely will differ across transfer agents, as their size and the level of their services may vary. Transfer agents, among other functions, may: (1) track, record, and maintain on behalf of issuers the official record of ownership of each issuer's securities; (2) cancel old certificates, issue new ones, and perform other processing and recordkeeping functions that facilitate the issuance, cancellation, and transfer of those securities; (3) facilitate communications between issuers and registered securityholders; and (4) make dividend, principal, interest, and other distributions to securityholders.[819] A cybersecurity incident at a transfer agent would have varying negative impacts depending on the range of services offered by the transfer agent. Nonetheless, for the issuer who depends on the transfer agent to maintain the official record of ownership, or for securityholders who depend on the transfer agent for distributions, an incident at even a small transfer agent with limited services could have profound negative implications.

In addition, some transfer agents may maintain records and information related to securityholders that could include names, addresses, phone numbers, email addresses, employers, employment history, bank and specific account information, credit card information, transaction histories, securities holdings, and other detailed and individualized information related to the transfer agents' recordkeeping and transaction processing on behalf of issuers.

---

818 *See* section IV.C.1.d.iii. of this release (discussing as part of the baseline the current relevant CFTC regulations applicable to swap dealers).

819 *See* section I.A.2.i. of this release (discussing critical operations and functions of transfer agents).

This information may make a transfer agent particularly attractive to threat actors. Compliance with written cybersecurity policies and procedures under proposed Rule 10, along with annual reviews and a written assessment report, would likely produce a large benefit for clients and investors of transfer agents.

Preventing successful cyberattacks would keep securities from being stolen by threat actors and would ensure that dividends are paid when promised. In addition, because transfer agents have information on the securityholders' personal information, policies and procedures to protect that information from unauthorized access or use would benefit the transfer agent and the securityholders. Moreover, if a significant cybersecurity incident materializes, transfer agents would have a plan to resolve the issue, thus potentially reducing the timeframe and damage associated with the incident.

As discussed in the baseline, transfer agents registered with the Commission (but not transfer agents registered with another appropriate regulatory agency) are subject to the Regulation S-P Disposal Rule and may be subject to Regulation S-ID.[820] The Regulation S-P Disposal Rule and Regulation S-ID require measures that implicate a certain cybersecurity risk.[821] Nonetheless, the policies and procedures requirements of proposed Rule 10 would still provide substantial benefits to transfer agents. This is because, as discussed above, proposed Rule 10 would require all transfer agents to establish, maintain, and enforce policies and procedures to address cybersecurity risks that are broader and more comprehensive than those policies and procedures required by the existing requirements of Regulation S-P or Regulation S-ID.

ii. Costs

---

820 *See* section IV.C.1.b.v. of this release (discussing as part of the baseline the current relevant regulations applicable to transfer agents). Transfer agents that are subsidiaries of bank holding companies would incur minimal cost since they are already subject to federal banking cybersecurity regulations.

821 *See* section II.F.1.c. of this release (discussing in more detail the existing requirements of the Regulation S-P Disposal Rule and Regulation S-ID).

Transfer agents likely would incur moderate costs in complying with the policies and procedures requirements of proposed Rule 10 if their current policies and procedures—including those to comply with the Regulation S-P Disposal Rule and Regulation S-ID (if either or both apply)—would need to be augmented to meet the requirements of proposed Rule 10. Transfer agents also would have to do annual reviews and write assessment reports. Such costs likely would be passed on to the entities that use transfer agent's services. Transfer agents that have made the business decision to implement robust cybersecurity policies, procedures, and practices would incur lower marginal compliance costs, to the degree those policies, procedures, and practices are consistent with the requirements of proposed Rule 10.

h. Request for Comment

The Commission requests comment on all aspects of the foregoing analysis of the benefits and costs of the policies and procedures, review and assessment, and report requirements of proposed Rule 10. Commenters are requested to provide empirical data in support of any arguments or analyses. In addition, the Commission is requesting comment on the following matters:

1. Please discuss which types of Covered Entities have some level of cybersecurity in place and which may not? If not, explain why. Please describe the level of cybersecurity policies and procedures that have been implemented by Covered Entities and compare them to the requirements of proposed Rule 10.
2. Do the benefits and costs associated with Covered Entities having written cybersecurity policies and procedures, including provisions for written annual reviews and assessments, reports, and updates (if necessary) vary by the type of Covered Entity? If so, explain how. Are there benefits and costs of the proposals not described above? If so, please describe them.
3. Are the estimated compliance costs (both initially and on an ongoing basis) for Covered Entities to adopt cybersecurity policies and procedures, along with

reviewing them annually and drafting a summary report, reasonable? If not, explain why and provide estimates of the compliance costs.

4. How costly would it be for a given type of Covered Entity to become compliant with proposed Rule 10? Please explain and provide estimates of the costs.

5. Do Covered Entities typically document their cybersecurity policies and procedures? If not, how costly would it be for them to be documented?

6. Please describe practices of Covered Entities with regard to the use of service providers in connection with their information systems and the information residing on those systems. How many Market Entities contract with service providers? What functions are contracted out versus completed in house? Are the cybersecurity policies and procedures implemented by these service providers comparable to the requirements of proposed Rule 10? Please explain. Would it be costly contractually to request that a service provider provide compliant services, including documented policies and procedures? What are the costs of finding a new service provider if one or more could not provide services that are compliant with the proposed rule?

7. How costly would it be to review and update, if necessary, cybersecurity policies and procedures at least annually? Would it be preferable to conduct the reviews on either a more or less frequent basis? Explain why. Would it be less costly to have a third party conduct the review and update of a Covered Entities' cybersecurity policies and procedures? Please explain.

3. Regulatory Reporting of Cybersecurity Incidents by Covered Entities

Under proposed Rule 10, Covered Entities would need to provide the Commission with immediate written electronic notice of a significant cybersecurity incident affecting the Covered Entity and, thereafter, report and update information about the significant cybersecurity incident

by filing Part I of proposed Form SCIR with the Commission through the EDGAR system.[822] The form would elicit information about the significant cybersecurity incident and the Covered Entity's efforts to respond to, and recover from, the incident. In the case of certain Covered Entities, the notice and subsequent reports would need to be provided to other regulators.

a. Benefits

The requirements of proposed Rule 10 that Covered Entities provide immediate written electronic notice and subsequent reporting about significant cybersecurity incidents to the Commission and would improve the Commission's ability to assess these incidents. These requirements also would allow the Commission to understand better the causes and impacts of significant cybersecurity incidents and how Covered Entities respond to and recover from them. Thus, the notification and reporting requirements—through the information they would provide the Commission—could be used to understand better how significant cybersecurity incidents materialize and, therefore, how Covered Entities can better protect themselves from them and, when they occur, how Covered Entities can better mitigate their impacts and recover more quickly from them. Over time, this database of information could provide useful insights into how to minimize the harm more broadly that is caused by significant cybersecurity incidents, which have the potential to cause broader disruptions to the U.S. securities markets and undermine financial stability.

A Covered Entity would be required to provide immediate written electronic notice to the Commission of a significant cybersecurity incident upon having a reasonable basis to conclude that the incident has occurred or is occurring.[823] This timeframe allows for quick notification to the Commission and, in some cases, other regulators about the significant cybersecurity incident, which—in turn—would allow for more timely assessment of the incidents. These incidents, if

---

822 *See* sections II.B.2. and II.B.4. of this release (discussing these proposed requirements in more detail).

823 *See* paragraph (c)(1) of proposed Rule 10.

not addressed quickly, could have harmful spillover impacts to other Market Entities and participants in the U.S. securities markets.

The immediate written electronic notice would need to identify the Covered Entity, state that the notice is being given to alert the Commission of a significant cybersecurity incident impacting the Covered Entity, and provide the name and contact information of an employee of the Covered Entity who can provide further details about the significant cybersecurity incident.[824] By not requiring detailed information about the significant cybersecurity incident, the Covered Entity would be able to provide the notice quickly while it continues to assess which information systems have been subject to the significant cybersecurity incident and the impact that the incident has had on those systems. This would facilitate the Covered Entity's ability to alert the Commission and other regulators (if applicable) at a very early stage after it has a reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring. This, in turn, would allow the Commission and other regulators (if applicable) to begin taking steps to assess the significant cybersecurity incident at that early stage.

This proposed immediate written electronic notification requirement is modelled on other notification requirements that apply to broker-dealers and SBSDs pursuant to other Exchange Act rules. Under these existing requirements, broker-dealers and certain SBSDs must provide the Commission with same-day written notification if they undergo certain adverse events, including falling below their minimum net capital requirements or failing to make and keep current required books and records.[825] The objective of these requirements is to provide the Commission staff with the opportunity to respond when a broker-dealer or SBSD is in financial or operational difficulty.[826] Similarly, the immediate written electronic notification requirement

---

824 *Id.*

825 *See* 17 CFR 240.17a-11 (notification rule for broker-dealers); 17 CFR 240.18a-8 (notification rule for SBS Entities).

826 *See* SBS Entity Recordkeeping and Reporting Proposing Release, 79 FR at 25247.

of proposed Rule 10 would provide the Commission staff with the opportunity to promptly begin to assess the situation when a Covered Entity is experiencing a significant cybersecurity incident.

Promptly thereafter (but no later than 48 hours), a Covered Entity would be required to report separately more detailed information about the significant cybersecurity incident by filing initial, amended and final versions of Part I of proposed Form SCIR with the Commission through the EDGAR.[827] The Covered Entity also would be required to file updated reports and a final report.

The reporting requirements under proposed Rule 10 would provide the Commission and its staff with information to understand better the nature and extent of a particular significant cybersecurity incident and the efficacy of the Covered Entity's response to mitigate the disruption and harm caused by the incident.[828] It also strengthens and expands the Commission's knowledge regarding cybersecurity incidents beyond what is already required by current Commission regulations. In addition, the reporting would provide the staff with a view into the Covered Entity's understanding of the scope and impact of the significant cybersecurity incident. All of this information would assist the Commission and its staff in assessing the significant cybersecurity incident impacting the Covered Entity. It also could benefit other Market Entities to the extent the confidential information provided by the impacted Covered Entity could be used to assist them (without divulging the identity of the impacted Covered Entity) in avoiding a similar significant cybersecurity incident or succumbing to an attack by the same threat actor that caused the significant cybersecurity incident.

The information provided to the Commission under the proposed reporting requirements also would be used to assess the potential cybersecurity risks affecting U.S. securities markets

---

827 *See* paragraphs (c)(2) of proposed Rule 10. As discussed below, Part II of proposed Form SCIR would be used by Covered Entities to make public disclosures about the cybersecurity risks they face and the significant cybersecurity incidents they experienced during the current or previous calendar year. *See* sections II.B.2. and II.B.4. of this release (discussing these proposed requirements).

828 *See* Line Items 2 through 14 of Part I of proposed Form SCIR (eliciting information about the significant cybersecurity incident and the Covered Entity's response to the incident).

more broadly. This information could be used to address future significant cybersecurity incidents or address cybersecurity vulnerabilities that may be present at other similar Covered Entities. For example, these reports could assist the Commission in identifying patterns and trends across Covered Entities, including widespread cybersecurity incidents affecting multiple Covered Entities at the same time. Further, the reports could be used to evaluate the effectiveness of various approaches to respond to and recover from a different types of significant cybersecurity incidents. This could benefit all Market Entities, other participants in the U.S. securities markets, and ultimately promote the fair, orderly, and efficient operation of the U.S. securities markets.

Requiring Covered Entities to file Part I of proposed Form SCIR in EDGAR in a custom XML would allow for more efficient processing of information about significant cybersecurity incidents. It would create a comprehensive set of data of all significant cybersecurity incidents impacting Covered Entities that is based on these entities responding to the same check boxes and questions on the form. This would facilitate analysis of the data, including analysis across different Covered Entities and significant cybersecurity incidents. Eventually, this set of data and the analysis of it by searching and sorting based on how different Covered Entities responded to the same questions on the form could be used to spot common trending risks and vulnerabilities as well as best practices employed by Covered Entities to respond to and recover from significant cybersecurity incidents.

As discussed above, Covered Entities have incentives to not disclose information about significant cybersecurity incidents. Such incentives constrain the information available about cybersecurity threats and thereby inhibit the efficacy of collective (*i.e.*, an industry's or a society's) cybersecurity measures.[829] At the same time, complete transparency in this area likely

---

[829] *See* section IV.B. of this release (discussing broad economic considerations); *see, e.g.,* Lewis and Zheng, Cyber Threat Information Sharing (recommending that regulators encourage information sharing).

runs the risk of facilitating future attacks.[830] As discussed above, the challenge of effective information sharing has long been recognized, and government efforts at encouraging such sharing on a voluntary basis have had only limited success.[831] The Commission would not publicly disclose and would keep them confidential to the extent permitted by law Part I of proposed Form SCIR. This would limit the risks associated with public disclosure of vulnerabilities as a result of successful cybersecurity incidents. The Commission also may share information with relevant law enforcement or national security agencies.

The aforementioned benefits arise from improved information sharing between the affected Covered Entity and the Commission. Delays in incident reporting may hinder the utility of Part I of proposed Form SCIR because the Commission would not be able to assess the situation close to the time of its occurrence or discovery. Thus, the utility of such reports, at least initially, may be more limited if they are not filed as quickly as proposed.

Requiring Covered Entities to identify themselves on Part I of proposed Form SCIR with a UIC[832] if they already have a UIC would be beneficial because the LEI—which is a Commission-approved UIC—is a globally-recognized standard identifier[833] with reference data

---

830 Although "security through obscurity" as a cybersecurity philosophy has long been derided, "obscurity," or more generally "deception," has been recognized as an important cyber resilience technique. *See* Ron Ross, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, and Rosalie McQuaid, *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, 2 Nat. Inst. of Standards and Tech. (Dec. 2021), *available at* https://doi.org/10.6028/NIST.SP.800-160v2r1. *See also* Section IV.D.2.b (discussion of costs associated with disclosure).

831 *See* section IV.C.1.e. of this release (discussing information sharing).

832 As mentioned in section II.B.2.b. of this release, the instructions of proposed Form SCIR would define UIC to mean an identifier that has been issued by an IRSS that has been recognized by the Commission pursuant to Rule 903(a) of Regulation SBSR (17 CFR 242.903(a)).

833 "The [LEI] is a reference code — like a bar code — used across markets and jurisdictions to uniquely identify a legally distinct entity[.]" Office of Financial Research, U.S. Treasury Dep't, *Legal Entity Identifier – Frequently Asked Questions*, *available at* https://www.financialresearch.gov/data/legal-entity-identifier-faqs/. "The financial crisis underscored the need for a global system to identify financial connections, so regulators and private sector firms could understand better the true nature of risk exposures across the financial system." *Id.* Using the LEI as a UIC to facilitate tracking financial entity cybersecurity incidents and risks is feasible because "[t]he Global LEI System was established for a large range of potential uses." The Legal Entity Identifier Regulatory Oversight Committee ("LEIROC"), *LEI Uses*, *available at* https://www.leiroc.org/lei/uses.htm. The functionality of the LEI is such that it could be used to identify and track entities for various purposes. For example, the LEI is one of three identifiers that firms

that is available free of charge.[834] Unlike many identifiers that are specific to a particular regulatory authority or jurisdiction, the LEI is a permanent, unique global identifier that also contains "Level 2" parent and (direct/indirect) child entity information. Entity parent-child relationships are particularly relevant to assessing the risks of entities operating in the securities markets, where financial entities' interconnectedness and complex group structures could otherwise make understanding the scope of potential widespread risks challenging.[835] Additionally, unlike most company registries, all LEI data elements are validated annually and subject to a "quality program [that] scans the full [data] repository daily and publishes the results monthly in quality reports[,]" which helps to ensure the accuracy—and usefulness—of LEI data as compared to other types of entity identifiers that lack such features.[836]

---

can use under a December 2022 U.S. Customs & Border Protection Pilot for automation program for enhanced tracing in international supply chains. *See* U.S. Customs and Border Protection, *Announcement of the National Customs Automation Program Test Concerning the Submission Through the Automated Commercial Environment of Certain Unique Entity Identifiers for the Global Business Identifier Evaluative Proof of Concept*, 87 FR 74157 (Dec. 2, 2022), *available at* https://www.federalregister.gov/documents/2022/12/02/2022-26213/announcement-of-the-national-customs-automation-program-test-concerning-the-submission-through-the.

834 Bank for Int'l Settlements, David Leung, et al., *Corporate Digital Identity: No Silver Bullet, but a Silver Lining*, BIS Paper No. 126, at 20 (June 2022), *available at* https://www.bis.org/publ/bppdf/bispap126.pdf. ("BIS Papers 126") (stating that "LEI data [is] available free of charge to users in both the public and private sector"). The FSOC has stated the LEI "enables unique and transparent identification of legal entities." FSOC, 2021 Annual Report, at 171 (stating that "[b]roader adoption of the LEI by financial market participants continues to be a Council priority"). The FSOC also has stated that the LEI "facilitate[s] many financial stability objectives, including improved risk management in firms [and] better assessment of microprudential and macroprudential risks[.]" FSOC, 2022 Annual Report 99 (2022), *available at* https://home.treasury.gov/system/files/261/FSOC2022AnnualReport.pdf. The same principles that make the LEI well-suited for allowing regulators to track entity exposures to financial market risks across jurisdictions and entities should apply in other contexts, such as cross-border payments. *See* FSB, *FSB Options to Improve Adoption of the LEI, in Particular for Use in Cross-border Payments* (July 7, 2022), *available at* https://www.fsb.org/wp-content/uploads/P070722.pdf.

835 FSB Peer Review Report; *see also* European Systemic Risk Board, Francois Laurent, et al., *The Benefits of the Legal Entity Identifier for Monitoring Systemic Risk*, Occasional Paper Series No. 18, (Sept. 2021) ("The fact that the LEI enables full reporting of the group structure in the LEI database is also crucial for risk analysis. Indeed, the risk usually stems from the group and not from individual entities, and conducting a relevant risk analysis implies aggregating exposures at the level of the group."). For a discussion of the cybersecurity implications of the interconnectedness of Market Entities' information systems, *see* section I.A.1 of this release.

836 *See* BIS Papers 126, at 16 (noting that "[h]istorically, corporate identification has mainly come from company registries in individual jurisdictions[,]" with the registries connected to the filing of certain documents and the paying of required fees necessary to create legal entities). Under company registry regimes, each company typically is identified by name and "a company registration number" that is not standardized across jurisdictions and is not part of a harmonized system of corporate identification. *See id.*

b. Costs

Covered Entities would incur costs complying with the requirements of proposed Rule 10 to provide immediate written electronic notice and subsequent reporting about significant cybersecurity incidents to the Commission and, in the case of certain Covered Entities, other regulators, on Part I of proposed Form SCIR. The immediate notification requirement would impose minimal costs given the limited nature of the information that would need to be included in the written notice and the fact that it would be filed electronically.

The costs of complying with the requirements to file Part I of proposed Form SCIR to report a significant cybersecurity incident would be significantly greater than the initial notice, given the amount of information that would need to be included in the filing. In addition, because Part I of proposed Form SCIR is a regulatory filing, Covered Entities likely would incur costs associated with a legal and compliance review prior to the form being filed on EDGAR.

In terms of the costs of filing Part I of Form SCIR on EDGAR, several categories of Covered Entities already file forms in EDGAR. Specifically, all transfer agents, SBSDs, MSBSPs, and SBSDRs must file registration or reporting forms in EDGAR,[837] and some broker-dealers choose to file certain reports on EDGAR rather than filing them in paper form. The applicable EDGAR forms for these entities are filed, at least in part, in a custom XML. Covered Entities that do not currently file registration or reporting forms on EDGAR would have to file a notarized Form ID to receive a CIK number and access codes to file on EDGAR.[838] Consequently, the requirement to file Part I of proposed Form SCIR in EDGAR using a form-

---

(stating that "[w]ith greater globalization of business and finance, [the existing company registry system] has become a source of inefficiency and risks from the standpoint of financial stability, market integrity, and investor protection"). Further, "company registries typically do not offer similar types of quality programs for the corporate data they provide" and that such data generally is "declarative—provided by the registrant" without independent verification or validation. *See id.* at 20.

837 SBSDRs received temporary relief from filing through EDGAR. *See Cross-Border Application of Certain Security-Based Swap Requirements*, Exchange Act Release No. 87780 (Dec. 18, 2019) [85 FR 6270, 6348 (Feb. 2, 2020)].

838 *See* section V of this release (discussing of the number of Covered Entities who do not currently file forms in EDGAR and the costs that would be associated with an EDGAR-filing requirement in more detail).

specific XML may impose some compliance costs on certain Covered Entities. These Covered Entities would need to complete Form ID to obtain the EDGAR-system access codes that enable entities to file documents through the EDGAR system. They would have to pay a notary to notarize Form ID. The inclusion of a UIC on proposed Form SCIR would not impose any marginal costs because a Covered Entity would only be required to provide a UIC if they have already obtained one.

To estimate the costs for Market Entities to research the validity of a suspected significant cybersecurity incident and to provide immediate written electronic notification to the Commission regarding the significant cybersecurity incident that are real or reasonably determined to be true, the Commission considered the initial and ongoing compliance costs.[839] The internal annual costs for these requirements (which include an initial burden estimate annualized over a three year period) are estimated to be $1,648.51 per Market Entity, and $6,524,802.58 in total. These costs include a blended rate of $353 for an assistant general counsel, compliance manager, and systems analyst for a total of 4.67 hours. The annual external costs for these requirements are estimated to be $1,488 per Market Entity, and $5,889,504 in total. This includes the cost of using outside legal counsel at a rate of $496 per hour for a total of three hours.

To estimate the costs for Covered Entities to fill out an initial Part I of proposed Form SCIR, and file an amended Part I of Form SCIR, the Commission considered the initial and ongoing compliance costs.[840] The internal annual costs for these requirements (which include an initial burden estimate annualized over a three year period) are estimated to be $1,077.50 per Covered Entity, and $2,143,147.50 in total. These costs include a blended rate of $431 for an assistant general counsel and compliance manager for a total of 2.5 hours. The annual external

---

[839] *See* section V of this release (discussing these costs in more detail).

[840] *See* section V of this release (discussing these costs in more detail).

costs for these requirements are estimated to be $992 per Covered Entity, and $1,973,088 in total. This includes the cost of using outside legal counsel at a rate of $496 per hour for a total of two hours.

c. Request for Comment

The Commission requests comment on all aspects of the foregoing analysis of the benefits and costs of the requirements to provide immediate notification and subsequent reporting of significant cybersecurity incidents. Commenters are requested to provide empirical data in support of any arguments or analyses. In addition, the Commission is requesting comment on the following matters:

8. Are the estimated compliance costs (both initially and on an ongoing basis) for Covered Entities to provide the notification and subsequent reports reasonable? If not, explain why and provide estimates of the compliance costs.
9. Are there any other benefits and costs that the confidential reporting would provide the Commission? If so, please describe them. Please provide views on the costs of reporting significant cybersecurity incidents to the Commission relative to the Commission's cost estimates.
10. What are the costs and benefits associated with requiring Covered Entities to file Part I of proposed Form SCIR using a structured data language? Should the Commission require Covered Entities to file Part I of proposed Form SCIR using a structured data language, such as a custom XML? Should the Commission require Covered Entities to file Part I of proposed Form SCIR using a different structured data language than a custom XML, such as Inline XBRL? Why or why not?
11. Are there any Covered Entities that should be exempted from the proposed structured data requirements for filing Part I of proposed Form SCIR? If so, what

particular exemption threshold should the Commission use for the structured data requirements and why?

12. Should Covered Entities be required to file proposed Form SCIR with a CIK number? What are the costs and benefits associated with requiring Covered Entities to identify themselves on Part I of proposed Form SCIR with a CIK number?

13. Should Covered Entities be required to file Part I of proposed Form SCIR with a UIC (i.e., such as an LEI), particularly when some Covered Entities do not have a UIC and would have to obtain one? What are the benefits associated with requiring Covered Entities with a UIC to identify themselves with that UIC?

14. Would requiring a UIC on Part I of proposed Form SCIR allow the Commission to better evaluate cybersecurity threats to Covered Entities using data from other regulators and from law enforcement agencies? Please explain how.

15. Are there any Covered Entities for which the proposed structured data requirements for Part I of proposed Form SCIR should be exempted? If so, what particular exemption threshold or thresholds should the Commission use for the structured data requirements under the proposed rule amendments, and why?

4. Public Disclosure of Cybersecurity Risks and Significant Cybersecurity Incidents

Under proposed Rule 10, Covered Entities would need to publicly disclose summary descriptions of their cybersecurity risks and the significant cybersecurity incidents they experienced during the current or previous calendar year on Part II of proposed Form SCIR.[841] The form would need to be filed with the Commission through the EDGAR system and posted on the Covered Entity's business Internet website and, in the case of Covered Entities that are

---

[841] *See* sections II.B.3. and II.B.4. of this release (discussing these proposed requirements in more detail).

carrying or introducing broker-dealers, provided to customers at account opening and at least annually thereafter.

a. Benefits

As discussed above, there exists an information asymmetry between Covered Entities and their customers, counterparties, members, registrants, or users.[842] This information asymmetry, together with limitations to private contracting, inhibits the ability of customers, counterparties, members, registrants, and users to screen and discipline the Covered Entities with whom they do business or obtain services from based on the effectiveness of the Covered Entity's cybersecurity policies. The public disclosure requirements of proposed Rule 10 would help alleviate this information asymmetry, and in so doing would enable customers, counterparties, members, registrants, or users to better assess the effectiveness of Covered Entities' cybersecurity preparations and the cybersecurity risks of doing business with any one of them. For example, customers, counterparties, members, registrants, or users could use the frequency or nature of significant cybersecurity incidents—as disclosed under the proposed public disclosure requirement—to infer a Covered Entity's effort toward preventing cybersecurity incidents. Likewise customers, counterparties, members, registrants, or users could use the descriptions of cybersecurity risks to avoid certain Covered Entities with less well-developed cybersecurity procedures.

Public disclosures mitigate the information asymmetry. Customers, counterparties, members, registrants, or users can use the information to understand better the risks of doing business with certain Covered Entities. A Covered Entity disclosing that it addresses cybersecurity risks in a robust manner and that it has not experienced a significant cybersecurity incident or few such incidents could signal to customers, counterparties, members, registrants, or users that customer information, funds, and assets are safeguarded properly. In contrast,

---

842 *See* section IV.B. of this release (discussing broad economic considerations).

disclosures of sub-par cybersecurity practices or a history of significant cybersecurity incidents may convince customers, counterparties, members, registrants, or users to not do business with that Covered Entity.

In addition to mitigating information asymmetries with stakeholders in general, public disclosure would also mitigate a source of principal-agent problems in the customer-Covered Entity relationship. As discussed above, Covered Entities may have different incentives than customers in the area of cybersecurity prevention.[843] Insofar as principals (customers) prefer a higher level of cybersecurity focus by agents (Covered Entities), public disclosure would act as an incentive for Covered Entities to increase their focus in this area and signal their commitment to protecting customers' funds and data.

The proposed requirement for Covered Entities to post the required disclosures on their websites would help inform, for example, retail customers about Covered Broker-Dealers because they are likely to look for information about their broker-dealers on the firm's websites. In addition, requiring the submission of Part II of proposed Form SCIR in a custom XML data language would likely facilitate more effective and thorough review, analysis, and comparison of cybersecurity risks and significant cybersecurity incidents by the Commission and by Covered Entities' existing and prospective customers, counterparties, members, registrants, or users.[844] The public disclosure requirement of proposed Rule 10 expands Market Entities', other market participants', the public's, the Commission's, and other regulatory bodies' knowledge about the cybersecurity risks faced by Covered Entities as well as their past experiences regarding significant cybersecurity incidents that is beyond what is provided by current Commission regulations.

---

843 *See* section IV.B. of this release (discussing broad economic considerations).

844 While the Commission would separately receive the information significant cybersecurity incidents impacting Covered Entities thought the filings of Part I of proposed Form SCIR, those filings would not include the Covered Entity's summary description of the cybersecurity risks that could materially affect the Covered Entity's business and operations and how it assesses, prioritizes, and addresses those cybersecurity risks that would be disclosed on Part II of proposed Form SCIR.

Requiring Covered Entities to file Part II of proposed Form SCIR through the EDGAR system would allow the Commission—as well as customers, counterparties, members, and users of Covered Entity services—to download the Part II disclosures directly from a central location, thus facilitating efficient access, organization, and evaluation of the reported disclosures about significant cybersecurity incidents. Likewise, because Part II of proposed Form SCIR would be structured in SCIR-specific XML, the public disclosures would be machine-readable and, therefore, more readily accessible to the public and the Commission for comparisons across Covered Entities and time periods. With centralized filing in EDGAR in a custom XML, Commission staff as well as Covered Entities' customers, counterparties, members, registrants, or users (and the Covered Entities themselves) would be better able to assemble, analyze, review, and compare a large collection of data about reported cybersecurity risks and significant cybersecurity incidents, which could facilitate the efficient identification of trends in cybersecurity risks and significant cybersecurity incidents in the U.S. securities markets.

Centralized filing of the summary descriptions of the Covered Entity's cybersecurity risks and significant cybersecurity incidents on Part II of proposed Form SCIR in a structured format on EDGAR would enable investors and others—such as other government agencies, standard-setting groups, analysts, market data aggregators, and financial firms—to more easily and efficiently compare how one Covered Entity compares with others in terms of cybersecurity risks and incidents. For example, banks assessing potential security-based swap counterparties could efficiently aggregate and compare disclosures of multiple security-based swap dealers. Similarly, public companies deciding which transfer agent to use could efficiently aggregate and compare the disclosures of many transfer agents.

These market participants would also be able to discern broad trends in cybersecurity risks and incidents more efficiently due to the central filing location and machine-readability of the disclosures. The more efficient dissemination of information about trends regarding cybersecurity risks and significant cybersecurity incidents could, for example, enable Covered

Entities to better and more efficiently determine if they need to modify, change, or upgrade their cybersecurity defense measures in light of those trends. Likewise, more efficient assimilation of information about trends in significant cybersecurity incidents could enable Covered Entities customers, counterparties, members, or users and their services to more efficiently understand and manage their cybersecurity risks. Accordingly, centralized EDGAR filing of public cybersecurity disclosures in a machine-readable data language could help reduce the number of Covered Entities or their customers, counterparties, members, or users that suffer harm from cybersecurity breaches, or reduce the extent of such harm in the market, thus helping prevent or mitigate cybersecurity-related disruptions to the orderly operations of the U.S. securities markets.

Lastly, Covered Entities rely on electronic information, communication, and computer systems to perform their functions.[845] Because many Covered Entities play critical global financial system, a cyberattack against Covered Entities without strong cybersecurity protocols could lead to more widespread breaches. Therefore, the centralized, public, structured filing of cybersecurity disclosures with Part II of proposed Form SCIR, which would be updated promptly upon the occurrence of a new significant cybersecurity incident, would increase the efficiency with which new cybersecurity information would be assimilated into the market, thereby also likely increasing the speed with which Covered Entities could react to potential contagion. This increased agility on the part of Covered Entities could reduce potential contagion in the U.S. securities markets. Additionally, Covered Entities would know that the centralized, public filing of information about significant cybersecurity incidents would make comparison with their competitors easier, and this could motivate Covered Entities to take cybersecurity preparedness and risk management more seriously than they might otherwise, either by devoting more resources to cybersecurity or by addressing cybersecurity risks in a more effective manner. Such

---

[845] *See* section I.A.2. of this release (discussing how Covered Entities use information systems).

an effect could help reduce the number and extent of cybersecurity incidents, particularly those that negatively impact the U.S. securities markets.

As with Part I of proposed Form SCIR, the Commission also is proposing to require Covered Entities to identify themselves on Part II of proposed Form SCIR with a UIC, such as an LEI, if they have obtained one, to help facilitate efficient collection and analysis of cybersecurity incidents in the financial markets. The addition of UICs could facilitate coordinated inter-governmental responses to cybersecurity incidents that affect U.S. firms.[846] Existing identifiers that are not UICs are more limited in scope, such as CIK numbers, which are Commission-specific identifiers for companies and individuals that have filed reports with the Commission. This limits their utility in analyzing and comparing significant cybersecurity incidents among Covered Entities and non-Commission-regulated financial institutions.

The markets for different Covered Entities present customers, counterparties, members, registrants, or users with a complex, multi-dimensional, choice problem. In choosing a Covered Entity to work with, customers, counterparties, members, registrants, or users may consider cybersecurity risk exposure (*i.e.*, financial, operational, legal, etc.), past significant cybersecurity incidents, reputation, etc. While the Commission is not aware of any studies that examine the role perceptions of cybersecurity play in this choice problem, the extant academic literature suggests that investors focus on salient, headline-grabbing information, such as large losses of customer information, when making such choices.[847] Details regarding significant cybersecurity

---

[846] The Commission has recognized the benefits of LEIs in other contexts. *See Joint Industry Plan; Order Approving the National Market System Plan Governing the Consolidated Audit Trail*, Release No. 34–79318; File No. 4–698 (Nov. 15, 2016), 81 FR 84696, 84745 (Nov. 23, 2016) ("The Commission believes use of the LEI enhances the quality of identifying information for Customers by incorporating a global standard identifier increasingly used throughout the financial markets."); Investment Company Reporting Modernization, Release Nos. 33-10231; 34-79095; IC-32314; File No. S7-08-15 (Oct. 13, 2016), 81 FR 81870, 81877 (Nov. 18, 2016) ("Uniform reporting of LEIs by funds [] will help provide a consistent means of identification that will facilitate the linkage of data reported on Form N-PORT with data from other filings and sources that is or will be reported elsewhere as LEIs become more widely used by regulators and the financial industry.").

[847] *See, e.g.,* Brad M. Barber, Terrance Odean, and Lu Zheng, *Out of Sight, Out of Mind: The Effects of Expenses on Mutual Fund Flows*, 78 J. Bus. 2095 (2005) ("Out of Sight, Out of Mind").

incidents may allow customers, counterparties, members, registrants, or users to assess the severity of one incident compared to that of another. However, the public disclosures will be generalized (*i.e.*, summary descriptions) to a degree such that threat actors cannot take advantage of known vulnerabilities. Therefore, to the extent that cybersecurity disclosures from Covered Entities are "boilerplate," they may be less informative.[848] Thus, it may be difficult to choose among Covered Entities that have experienced similar significant cybersecurity incidents.

Significant cybersecurity incidents—especially those that involve loss of data or assets of customers, counterparties, members, registrants, or users—are likely to garner attention. Thus, the Commission expects that the proposed requirement to disclose significant cybersecurity incidents would have a direct effect on the choices of customers, counterparties, members, registrants, or users. In addition, third parties such as industry analysts—who may be more capable of extracting useful information across Covered Entities' disclosures—may incorporate it in assessment reports that are ultimately provided to customers, counterparties, members, registrants, or users. Whether directly or indirectly, Covered Entities with subpar cybersecurity policies and procedures—as revealed by a relatively large number of significant cybersecurity incidents—could face pressure to improve their policies procedures to reduce such incidents.[849]

The disclosures of significant cybersecurity incidents also should benefit a Covered Entity's current customers, counterparties, members, registrants, or users if the Covered Entity experiences a significant cybersecurity incident by providing notice that, for example, personal information, transaction data, securities, or funds may have been compromised. While the customers, counterparties, members, registrants, or users that are directly impacted may be individually notified of significant cybersecurity incidents based on individual state laws and

---

848 However, as discussed above, the process of adopting "boilerplate" language by Covered Entities may itself affect improvements in policies and procedures.

849 This assumes that customers, counterparties, members, registrants, or users evaluating the Covered Entities would favor those Covered Entities that include language that cites strong cybersecurity procedures in their disclosures. Further, the Commission assumes that customers, counterparties, members, registrants, and users would prefer to do business with Covered Entities that have "superior" cybersecurity procedures.

Commission rules, thus initiating timely remedial actions, other parties may benefit from the disclosures. Specifically, customers, counterparties, members, registrants, or users that are not affected by a significant cybersecurity incident may take the time to change and strengthen passwords, monitor account activity on a more consistent basis, and audit their financial statements for discrepancies.

b. Costs

The requirements to have reasonably designed policies and procedures to address cybersecurity risk and to report significant cybersecurity incidents to the Commission by filing Part I of proposed Form SCIR on EDGAR would—in practice—require the collection of the information that also would be used in the proposed public disclosures required to be made on Part II of proposed Form SCIR. Therefore, the disclosure requirement itself would not impose significant compliance costs beyond those already discussed with respect to the requirements to have reasonably designed policies and procedures to address cybersecurity risk and to report significant cybersecurity incidents to the Commission by filing Part I of proposed Form SCIR on EDGAR.[850] Generally, it is expected that a compliance analysis would be needed to summarize the cybersecurity risks faced by the Covered Entity and a summary of previous significant cybersecurity incidents. In addition, there may be internal legal review of the public disclosure and administrative costs would be incurred associated with posting the disclosure on the Covered Entity's website.

However, if the action of disclosing summary descriptions of a Covered Entity's cybersecurity risks and significant cybersecurity incidents encourages the Covered Entity and/or other Covered Entities to review their policies and procedures and potentially direct more resources to cybersecurity protection, that would be an additional cost. Moreover, the

---

[850] *See* sections IV.D.2. and IV.D.3. of this release (discussing the costs of those requirements).

disclosures may impose costs due to market reactions and exploitable information they may reveal to adverse parties.

Depending on the Covered Entity, reports of many significant cybersecurity incidents and, to a lesser extent, reports of greater cybersecurity risks and exposure to financial, operational, legal, reputational, or other consequences that could materially affect its business and operations as a result of a cybersecurity incident adversely impacting its information systems may bear costs arising from reactions in the marketplace. That is, a Covered Entity may lose business or suffer harm to its reputation and brand value.[851] These costs would be borne by the affected Covered Entity even if it made reasonable efforts to prevent them. If customers, counterparties, members, registrants, or users "overreact"[852] to disclosures of significant cybersecurity incidents, Covered Entities may pursue a strategy of overinvesting in cybersecurity precautions (to avoid such overreactions), resulting in reduced efficiency. The extent of such costs likely depends on a number of factors, including the size of a Covered Entity relative to others in the same category (*e.g.*, Covered Broker-Dealers, national securities exchanges, and clearing agencies), the severity and scope of the cybersecurity incident, and the availability of substitutes for a given Covered Entity.[853]

---

851 Customers, counterparties, members, registrants, and users would be more likely to act in response to realized significant cybersecurity incidents than in response to Covered Entities' descriptions of their cybersecurity risks and how they address those risks.

852 Such overreactions can be the result of overconfidence about the precision of the signal. *See, e.g.*, Kent Daniel, David Hirshleifer and Avanidhar Subrahmanyam, *Investor Psychology and Security Market Under- and Overreactions*, 53 J. Fin. 1839 (1998); *see also* Out of Sight, Out of Mind.

853 One can differentiate between the smallest and largest Covered Broker-Dealer. A large broker-dealer may be more able to absorb more costs associated with a cybersecurity incident and continue to stay in business than a small broker-dealer. In addition, a large broker-dealer could have a more prestigious reputation that may persuade customers to continue using it despite the cybersecurity event. Or a large broker-dealer could have more news about it in the public domain that dilutes bad news about cybersecurity incidents, whereas a smaller firm's name may become inextricably associated with one significant cybersecurity incident. In addition, significant cybersecurity incidents that are crippling and affect all of a Covered Entity's customers, counterparties, members, registrants, and users would be more costly its reputation than ones that are more localized. Lastly, the cost of lost business for a Covered Entity may be muted if there are fewer competitors to choose from. For example, there is only one national securities association (*i.e.*, FINRA) relative to 353 transfer agents. It therefore could be costly in terms of lost business for a transfer agent as its customers can transfer their business to one of the many others that perform the same services.

The national securities exchanges and clearing agencies that are currently registered with the Commission but are not active would not incur any costs related to the proposed public disclosure requirement if they remain inactive. However, if their operations restart, they likely would incur moderate costs associated with the disclosure because they may need to restart their websites and provide summary descriptions of their cybersecurity risks. No significant cybersecurity incidents would need to be disclosed initially since they have been dormant for so long. In addition, many transfer agents do not have websites. Therefore, those transfer agents that do not have websites would incur the cost of obtaining a domain name as well as establishing and maintaining a website (either by themselves or using a third party) before being able to post their public disclosures. Small, independent broker-dealers also may not have websites. In a 2015 survey of 13 broker-dealers, 80% of respondents stated that they have a web policy or program; however, 7.6% do not have a web policy or program and 13.3% of the respondents were not sure. Furthermore, 47% of respondents reported that less than half of their firm's advisors (i.e., registered representatives) currently have a website. Interestingly, the survey participants noted the value of having a website to establish credibility (80%), generate leads (53%), get referrals (40%), qualify and engage prospects (40%) and maintain existing client relationships (47%).[854] The remaining Market Entities likely have websites.

Website costs can be broken into several categories: (1) obtaining a domain name ($12 to $15 per year); (2) web hosting ($100 per month for premium service); (3) website theme or template (one-time fee of $20 to $200 or more); and SSL certificate ($10 to $200 per year).[855] Ongoing website costs could be as high as $1,215 per year to maintain.

---

854 *See Broker Dealers and Web Marketing: What You Should Know* (Dec. 9, 2015), *available at* https://www.advisorwebsites.com/blog/blog/general/broker-dealers-and-web-marketing-what-you-should-know#:~:text=While%2080%25%20of%20Broker-Dealers%20reps%20we%20polled%20say,to%20build%20and%20maintain%20a%20strong%20web%20presence.

855 *See* Jennifer Simonson, *Website Hosting Cost Guide 2023*, Forbes, *available at* https://www.forbes.com/advisor/business/website-hosting-cost/.

Mandating the disclosure of significant cybersecurity incidents entails a tradeoff. While disclosure can inform customers, counterparties, members, registrants, and users, disclosure can also inform cyber attackers that they have been detected. Also, disclosing too much (*e.g.*, the types of systems that were affected and how they were compromised) could be used by threat actors to better attack their targets, imposing subsequent potential losses on Covered Entities. For example, announcing a significant cybersecurity incident naming a specific piece of malware and the degree of compromise can provide details about the structure of the target's computer systems, the security measures employed (or not employed), and potentially suggest promising attack vectors for future targets by other would-be attackers.

Under proposed Rule 10, to mitigate these costs and to promote compliance with the disclosure requirements, each Covered Entity would be required to disclose summary descriptions of their cybersecurity risks and significant cybersecurity incidents on Part II of proposed Form SCIR.[856] In the summary description of the significant cybersecurity incident, the Covered Entity would need to identify: (1) the person or persons affected; (2) the date the incident was discovered and whether it is still ongoing; (3) whether any data were stolen, altered, or accessed or used for any other unauthorized purpose; (4) the effect of the incident on the Covered Entity's operations; and (5) whether the Covered Entity, or service provider, has remediated or is currently remediating the incident.[857] Thus, Covered Entities generally would not be required to disclose technical details about significant cybersecurity incidents that could compromise their cybersecurity protections going forward. As before, the costs associated with conveying this information to attackers is impracticable to estimate.[858]

---

856 *See* paragraph (d)(1) of proposed Rule 10.

857 *See* paragraph (d)(1)(ii) of proposed Rule 10.

858 As noted in section IV.B. of this release, firms are generally hesitant to provide information about cyberattacks. Similarly, cybercriminals are not generally forthcoming with data on attacks, their success, or factors that made the attacks possible. Consequently, data from which plausible estimates could be made is not available.

While registering with the EDGAR system is free, the requirement to centrally file Part II of proposed Form SCIR in EDGAR would impose incremental costs on Covered Entities that have not previously filed documents in EDGAR. More specifically, Covered Entities that have never made a filing with the Commission via EDGAR would need to file a notarized Form ID, which is used to request the assignment of access codes to file on EDGAR. Thus, first-time EDGAR filers would incur modest costs associated with filing Form ID.[859] That said, Covered Entities that already file documents in EDGAR would not incur the cost of having to register with EDGAR. As discussed earlier, the extent to which different categories of Covered Entities are already required to file documents in EDGAR varies. For example, SBSDs, MSBSPs, SBSDRs, and transfer agents are already required to file some forms in EDGAR.

Likewise, as mentioned earlier, the Commission approved a UIC—namely, the LEI—in a previous rulemaking. The Commission could approve another standard identifier as a UIC in the future, but currently the LEI is the only approved UIC. Covered Entities that already have an LEI would not bear any cost to including it on proposed Form SCIR, as they would have already paid to obtain and maintain an LEI for some other purpose. Covered Entities that do not already have an LEI are not required to obtain an LEI in order to file proposed Form SCIR, thus, there is no additional cost to those Covered Entities that do not have an LEI.

In addition, a Covered Broker-Dealer would be required to provide the written disclosure form to a customer as part of the account opening process. Thereafter, the Covered Broker-Dealer would need to provide the customer with the written disclosure form annually and when it is updated using the same means that the customer elects to receive account statements (*e.g.*, by email or through some type of postal service). The Commission anticipates that the cost of initial and annual reporting will be negligible because the report text can be incorporated into

---

[859] Any Covered Entity that has made at least one filing with the Commission via EDGAR since 2002 has been entered into the EDGAR system by the Commission and will not need to file Form ID to file electronically on EDGAR.

other initial disclosures and periodic statements. The cost of furnishing updated reports in response to significant cybersecurity incidents depends on the degree to which such incidents occur and are detected, which cannot reliably be predicted. The Commission assumes that the delivery costs are the same regardless of the delivery method.

To estimate the costs associated for a Covered Entity to file a Part II of proposed Form SCIR with the Commission through EDGAR, as well as post a copy of the form on its website, the Commission considered the initial and ongoing compliance costs.[860] The internal annual costs for these requirements (which include an initial burden estimate annualized over a three year period) are estimated to be $1,377.46 per Covered Entity, and $2,739,767.94 in total. These costs include a blended rate of $375.33 for an assistant general counsel, senior compliance examiner, and compliance manager for a total of 3.67 hours. The annual external costs for these requirements are estimated to be $1,488 per Covered Entity, and $2,959,632 in total. This includes the cost of using outside legal counsel at a rate of $496 per hour for a total of three hours.

To estimate the costs associated for a Covered Broker-Dealer to deliver its disclosures to new customers, as well as deliver disclosures to existing customers on an annual basis, the Commission considered the initial and ongoing compliance costs.[861] The internal annual costs for these requirements (which include an initial burden estimate annualized over a three year period) are estimated to be $3,536.94 per Covered Broker-Dealer, and $5,450,424.54 in total. These costs include a rate of $69 per hour for a general clerk for a total of 51.26 hours. It is estimated that there will be $0 annual external cost for this additional disclosure requirement for Covered Broker-Dealers. With respect to the additional disclosure fees for broker dealers, the cost covers the clerks employed by the broker-dealers for stuffing envelopes and mailing them

---

860 *See* section V of this release (discussing these costs in more detail).

861 *See* section V of this release (discussing these costs in more detail).

out. The legal fees associated with drafting the disclosure is already tied to the burden of filing the disclosure in Part II of EDGAR and putting the disclosure on its website.

c. Request for Comment

The Commission requests comment on all aspects of the foregoing analysis of the benefits and costs of the requirements to provide immediate notification and subsequent reporting of significant cybersecurity incidents. Commenters are requested to provide empirical data in support of any arguments or analyses. In addition, the Commission is requesting comment on the following matters:

16. Please provide views on the benefits and costs associated with posting the public disclosures on Covered Entities' websites and submitting them to the Commission through EDGAR. Will the general nature of the public disclosure be useful to Market Entities as well as customers, counterparties, members, participants, and users? Should the Commission require Covered Entities to both post cybersecurity risk and incident histories on Covered Entity websites and file that information on Part II of proposed Form SCIR in EDGAR? Should the Commission exempt some subset(s) of Covered Entities from the requirement to file Part II of proposed Form SCIR in EDGAR? If so, please explain. Should the Commission exempt some subset(s) of Covered Entities from the requirement to post cybersecurity risk and incident history information on their websites? Explain.

17. Are the cost estimates associated with posting the public disclosure on the Covered Entities' websites, submitting Part II of proposed Form SCIR to the Commission through EDGAR, and providing disclosures to new and existing customers reasonable? If not, explain why? Are there any other benefits and costs of these proposed requirements? If so, please describe them.

18. Are there any other costs and benefits associated with requiring Covered Entities to file Part II of proposed Form SCIR using a structured data language? If so, please describe them. Should the Commission require Covered Entities to file Part II of proposed Form SCIR using a structured data language, such as a custom XML? Should the Commission require Covered Entities to file Part II of proposed Form SCIR using a different structured data language than a custom XML, such as Inline XBRL? Why or why not?

19. Are there any Covered Entities for whom the proposed structured data requirements of Part II of proposed Form SCIR should be exempted? If so, what particular exemption threshold or thresholds should the Commission use for the structured data requirements under the proposed rule amendments, and why?

20. Please provide views on the benefits and costs associated with requiring Covered Entities to identify themselves on Part II of proposed Form SCIR with both a CIK number and a UIC (such as an LEI)? What would be the benefits and costs of requiring Covered Entities without a UIC to obtain one in order to file Part II of proposed Form SCIR? What, if any, standard identifiers should the Commission require Covered Entities to use to identify themselves on Part II of proposed Form SCIR?

21. What would be the benefits and costs of requiring Covered Entities to place the required cybersecurity risk and incident history disclosures on individual Covered Entity websites and in EDGAR with Part II of proposed Form SCIR relative to the alternatives discussed below in section IV.F. of this release? Should the Commission instead adopt one of the alternatives for the requirements around where Covered Entities must place the public cybersecurity disclosures? Specifically, the Commission is proposing to require Covered Entities to publish the disclosures on their individual firm websites and to file the information in

EDGAR using Part II of proposed Form SCIR. Should the Commission eliminate one, or both, of those requirements?

22. Are there any Covered Entities for whom the proposed structured data requirements for Part II of proposed Form SCIR should be exempted? If so, what particular exemption threshold or thresholds should the Commission use for the structured data requirements under the proposed rule amendments, and why?

5. Record Preservation and Maintenance by Covered Entities

As discussed above, proposed Rule 10 would require a Covered Entity to: (1) establish, maintain, and enforce written policies and procedures that are reasonably designed to address cybersecurity risks; (2) create written documentation of risk assessments; (3) create written documentation of any cybersecurity incident, including its response to and recovery from the incident; (4) prepare a written report each year describing its annual review of its policies and procedures to address cybersecurity risks; (5) provide immediate written notice of a significant cybersecurity incident; (6) report a significant cybersecurity incident on Part I of proposed Form SCIR; and (7) provide a written disclosure containing a summary description of its cybersecurity risk and significant cybersecurity incidents on Part II of proposed Form SCIR. Consequently, proposed Rule 10 would require a Covered Entity to create several different types of records, but it would not include its own record preservation and maintenance provisions. Instead, these requirements would be imposed through amendments, as necessary, to the existing record preservation and maintenance rules applicable to the Covered Entities. In particular, the Commission is proposing to amend the record preservation and maintenance rules for: (1) broker-dealers (*i.e.*, Rule 17a-4); (2) SBS Entities (*i.e.*, Rule 18a-6); and (3) transfer agents (*i.e.*, Rule 17ad-7). The proposed amendments would specify that the Rule 10 Records must be retained for three years. In the case of the written policies and procedures to address cybersecurity risks, the record would need to be maintained until three years after the termination of the use of the policies and procedures.

The existing record maintenance and preservation rule applicable to registered clearing agencies, the MSRB, national securities associations, and national securities exchanges (*i.e.*, Rule 17a-1) requires these categories of Covered Entities keep and preserve at least one copy of all documents, including all correspondence, memoranda, papers, books, notices, accounts, and other such records as shall be made or received by the Covered Entity in the course of its business as such and in the conduct of its self-regulatory activity. Under the existing provisions of Rule 17a-1, registered clearing agencies, the MSRB, national securities associations, and national securities exchanges would be required to preserve at least one copy of the Rule 10 Records for at least five years, with the first two years in an easily accessible place. Similarly, the existing record maintenance and preservation rule applicable to SBSDRs (*i.e.* Rule 13n-7) requires these Market Entities to preserve records. And with respect to exempt clearing agencies, the Commission is proposing to amend the clearing agency exemption orders to add a condition that each exempt clearing agency must retain the Rule 10 Records for a period of at least five years after the record is made or, in the case of the written policies and procedures to address cybersecurity risks, for at least five years after the termination of the use of the policies and procedures.

a. Benefits

There would be a number of benefits for Covered Entities to preserving and maintaining the Rule 10 records. With respect to cybersecurity policies and procedures and the written documentation concerning risk assessments and any cybersecurity incidents, the Covered Entity's records could be reviewed for compliance purposes as well as a reference in future self-conducted audits of the Covered Entity's cybersecurity system. In addition, the written report each year describing the Covered Entity's annual review of its policies and procedures could be used to determine if the Covered Entity's cybersecurity risk management program is working as expected and to see if any changes should be made. Lastly, maintaining records of compliance would assist the Commission in its oversight role, particularly when conducting examinations of

Covered Entities. With respect to the immediate written notice of a significant cybersecurity incident, as well as any submitted Part I of proposed Form SCIR, the records would facilitate examination of Covered Entities for compliance with proposed Rule 10.

Finally, with respect to the public disclosures that Covered Entities would make on Part II of proposed Form SCIR, keeping records of these forms and submissions would be beneficial to Covered Entities for compliance purposes as well as use as a reference when updating the public disclosure. For example, a Covered Entity would need to file an updated Part II of proposed Form SCIR if the information in the summary description of a significant cybersecurity incident included on the form is no longer within the look-back period (*i.e.*, the current or previous calendar year). However, the retention period for the records (*e.g.*, three years in the case of broker-dealers, SBS Entities, and transfer agents, or five years in the case of registered clearing agencies, the MSRB, national securities associations, national securities exchanges, SBSDRs, and certain exempt clearing agencies) would require the Covered Entity to maintain a record of that particular public disclosure for a longer period of time.

Benefits also arise due to the Commission's regulation and oversight of Covered Entities with respect to their books and records.[862]

b. Costs

The costs associated with preserving the Covered Entity's cybersecurity policies and procedures and annual review are likely to be small. The cost would result from the requirement to preserve the Rule 10 Records for either three or five years. Given that the incremental volume of records that each Covered Entity would be required to retain would be relatively small, the costs should be minimal. Moreover, Covered Entities subject to other record retention requirements likely already have a system in place to maintain those records. Therefore, adding the records associated with proposed Rule 10 likely would be a small burden.

---

[862] The Commission also would retain copies of Parts I and II of proposed Form SCIR filed through EDGAR.

To estimate the costs associated for a Covered Entity to comply with its recordkeeping maintenance and preservation requirement, the Commission considered the initial and ongoing compliance costs.[863] The internal annual cost for this requirement is estimated to be $441 per Covered Entity, and $877,149 in total. These costs include a blended rate of $73.50 for a general clerk and compliance clerk for a total of 6 hours. It is estimated that there will be $0 annual external cost for the recordkeeping maintenance and preservation requirement.

c. Request for Comment

The Commission requests comment on all aspects of the foregoing analysis of the benefits and costs of the proposed record preservation and maintenance requirements. Commenters are requested to provide empirical data in support of any arguments or analyses. In addition, the Commission is requesting comment on the following matter:

23. Are there any other benefits and cost associated with the requirements to preserve the Rule 10 Records? If so, please describe them.

6. Policies and Procedures, Annual Review, Immediate Notification of Significant Cybersecurity Incidents, and Record Preservation Requirements for Non-Covered Broker-Dealers

As discussed earlier, proposed Rule 10 would require Non-Covered Broker-Dealers to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks taking into account the size, business, and operations of the firm.[864] The proposed rule also would require Non-Covered Broker-Dealers to review the design and effectiveness of their cybersecurity policies and procedures annually, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review. Furthermore, Non-Covered Broker-Dealers would be required to provide the Commission and their examining authority with immediate written electronic notice of the

---

863 *See* section V of this release (discussing these costs in more detail).

864 *See* section II.C.1. of this release (discussing in more detail the proposed policies and procedures, annual review, and record preservation requirements for Non-Covered Broker-Dealers).

occurrence of a significant cybersecurity incident.[865] The Commission also is proposing to amend the record preservation and maintenance rule for broker-dealers (Rule 17a-4) to specifically require Non-Covered Broker-Dealers to preserve certain records in connection with Rule 10.

a. Benefits

The requirement under proposed Rule 10 for Non-Covered Broker-Dealers to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks would generally improve cybersecurity preparedness of Non-Covered Broker-Dealers—and hence reduce their clients' exposure to cybersecurity incidents. This is because, in establishing and maintaining a set of cybersecurity policies and procedures in a written format, a Non-Covered Broker-Dealer can evaluate whether its cybersecurity policies and procedures continue to work as designed and whether changes are needed to assure their continued effectiveness. In addition, by permitting Non-Covered Broker-Dealers to take into account their size, business, and operations of the firm when designing their written policies and procedures, Non-Covered Broker-Dealers can more efficiently utilize their resources. Moreover, by requiring Non-Covered Broker-Dealers to establish reasonably designed cybersecurity policies and procedures, the Commission would be better able to understand the protections that these broker-dealers put in place to address cybersecurity risk. During an examination, the Commission can assess the adequacy and completeness of a Non-Covered Broker-Dealers cybersecurity policies and procedures. Documenting a Non-Covered Broker-Dealer's cybersecurity policies and procedures in a written format also would aid the Commission in its review and oversight.

---

[865] The Commission is not proposing that Non-Covered Broker Dealers be subject to the requirements to file Parts I and II of proposed Form SCIR and post copies of the most recently filed Part II of proposed Form SCIR on their websites and provide copies of that filing to their customers.

Due to the varying sizes and operations of Non-Covered Broker-Dealers, the benefits that accrue from the cybersecurity policies and procedures requirement likely differ across entities. Because Non-Covered Broker-Dealers are generally smaller and have fewer assets and interconnections with other Market Entities than Covered Broker-Dealers, there is less of a risk that a significant cybersecurity incident at a Non-Covered Broker-Dealer could provide the threat actor with access to other Market Entities. However, even though a Non-Covered Broker-Dealer may not pose a significant overall risk to the U.S. securities markets, a significant cybersecurity event at a Non-Covered Broker-Dealer could have profound negative effects if a threat actor is able to misappropriate customers' confidential financial information. Consequently, greater cybersecurity investment by a Non-Covered Broker-Dealer likely would lead to significant benefits for itself and its customers.

Non-Covered Broker-Dealers may already have implemented cybersecurity policies and procedures. The marginal benefits of the proposed rule would be mitigated to the extent that these existing policies and procedures are consistent with the proposed rule's requirements. However, existing policies and procedures that are already consistent with the proposed rule would facilitate Non-Covered Broker-Dealers in conducting annual reviews, assessing the design and effectiveness of their cybersecurity policies and procedures, and making necessary adjustments.

The primary benefit of reviewing a Non-Covered Broker-Dealer's cybersecurity policies and procedures on an annual basis would help to ensure that they are working as designed, that they accurately reflect the firm's cybersecurity practices, and that they reflect changes and developments in the firm's cybersecurity risk over the time period covered by the review. The documented policies and procedures would serve as a benchmark when conducting the annual review. The Non-Covered Broker-Dealer would be required, for compliance purposes and future reference, to make a written record that documents the steps taken in performing the annual review and the conclusions of the annual review.

Cybersecurity threats constantly evolve, and threat actors consistently identify new ways to infiltrate information systems. An annual review requirement would ensure that Non-Covered Broker-Dealers conduct a regular assessment and undertake updates to prevent policies and procedures from becoming stale or ineffective, in light of the dynamism of cybersecurity threats.

The primary benefit of requiring Non-Covered Broker-Dealers to retain their written cybersecurity policies and procedures as well as a record of the annual reviews, is to assist the Commission in its oversight function. In reviewing their records, Non-Covered Broker-Dealers may see trends in their own cybersecurity risks, which may serve as an impetus to make adjustments to their cybersecurity policies and procedures. Furthermore, Proposed Rule 10 would expand beyond current Commission regulations Non-Covered Broker-Dealers' cybersecurity policies and procedures that address all cybersecurity risks that may affect their information systems and the funds and securities as well as personal, confidential, and proprietary information that may be stored on those systems.

As noted above, Non-Covered Broker-Dealers would be required to give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring. Compared to the suite of proposed requirements for Covered Entities, including filing Parts I and II of proposed Form SCIR and publicly disclosing Part II (which would contain summary descriptions of the Covered Entity's cybersecurity risks and significant cybersecurity incidents that occurred in current and previous calendar years), the proposed requirement to provide immediate written electronic notice of significant cybersecurity incidents is relatively small but can yield significant benefits. Most notably, such immediate notifications would make Commission staff aware of significant cybersecurity incidents across all broker-dealers and not just at Covered Broker-Dealers, thus significantly increasing its oversight powers in the broker-dealer space with respect to cybersecurity incidents. Trends that impact Non-Covered Broker-Dealers, such as through malware or a particular type of software, may be detected by staff,

which can then inform other Market Entities of emerging risks. This is particularly important due to the interconnected nature of the U.S. securities industry. Breaches that occur at Non-Covered Broker-Dealers may spread to larger firms, such as Covered Entities, that could cause more widespread financial disruptions. Furthermore, we anticipate that the burden on Non-Covered broker dealers of furnishing immediate written notification of a significant cybersecurity incident will be minimal.[866]

b. Costs

The costs associated with proposed Rule 10 for Non-Covered Broker-Dealers with respect to the written cybersecurity policies and procedures requirements would primarily result from establishing written cybersecurity policies and procedures that are reasonably designed. Such costs may be passed on to the Non-Covered Broker-Dealers' customers, either in part or in full.

Many Non-Covered Broker-Dealers currently have cybersecurity policies and procedures in place; to the extent a Non-Covered Broker-Dealer's existing policies and procedures are consistent with the requirements of the proposed rule, those Non-Covered Broker-Dealers would have limited need to update those policies and procedures, thus mitigating the costs of the proposal. Non-Covered Broker-Dealers may be subject to Regulation S-P, Regulation S-ID, and state regulations. In those particular instances, they may have already implemented policies and procedures that are consistent with the requirements of the proposed Rule 10, which would mitigate some of the compliance costs associated with the proposed policies and procedures requirements.

The cost of complying with the proposed annual review requirement along with the accompanying written review and conclusion would depend on the size, business, and operations of the Non-Covered Broker-Dealer. A Non-Covered Broker-Dealer with simpler operations

---

866 *See* section IV.D.6.b. of this release.

likely would incur lower annual review and modification costs than firms with larger operations. Furthermore, a Non-Covered Broker-Dealer may choose to hire a third-party for assistance or consultation regarding the completion of a written annual review and conclusion. This cost, in those situations, would depend on the services requested and the fees that are charged by the third-parties and consultants. Such costs could be passed along to the Non-Covered Broker-Dealer's customers depending on the competitive nature of the Non-Covered Broker-Dealer's market and its business model.

In either case, Non-Covered Broker-Dealers could tailor the policies and procedures to its cybersecurity risks taking into account its size, business, and operations. This offers Non-Covered Broker-Dealers the flexibility to implement cybersecurity policies and procedures based on the sophistication and complexity of their information systems. Of course, the cost of cybersecurity systems and modifications to cybersecurity policies and procedures may be higher as the size, business, and operation of a Non-Covered Broker-Dealer increases and becomes more complex.

The costs associated with giving the Commission immediate written electronic notice of a significant cybersecurity incident are likely to be relatively similar to, or possibly somewhat larger, than those incurred by Covered Broker-Dealers. As noted previously, the cost of immediate notification consists of notifying the Commission of a significant cybersecurity incident upon having a reasonable basis to conclude it has occurred or is occurring as well as researching the detailing of the incident in question. Non-Covered Broker-Dealers may be able to make the same determination and notify the Commission in the same amount of time as their Covered Broker-Dealer counterparts. However, smaller broker-dealers may not have the staffing or information technology expertise to make a reasonable decision about a suspected significant cybersecurity event as quickly as a Covered Broker-Dealer that may have in-house staff dedicated to this function, thus increasing the overall immediate notification cost. On the other hand, smaller broker-dealers could instead contract with third parties for cybersecurity functions

that could identify plausible significant cybersecurity attacks in the same amount of time as Covered Broker-Dealers. Unlike Covered Broker-Dealers, Non-Covered Broker-Dealers do not have to provide more detail beyond the immediate written notification requirement. Additional information regarding significant cybersecurity incidents do not have to be provided to the Commission on a confidential basis through the filing of Part I of proposed Form SCIR. Moreover, a summary of past incidents do not have to be publicly disclosed on their websites and with the Commission.

To estimate the costs associated with the proposed policies and procedures requirements and annual review requirements, the Commission considered the initial and ongoing compliance costs.[867] The internal annual costs for these requirements (which include an initial burden estimate annualized over a three year period) are estimated to be $9,702 per Non-Covered Broker-Dealer, and $19,103,238 in total. These costs include a blended rate of $462 for a compliance attorney and assistant general counsel for a total of 21 hours. The annual external costs for adopting and implementing the policies and procedures, as well as the annual review of the policies and procedures are estimated to be $2,480 per Non-Covered Broker-Dealer, and $4,883,120 in total. This includes the cost of using outside legal counsel at a rate of $496 per hour for a total of five hours.

The cost associated Non-Covered Broker Dealer to research a suspected cybersecurity incident and provide immediate written notification to the Commission were combined earlier with those costs for Covered Entities.[868] Broken out solely for Non-Covered Broker-Dealers, the Commission considered the initial and ongoing compliance costs. The internal annual costs for these requirements (which include an initial burden estimate annualized over a three year period) are estimated to be $1,648.51 per Non-Covered Broker-Dealer, and $3,245,916 in total. These

---

867 *See* section V of this release (discussing these costs in more detail).

868 *See* section IV.D.3.b. of this release (discussing the cost of immediate notification).

costs include a blended rate of $353 for an assistant general counsel, compliance manager, and systems analyst for a total of 4.67 hours. The annual external costs for these requirements are estimated to be $1,488 per Non-Covered Broker-Dealer, and $2,959,872 in total. This includes the cost of using outside legal counsel at a rate of $496 per hour for a total of three hours.

Pursuant to proposed Rule 10, a Non-Covered Broker-Dealer would be required to: (1) establish, maintain, and enforce written policies and procedures that are reasonably designed to address the cybersecurity risks of the firm; (2) make a written record that documents its annual review; and (3) provide immediate electronic written notice to the Commission of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring. The additional cost of the proposed amendments to Rule 17a-4 of preserving and maintaining these documents for three years, whether in paper or digital form, is likely minimal.

To estimate the costs associated for a Non-Covered Broker-Dealer to comply with its recordkeeping maintenance and preservation requirement, the Commission considered the initial and ongoing compliance costs.[869] The internal annual cost for this requirement is estimated to be $220.50 per Non-Covered Broker-Dealer, and $434,164.50 in total. These costs include a blended rate of $73.50 for a general clerk and compliance clerk for a total of 2 hours. It is estimated that there will be $0 annual external cost for the recordkeeping maintenance and preservation requirement.

c. Request for Comment

The Commission requests comment on all aspects of the foregoing analysis of the benefits and costs of the proposed requirements for Non-Covered Broker-Dealers. Commenters are requested to provide empirical data in support of any arguments or analyses. In addition, the Commission is requesting comment on the following matters:

---

[869] *See* section V of this release (discussing these costs in more detail).

24. What level of cybersecurity policies and procedures have Non-Covered Broker-Dealers implemented? For example, would they meet the cybersecurity policies and procedures requirements of the proposed rule, thus making the compliance cost relatively low? Are those policies and procedures documented?

25. Are there any other benefits and costs for a Non-Covered Broker-Dealer in establishing, maintaining, and enforcing written policies and procedures under proposed Rule 10? If so, please describe them.

26. Are the estimated costs of compliance for Non-Covered Broker-Dealers to establish, maintain, and enforce written policies and procedures cybersecurity policies and procedures that comply with the proposed rule reasonable? If not, why not?

27. Would Non-Covered Broker-Dealers consult with a third party or hire a consultant with cybersecurity expertise in order to establish the cybersecurity policies and procedures under proposed Rule 10?

28. Are there quantifiable benefits to complying with the cybersecurity policies and procedures requirements of the proposed rule? If so, please describe them. Are there quantifiable costs for Non-Covered Broker-Dealers to review their cybersecurity policies annually that are different than those discussed above? If so, describe them.

29. Are there any other benefits in reviewing and updating Non-Covered Broker-Dealers' cybersecurity policies and procedures on an annual basis? If so, please describe them.

30. Is the estimated cost to review Non-Covered Broker-Dealers cybersecurity policies and procedures reasonable? If not, explain why?

31. Would it be more or less costly to outsource the responsibility of an annual review of cybersecurity policies and procedures to a third party?

7. Substituted Compliance for Non-U.S. SBS Entities

Commission Rule 3a71-6 states that the Commission may, conditionally or unconditionally, by order, make a determination with respect to a foreign financial regulatory system that compliance with specified requirements under such foreign financial regulatory system by a registered SBS Entity or class thereof, may satisfy the certain requirements that would otherwise apply to such an SBS Entity (or class thereof). The Commission may make such substituted compliance determinations to permit SBS Entities that are not U.S. persons (as defined in 17 CFR 240.3a71-3(a)(4)), but not SBS Entities that are U.S. persons, to satisfy the eligible requirements by complying with comparable foreign requirements.[870] The Commission is proposing to amend Rule 3a71-6 to permit eligible applicants[871] to seek a Commission determination with respect to the cybersecurity requirements of proposed Rule 10 and Form SCIR as applicable to SBS Entities that are not U.S. persons.[872] Additionally, Rule 3a71-6 currently permits eligible applicants to seek a substituted compliance determination from the Commission with regard to the requirements of Rule 18a-6, including the proposed amendments to Rule 18a-6 if adopted.[873]

a. Benefits

The Commission is proposing amendments to Rule 3a71–6 to make substituted compliance available to eligible SBS Entities that are not U.S. persons, if the Commission determines that compliance with specified requirements under a foreign financial regulatory system by a registered SBS Entity, or class thereof, satisfies the corresponding requirements of proposed Rule 10 and Form SCIR. Other regulatory regimes may achieve regulatory outcomes that are comparable to the Commission's proposed cybersecurity risk management requirements.

---

870 *See* 17 CFR 240.3a71-6(d).

871 *See* 17 CFR 240.3a71-6(c).

872 *See* section II.D.3.

873 *See* paragraph (d)(6) of Rule 3a71-6.

Allowing for the possibility of substituted compliance may avoid regulatory duplication and conflict that may increase entities' compliance burdens without an analogous increase in benefits. The availability of substituted compliance could decrease the compliance burden for non-U.S. SBS Entities, in particular as it pertains to the establishment, maintenance, and enforcement of cybersecurity policies and procedures, notification and reporting to regulators, disclosure of cybersecurity risks and incidents, and record preservation. Allowing for the possibility of substituted compliance may help achieve the benefits of proposed Rule 10, Form SCIR, and the proposed amendments to Rule 18a-6 in a manner that avoids the costs that SBS Entities that are not U.S. persons would have to bear due to regulatory duplication or conflict.

Further, substituted compliance may have broader market implications, namely greater foreign SBSDs' activity in the U.S. market, expanded access by both U.S. and foreign SBS Entities to global liquidity, and reduced possibility of liquidity fragmentation along jurisdictional lines. The availability of substituted compliance for non-U.S. SBS Entities also could promote market efficiency, while enhancing competition in U.S. markets. Greater participation and access to liquidity is likely to improve efficiencies related to hedging and risk sharing while simultaneously increasing competition between domestic and foreign SBS Entities.

b. Costs

The Commission believes that the availability of substituted compliance for proposed Rule 10, Form SCIR, and the proposed amendments to Rule 18a-6 will not substantially alter the benefits intended by those requirements. In particular, it is expected that the availability of substituted compliance will not detract from the risk management benefits that stem from implementing proposed Rule 10, Form SCIR, and the proposed amendments to Rule 18a-6.

To the extent that substituted compliance reduces duplicative compliance costs, non-U.S. SBS Entities may incur lower overall costs associated with cybersecurity preparedness than they would otherwise incur without the option of substituted compliance availability, either because a non-U.S. SBS Entity may have already implemented foreign regulatory requirements which have

been deemed comparable by the Commission, or because security-based swap counterparties eligible for substituted compliance do not need to duplicate compliance with two sets of comparable requirements.

A substituted compliance request can be made either by a foreign regulatory jurisdiction on behalf of its market participants, or by the registered market participant itself.[874] The decision to request substituted compliance is voluntary, and therefore, to the extent that requests are made by individual market participants, such participants would request substituted compliance only if compliance with foreign regulatory requirements was less costly, in their own assessment, than compliance with both the foreign regulatory regime and the relevant Title VII requirements, including the requirements of proposed Rule 10, Form SCIR, and the proposed amendments to Rule 18a-6. Even after a substituted compliance determination is made, market participants would only choose substituted compliance if the benefits that they expect to receive exceed the costs that they expect to bear for doing so.

E. Effects on Efficiency, Competition, and Capital Formation

As discussed in the foregoing sections, market imperfections could lead to underinvestment in cybersecurity by Market Entities, and information asymmetry could contribute to a market-wide inefficient provision of cybersecurity defenses. The proposed rule aims to mitigate the inefficiencies resulting from these imperfections by: (1) imposing mandates for cybersecurity policies and procedures that could reduce cybersecurity underinvestment; (2) creating a reporting framework that could improve information sharing and improved cybersecurity defense investment and protection; and (3) providing public disclosure to inform Covered Entities' customers, counterparties, members, registrants, or users about the Covered Entities' cybersecurity efforts and experiences, thus potentially reducing information

---

[874] *See* 17 CFR 240.3a71-6(c).

asymmetry.[875] While the proposed rule has the potential to mitigate inefficiencies resulting from market imperfections, the scale of the overall effect would depend on numerous factors, including the state of existing of cybersecurity preparations,[876] the degree to which the proposed provisions induce increases to these preparations, the effectiveness of additional preparations at reducing cybersecurity risks,[877] the degree to which customers, counterparties, members, registrants, and users value additional cybersecurity preparations,[878] the degree of information asymmetry and bargaining power between customers, counterparties, members, registrants, and users vis-à-vis Market Entities,[879] the bargaining power of Market Entities vis-à-vis service providers,[880] service providers' willingness to provide bespoke contractual provisions to affected Market Entities,[881] the informational utility of the proposed disclosures, the scale of the negative externalities on the broader financial system,[882] the effectiveness of existing information sharing arrangements, and the informational utility of the required regulatory reports (as well as the Commission's ability to make use of them).[883]

---

875 *See* sections IV.B. and IV.D. of this release (discussing the broad economic considerations and benefits and costs of the proposals, respectively.

876 *See* section IV.C.1. of this release. Here, the Commission is concerned about the degree to which Market Entities' state of cybersecurity preparations diverge from socially optimal levels.

877 Formally, the marginal product of the proposed policies and procedures in the production of cybersecurity defenses.

878 Formally, customers', counterparties', members', registrants', and users' utility functions – specifically the marginal utilities of Covered Entities' and Non-Covered Broker-Dealers' cybersecurity policies and procedures.

879 In other words, the degree to which customers, counterparties, members, registrants, or users can affect the policies of Market Entities. Generally, the Commission expects that customers, counterparties, members, registrants, or users may be smaller than the affected Market Entity with which they conduct business and thus be subject to asymmetry and have limited ability to affect the policies of the Market Entity. However, that may not always be the case. For example, for customers of broker-dealers, the situation is likely to involve more heterogeneity, with some parties (*e.g.*, small retail clients) wielding very little power over the broker-dealer's policies while others (*e.g.*, large institutional investors) wielding considerable power.

880 In certain cases, a Covered Entity may determine that a competing service provider can be used as a bargaining chip in the renegotiation of existing service agreements, potentially imposing substantial contracting costs on the parties, which would eventually be passed on to the Covered Entities' customers, counterparties, members, participants, or users.

881 *Id.*

882 *See* sections IV.D.2.a. and IV.D.2.b. of this release.

883 *See* section IV.D.3. of this release.

However, since the proposed cybersecurity policies and procedures and related annual assessment are intended to prevent cybersecurity incidents at Market Entities that would otherwise cause financial loss and operational failure, compliance with the proposed rule likely would result in a safer environment to engage in securities transactions that protects the efficiency with which markets operate. Specifically, the proposed requirements are intended to protect the efficiency of securities market through the prevention of cybersecurity incidents that can adversely impact Market Entities and that, in turn, can interrupt the normal operations of U.S. securities markets and disrupt the efficient flow of information and capital.

The additional requirements applicable to Covered Entities (namely, the specific elements of the cybersecurity policies and procedures, the reporting to the Commission of any significant cybersecurity incident through Part I of proposed Form SCIR, and the disclosure of cybersecurity risks and significant cybersecurity incidents) would also allow for greater information sharing and would reduce the risk of underinvestment in cybersecurity across the securities industry. For example, confidential reporting to the Commission through Part I of proposed Form SCIR would provide regulators with the opportunity to promptly begin to assess the situation when a Covered Entity is experiencing a significant cybersecurity incident and begin to evaluate potential impacts on the market. In addition, public disclosures by Covered Entities through Part II of proposed Form SCIR and website postings would allow their customers, counterparties, members, registrants, and users to manage risk and choose with whom to do business, potentially allocating their resources to Covered Entities with greater cybersecurity preparedness. In addition, the sharing of information through public disclosures could assist in the development and implementation of cybersecurity policies and procedures, particularly by smaller and less sophisticated Market Entities which likely have fewer resources to develop robust cybersecurity protocols. Such information may be useful to them in in choosing one option over another, potentially allowing those smaller and less sophisticated Market Entities to develop their cybersecurity protection in the most cost-effective way possible.

Because the proposed rule would likely have differential effects on Market Entities along a number of dimensions, its overall effect on competition among Market Entities may be difficult to predict in certain instances. For example, smaller Market Entities, such as Non-Covered Broker-Dealers and certain transfer agents are likely to face disproportionately higher costs relative to revenues resulting from the proposed rule.[884] With respect to broker-dealers, the Commission has endeavored to provide Non-Covered Broker-Dealers with a more limited and flexible set of requirements that better suits their business models and would therefore be less onerous. Still, a number of small broker-dealers would be subject to the proposed rule as Covered Entities, which could tilt the competitive playing field in favor of their larger Covered Broker-Dealer counterparts.[885] In addition, all transfer agents would be Covered Entities under the proposed rule, regardless of their size, so the same concern is present.

On the other hand, if customers, counterparties, members, registrants, or users believe that the proposed rule effectively induces the appropriate level of cybersecurity effort among Market Entities, smaller Market Entities would likely benefit the most from these improved perceptions, as they would be thought to have sufficient cybersecurity policies and procedures in place compared to not having enough cybersecurity protections. Similar differential effects can occur within a particular group of Market Entities and service providers that are more (or less) focused on their cybersecurity.

With respect to competition among Covered Entities' service providers, the overall effect of the proposed rule and amendments is similarly ambiguous. It is likely that requiring affected Covered Entities to request oversight of service providers' cybersecurity practices pursuant to a written contract would lead some service providers to cease offering services to affected Covered

---

884 *See* section IV.B. of this release.

885 *See* section VI.C. of this release (noting that certain small broker-dealers would meet the definition of "covered entity" for purposes of the proposed rule).

Entities.[886] The additional regulation could serve as a barrier to entry to new service providers and could disproportionally affect would-be Market Entities.

In terms of capital formation, the proposed rule would have second-order effects, namely through a safer financial marketplace. As noted above, FSOC states that a destabilizing cybersecurity incident could potentially threaten the stability of the U.S. financial system by causing, among other things, a loss of confidence among a broad set of market participants, which could cause participants to question the safety or liquidity of their assets or transactions, and lead to significant withdrawal of assets or activity.[887] The Market Entities covered by this rule play important roles in capital formation through the various services they provide.[888] Due to their interconnected systems, a significant cybersecurity incident affecting Market Entities could have a cascading effect across the U.S. financial system with a significant impact on investor confidence, resulting in withdrawal of assets and impairment of capital formation.

The proposed rule provides the backbone for having sufficient cybersecurity measures in place to protect customer information, funds, and securities. Moreover, proposed provisions likely would lead to increased efficiency in the market, thus resulting in improved capital formation.[889] With a more predictable investment environment due to improved cybersecurity implementation by Market Entities and service providers, capital formation through the demand for securities offerings will be less prone to interruptions.

---

886 *See* section I.A.1. of this release.

887 *See* FSOC 2021 Annual Report.

888 *See* sections I.A.1. and II.A.1. of this release.

889 The proposed provisions do not implicate channels typically associated with capital formation (*e.g.*, taxation policy, financial innovation, capital controls, intellectual property, rule-of-law, and diversification). Thus, the proposed rule are likely to have only indirect, second order effects on capital formation arising from any improvements to economic efficiency. Qualitatively, these effects are expected to be small.

As part of the analysis on competition, efficiency, and capital formation, the Commission requests comment from all parties, particularly the Market Entities that are affected by these proposed rule:

a. Do firms within the Covered Entity and Non-Covered Broker-Dealer groups compare their cybersecurity safety measures among themselves or among firms of a particular type within a group (e.g., national securities exchanges only or transfer agents only)? Does one entity's level of cybersecurity protection incentivize competing entities to improve their cybersecurity policies and procedures? Is it possible that an entity with subpar cybersecurity protocols may be forced to exit the market, either because of business migrating to its competitors or because of the sheer number of cybersecurity incidents at that entity?

b. Would better cybersecurity policies and procedures, especially those that are reviewed and updated, provide more stability in the securities markets that encourages additional investment?

c. Would public disclosures of cybersecurity risks and significant cybersecurity incidents during the current or previous calendar year encourage investment in cybersecurity protections that later provide more stability in the market, thus encouraging capital formation?

d. Does the Commission's knowledge of cybersecurity incidents as well as of the policy and procedures at Market Entities lead to a calming effect on the market though oversight and compliance with the proposed rule, which would then foster greater capital formation?

F. Reasonable Alternatives

1. Alternatives to the Policies and Procedures Requirements of Proposed Rule 10

a. Require Only Disclosure of Cybersecurity Policies and Procedures Without Prescribing Specific Elements

Rather than requiring Covered Entities to adopt cybersecurity policies and procedures with specific enumerated elements, the Commission considered requiring Covered Entities to only provide explanations or summaries of their cybersecurity practices to their customers, counterparties, members, registrants, or users. In this alternative scenario, each Covered Entity would provide a disclosure containing a general overview of its existing cybersecurity policies and procedures, rather than be required to establish cybersecurity policies and procedures pursuant to the requirements of paragraph (b) of proposed Rule 10. Under this alternative, the general disclosure about the Covered Entity's cybersecurity policies and procedures would be publicly available to its customers, counterparties, members, registrants, and users, but it would not reveal specific details of the Covered Entity's policies and procedures. Further, under this alternative, detailed and comprehensive information about the Covered Entity's cybersecurity risks and protocols—including the policies and procedures themselves—would remain internal to the Covered Entity. The only other organizations that would be able to review or examine this more detailed information would be the Commission, FINRA, the MSRB (to the extent applicable), and other regulators with authority to examine this information in the course of their oversight activities.

This alternative approach would create weaker incentives for Covered Entities to address potential underspending on cybersecurity measures, as it would rely, in part, on customers', counterparties', members', registrants', or users' (or third parties' providing analyses to those customers, counterparties, members, registrants, or users)[890] ability to assess the effectiveness of Covered Entities' cybersecurity practices from the Covered Entities' public disclosures. Further, any benefits to be gained by requiring public disclosure of a Covered Entity's cybersecurity

---

[890] *See* section IV.D.1.a. of this release.

policies and procedures can also be realized through the proposed rule's public disclosure requirement. In particular, proposed Rule 10 would require each Covered Entity to provide a summary description of the cybersecurity risks that could materially affect its business and operations and how the Covered Entity assesses, prioritizes, and addresses those cybersecurity risks. In addition, each Covered Entity would need to disclose a summary description of each significant cybersecurity incident that occurred during the current or previous calendar year, if applicable. This disclosure would serve as another way for market participants to evaluate the Covered Entity's cybersecurity risks and vulnerabilities apart from the general disclosure of its cybersecurity risks. As mentioned above, this information could be useful to the Covered Entity's customers, counterparties, members, registrants, or users to manage their own cybersecurity risks and, to the extent they have choice, select a Covered Entity with whom to transact or otherwise conduct business.[891]

Given the cybersecurity risks of disclosing detailed explanations of cybersecurity practices (which would necessarily be disclosed if the Covered Entity would be required to disclose its existing cybersecurity policies and procedures),[892] it is likely that requiring such disclosure would result in the Covered Entity including only general language in its disclosure and providing few, if any, specific details that could be used by threat actors to take advantage of weak links in a Covered Entity's cybersecurity preparedness. Consequently, this alternative "disclosure-only" regime for cybersecurity policies and procedures would be unlikely to provide enough information and detail to differentiate between one Covered Entity's cybersecurity policies and procedures from another's policies and procedures, thus maintaining information asymmetry between the Covered Entity and other market participants. If information asymmetry

---

891 Furthermore, third-party financial service firms could conduct studies on cybersecurity preparedness at Market Entities, such as certain entities not being in line with industry practices or standards, which also could inform the choices of customers, counterparties, members, registrants, or users.

892 *See* section IV.D.2.b. of this release (discussing tradeoffs of cybersecurity disclosure).

was maintained, it is unlikely that meaningful change could be effected in the Covered Entities' cybersecurity practices through market pressure or Commission oversight over the Covered Entity's policies and procedures.[893] Furthermore, not requiring specific enumerated elements in cybersecurity policies and procedures would likely result in less uniform cybersecurity preparedness across Covered Entities, leaving market participants with inconsistent information about the robustness of Covered Entities' cybersecurity practices. However, if Market Entities believed that providing more detailed information would give them a competitive advantage, they would do so.

On the other hand, the costs associated with this alternative likely would be minimal relative to those associated with the proposed requirements regarding written policies and procedures, as Covered Entities would be unlikely to face pressure to adjust their existing cybersecurity policies and procedures as long as they do not experience any significant cybersecurity incidents. However, if a Covered Entity does experience a significant cybersecurity incident, it may force the Covered Entity to revise its existing cybersecurity policies and procedures and consequently revise its disclosures to other market participants concerning its cybersecurity policies and procedures. It is also conceivable that being required to make public disclosures regarding its cybersecurity policies and procedures or undergoing third-party market analyses that aggregate these types of disclosures (and may focus on, for example, the Covered Entity's lack of conformity with industry practices and standards) may provide the impetus for a Covered Entity to make its cybersecurity policies and procedures more robust.

b. Limiting the Scope of the Proposed Cybersecurity Policies and Procedures with Respect to Third-Party Service Providers

The Commission also considered limiting the scope of the proposed requirement that the Covered Entity's policies and procedures require oversight of service providers that receive,

---

[893] Here, changes in cybersecurity practices would depend entirely on market discipline exerted by relatively uninformed market participants.

maintain, or process the Covered Entity's information, or are otherwise permitted to access the Covered Entity's information systems and the information residing on those systems, pursuant to a written contract between the Covered Entity and the service provider.[894] Specifically, the Commission considered narrowing the scope of service providers in the enumerated categories discussed above[895] and requiring a periodic review and assessment of the pared-down list of service providers' cybersecurity policies and procedures rather than apply the Service Provider Oversight requirement to each service prover that receives, maintains, or processes the Covered Entity's information, or is otherwise permitted to access the Covered Entity's information systems and the information residing on those systems. The types of service providers that would still be covered by the written contract requirement would be those that provide cybersecurity related-services as well as business-critical services that are necessary for a Covered Entity to operate its core functions. The Commission further considered requiring service providers that receive, maintain, or process the Covered Entity's information, or are otherwise permitted to access the Covered Entity's information systems and the information residing on those systems to provide security certifications in lieu of the written contract requirement.

Narrowing the scope of the types of service providers affected by the proposal could lower costs for Covered Entities, especially smaller Covered Entities that rely on generic contracts with service providers (because they have less negotiating power with their service providers) and would have difficulty effecting changes in contractual terms with such service providers.[896] However, in the current technological context in which businesses increasingly rely on third-party "cloud services" that effectively place business data out of the business'

---

894 *See* paragraph (b)(1)(iii)(B) of proposed Rule 10 (setting forth the Service Provider Oversight Requirement).

895 *See* section IV.C.2.h. of this release.

896 *See* section IV.D.1.b. of this release (discussing service providers).

immediate control, the cybersecurity risk exposure of Covered Entities is unlikely to be limited to (or even concentrated in) certain named service providers. Narrowing the scope of service providers likely would lead to lower costs only insofar as it reduces effectiveness of the regulation. A related basis to reject this alternative is the signaling effect that it sends to threat actors. By excluding certain categories of service providers, the Commission could be providing information to threat actors about which service providers would be easiest to attack, as that universe of excluded vendors may have relatively inferior policies and procedures than vendors that are covered by the proposed rule.

Alternatively, maintaining the proposed scope but only requiring a standard, recognized, certification in lieu of a written contract could also lead to cost savings for Covered Entities, particularly if the certification is completed in-house or if a particular entity has many service contracts with different third parties that specify they are in compliance with the certification.[897] However, the Commission preliminary believes that it would be difficult to prescribe a set of characteristics for such a "standard" certification that would sufficiently address the varied types of Covered Entities and their respective service providers.[898] Another difficulty may be that if a single third-party entity is used for the certification, that entity would have to be well-versed in all contracted services in order to accurately assess them for compliance. In contrast, individualized contracts with each service provider likely would ensure better compliance with the intent of the proposed rule as those third-party providers specialize in the services that they offer.

---

[897] Service providers may currently be providing certifications as part of a registrant's policies and procedures. *See also* section II.B.1.g. of this release (seeking comment on alternative approaches to the Service Provider Oversight Requirement, including whether this cybersecurity risk could be addressed through policies and procedures to obtain written assurances or certifications from service providers that the service provider manages cybersecurity risk in a manner that would be consistent with how the Covered Entity would need to manage this risk under paragraph (b) of proposed Rule 10).

[898] *See* section IV.C.3. of this release(discussing the variety of affected registrants); *see also* section IV.F.1. of this release (discussing the limitations of uniform prescriptive requirements).

c. Require Specific Standardized Elements for Addressing Cybersecurity Risks of Covered Entities

The Commission considered including more standardized elements in that would need to be included in a Covered Entity's cybersecurity policies and procedures. For example, Covered Entities could be required to implement particular controls (*e.g.*, specific encryption protocols, network architecture, or authentication procedures) that are designed to address each general element of the required cybersecurity policies and procedures. Given the considerable diversity in the size, focus, and technical sophistication of affected Covered Entities,[899] any specific requirements likely would result in some Covered Entities needing to substantially alter their cybersecurity policies and procedures.

The potential benefit of such an approach would be to provide assurance that Covered Entities have implemented certain specific cybersecurity practices. But this approach would also entail considerably higher costs, as many Covered Entities would need to adjust their existing practices to something else that is more costly than potential alternatives that could provide the same outcome level of protection. In addition, considering the variety of Covered Entities registered with the Commission, it would be exceedingly difficult for the Commission to devise specific requirements that are appropriately suited for all Covered Entities: a uniform set of requirements would certainly be both over- and under-inclusive, while providing varied requirements based on the circumstances of each Covered Entity would be complex and impractical. For example, standardized requirements that ensure reasonably designed cybersecurity policies and procedures for the largest, most sophisticated and active Covered Entities would likely be overly burdensome for smaller and less sophisticated Covered Entities with more limited cybersecurity risk exposures. Conversely, if these standardized requirements were tailored to smaller Covered Entities with more limited operations or cybersecurity risks,

---

[899] *See* section IV.C.3. of this release.

such requirements likely would be inadequate in addressing larger Covered Entities' cybersecurity risks. As a result, instituting blanket requirements likely would not provide the most efficient and cost-effective way of instituting appropriate cybersecurity policies and procedures.

An important cost associated with this approach is the burden and complexity of prescribing detailed technical requirements tailored to the broad variety of Covered Entities that would be subject to proposed Rule 10. More broadly, imposing standardized requirements would effectively place the Commission in the role of dictating details related to the information technology practices of Covered Entities without the benefit of the Covered Entities' knowledge of their own particular circumstances. Moreover, given the complex and constantly evolving cybersecurity landscape, detailed regulatory requirements for cybersecurity practices would likely limit Covered Entities' ability to adapt quickly to changes in the cybersecurity landscape.[900]

d. Require Audits of Internal Controls Regarding Cybersecurity

Instead of requiring all Market Entities to establish, maintain, and enforce cybersecurity policies and procedures, the Commission considered requiring these entities to obtain audits of the effectiveness of their existing cybersecurity controls—for example, obtaining third-party audits with respect to their cybersecurity practices. This approach would not require Market Entities to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks as proposed, but instead would require Market Entities to engage an independent, qualified third party to assess their cybersecurity controls and prepare a report describing its assessment and any potential deficiencies.

---

[900] If as in the previous example, the Commission were to require Covered Entities to adopt a specific encryption algorithm, future discovery of vulnerabilities in that algorithm would prevent registrants from fully mitigating the vulnerability (*i.e.*, switching to improved algorithms) in the absence of Commission action.

Under this alternative, an independent third party (*e.g.*, an auditing firm) would certify to the effectiveness of the Market Entities' cybersecurity practices. If the firms providing such certifications have sufficient reputational motives to issue credible assessment,[901] and if the scope of such certifications is not overly circumscribed,[902] it is likely that Market Entities' cybersecurity practices would end up being more robust under this alternative than under the current proposal. By providing certification of a Market Entities' cybersecurity practices, a firm would—in effect—be lending its reputation to the Market Entity. Because "lenders" are naturally most sensitive to downside risks (here, loss of reputation, lawsuits, damages, and regulatory enforcement actions), one would expect them to avoid "lending" to Market Entities with cybersecurity practices whose effectiveness is questionable.[903]

While certification by industry-approved third parties could lead to more robust cybersecurity practices, the costs of such an approach would likely be considerably higher. Because of the aforementioned sensitivity to downside risk, firms would likely be hesitant to provide cybersecurity certifications without a thorough understanding of a Market Entity's systems and practices. In many cases, developing such an understanding would involve considerable effort particularly for certain larger and more sophisticated Covered Entities.[904] In addition, there may be a need for a consensus as to what protocols constitute industry standards

---

901 This would be the case if there was sufficient market pressure or regulatory requirements to obtain certification from "reputable" third-parties with business models premised on operating as a going-concern and maintaining a reputation for honesty.

902 In this alternative, it is assumed that certification would not be limited to only evaluating whether a Market Entity's stated policies and procedures are reasonably designed, but rather also would include an assessment of whether the policies and procedures are actually implemented in an effective manner.

903 Under the proposal it is the Market Entity itself that effectively "certifies" its own cybersecurity policies and procedures. Like the third-party auditor, the Market Entity faces down-side risks from "certifying" inadequate cybersecurity practices (*i.e.*, Commission enforcement actions). However, unlike the auditor, the Market Entity also realizes the potential up-side: cost savings through reduced cybersecurity expenditures.

904 It would be difficult for an auditor to provide a credible assessment of the effectiveness of the Market Entity's cybersecurity practices without first understanding the myriad of systems involved and how those practices are implemented. Presumably, a Market Entity would not bear these costs as it is likely to possess such an understanding.

in which certifying third parties would need to stay proficient. Finally, while such a scenario is somewhat similar to the Service Provider Oversight Requirement, this alternative does not allow for immediate repercussions or remediation if the third-party finds deficiencies in the Covered Entity's cybersecurity policies and procedures. The Commission would need to have a copy of the report and audit the Market Entity to ensure that Market Entity subsequently resolved the problem(s). This leads to an inefficient method of implementing reasonably designed cybersecurity policies and procedures.

e. Bifurcate Non-Broker-Dealer Market Entities into Covered Entities and Non-Covered Entities

The Commission considered bifurcating other categories of Market Entities into Covered Entities and Non-Covered Entities (in addition to broker-dealers) based on certain characteristics of the firm such that the Non-Covered Entities would not be required to include certain elements in their cybersecurity risk management policies and procedures. For example, the Commission considered defining as Non-Covered Entities Market Entities with assets below a certain threshold or with only a limited number of customers, counterparties, members, registrants, or users. This approach also could be scaled based on a Covered Entity's size, business, or another criterion, similar to the proposed distinction between Covered Broker-Dealers and Non-Covered Broker-Dealers. However, as discussed above, cybersecurity risks are likely to be unique to each Covered Entity primarily because Covered Entities vary drastically based on their size, business, and the services they provide. It would be difficult come up with one characteristic that is common to all Covered Entities such that each of them can be both broken out into separate groups. For example, it would be difficult to differentiate between transfer agents the same way one could distinguish between large and small clearing agencies or even harder, national

securities associations. The only effective way to differentiate firms with a given Covered Entity category is to choose a characteristic that is sensible for the type of Covered Entity.[905]

Finally, as discussed earlier, in determining which Market Entities should be Covered Entities and which should be Non-Covered Entities, the Commission considered: (1) how the category of Market Entity supports the fair, orderly, and efficient operation of the U.S. securities markets and the consequences if that type of Market Entity's critical functions were disrupted or degraded by a significant cybersecurity incident; (2) the harm that could befall investors, including retail investors, if that category of Market Entity's functions were disrupted or degraded by a significant cybersecurity incident; (3) the extent to which the category of Market Entity poses cybersecurity risk to other Market Entities though information system connections, including the number of connections; (4) the extent to which the category of Market Entity would be an attractive target for threat actors; and (5) the personal, confidential, and proprietary business information about the category of Market Entity and other persons (*e.g.*, investors) stored on the Market Entity's information systems and the harm that could be caused if that information were accessed or used by threat actors through a cybersecurity breach.[906] However, the Commission seeks comment on this topic, particularly if certain proposed Covered Entities should be Non-Covered Entities with attendant reduced requirements.[907]

f. Administration and Oversight of Cybersecurity Policies and Procedures of Covered Entities

The Commission considered various alternative requirements with respect to administration and oversight of Covered Entities' cybersecurity policies and procedures, such as requiring them to designate a CISO (or another individual that serves in a similar capacity) or

---

905 For additional detail on the importance of each of the proposed Covered Entity's role in the U.S. securities markets, *see* section I.A.2. of this release (discussing critical operations of each Market Entity). *See also* section II.A.1. of this release (discussing why it would not be appropriate to exclude small transfer agents and certain small broker-dealers from the definition of Covered Entity).

906 *See* section II.A.1. of this release.

907 *See* section II.A.10. of this release.

requiring the boards of directors (to the extent applicable), to oversee directly a Covered Entity's cybersecurity policies and procedures. There is a broad spectrum of potential approaches to this alternative, ranging from the largely nominal (*e.g.*, requiring Covered Entities simply to designate someone to be a CISO) to the stringent (*e.g.*, requiring a highly-qualified CISO to attest to the effectiveness of the Covered Entities' policies).

Stringent requirements, such as requiring an attestation from a highly qualified CISO as to the effectiveness of a Covered Entity's cybersecurity practices in specific enumerated areas, could be quite effective. Expert practitioners in cybersecurity are in high demand and command high salaries.[908] Thus, such an approach would impose substantial ongoing costs on Covered Entities who do not already have appropriately qualified individuals on staff. This burden would be disproportionately borne by smaller Covered Entities, such as small Covered Broker-Dealers or small transfer agents, for whom keeping a dedicated CISO on staff would be cost prohibitive. Allowing Covered Entities to employ part-time CISOs would mitigate this cost burden, but such requirements would likely create a *de facto* audit regime. Such an audit regime would certainly be more effective if explicitly designed to function as such.[909]

2. Alternatives to the Requirements of Proposed Form SCIR and Related Notification and Disclosure Requirements of Proposed Rule 10

a. Public Disclosure of Part I of Proposed Form SCIR

The Commission considered requiring the public disclosure of Part I of proposed Form SCIR. Making Part I of proposed Form SCIR filings public would increase the knowledge of a

---

908 A recent survey reports CISO median total compensation of $668,903 for CISOs at companies with revenues of $5 billion or less. *See* Matt Aiello and Scott Thompson, *2020 North American Chief Information Security Officer (CISO) Compensation Survey* (2020), *available at* https://www.heidrick.com/-/media/heidrickcom/publications-and-reports/2020-north-american-chief-information-security-officer-ciso-compensation-survey.pdf.

909 In designing an effective audit regime, aligning incentives of auditors to provide credible assessments is a central concern. In the context of audit regimes, barriers to entry and the reputation motives of auditing firms helps align incentives. It would be considerably more difficult to obtain similar incentive alignment with itinerant part-time CISOs. *See* section IV.F.1.e. of this release (describing the audit regime alternative).

Covered Entity's customer, counterparties, members, registrants, or users about significant cybersecurity incidents impacting the Covered Entity and thus improve their ability to draw inferences about a Covered Entity's level of cybersecurity preparations. At the same time, doing so could assist would-be threat actors, who may gain additional insight into the vulnerabilities of a Covered Entity's system. As discussed above, releasing too much detail about a significant cybersecurity incident could further compromise cybersecurity of the victim, especially in the short term.[910] Given these risks, requiring public disclosure of Part I of proposed Form SCIR filings would likely have the effect of incentivizing Covered Entities to significantly reduce the detail provided in these filings. As a result, the information set of customers, counterparties, members, registrants, users, and would-be attackers would remain largely unchanged (vis-à-vis the proposal), while the ability of the Commission to facilitate information sharing and to coordinate responses aimed at reducing overall risks to the financial system would be diminished.

b. Modify the Standard Identifier Requirements for Proposed Form SCIR

In addition to proposing to require Covered Entities to identify themselves on Parts I and II of proposed Form SCIR with CIK numbers, the proposed rule requests that Covered Entities with a UIC—such as an LEI—include that identifier, if available, on both parts of proposed Form SCIR. Those Covered Entities that do not have a UIC may file either part of proposed Form SCIR without a UIC; they are not required to obtain a UIC prior to filing proposed Form SCIR.

The Commission considered modifying the requirement that Covered Entities identify themselves on proposed Form SCIR with CIK numbers and UICs (if they have UICs). For example, the Commission could eliminate the requirement that Covered Entities identify

---

910 *See* section IV.B. of this release.

themselves on the forms with a standard identifier, or the Commission could allow Covered Entities to select a different standard identifier (or identifiers) other than CIK numbers or UICs (if available). Alternatively, the Commission could require the use of only one proposed standard identifier—either CIK numbers, UICs (which would require Covered Entities to obtain a UIC—such as an LEI—if they do not have one),[911] or some other standard identifier. While CIK numbers are necessary to file in EDGAR and, as discussed earlier, the Commission anticipates that significant benefits would flow from requiring Parts I and II of proposed Form SCIR to be filed centrally in EDGAR using a structured data language. Accordingly, the Commission's proposal would require Covered Entities to identify themselves on the forms with CIK numbers. One limitation of CIK numbers, however, is that they are a Commission-specific identifier, which limits their utility for aggregating, analyzing, and comparing financial market data involving market participants that are not Commission registrants and EDGAR filers.

While the proposed rule does not require the inclusion of UICs on proposed Form SCIR for those Covered Entities that do not have a UIC, the Commission notes that the use of UICs would be beneficial because the LEI, as a Commission-approved UIC, is a low-cost, globally-utilized financial institution identifier that is available even to firms that are not EDGAR filers or Commission registrants. For that reason, the Commission considered proposing to require that every Covered Entity that would need to file Part I or II of proposed Form SCIR to identify themselves with a UIC. There is benefit to including a UIC identifier on proposed Form SCIR. Among the alternative entity identifier policy choices considered, requiring Covered Entities to identify themselves on Parts I and II of proposed Form SCIR with a UIC is superior to other

---

[911] Further, the Commission recognizes that some Covered Entities may not have LEIs, which means that those Covered Entities would have to register with a Local Operating Unit ("LOU") of the Global LEI System and pay fees initially and annually to obtain and renew the LEI. *See* LEIROC, *How To Obtain an LEI*, *available at* https://www.leiroc.org/lei/how.htm. A list of LOUs accredited by GLEIF can be found at https://www.gleif.org/en/about-lei/get-an-lei-find-lei-issuing-organizations. Currently, U.S. entities may obtain an LEI for a one-time fee of $65 and an annual renewal fee of $50. *See* Bloomberg Finance L.P., *Fees, Payments & Taxes* (2022), *available at* https://lei.bloomberg.com/docs/faq#what-fees-are-involved.

alternatives, such as not requiring an entity identifier on proposed Form SCIR or requiring only CIK numbers. Specifically, the mandatory inclusion of a UIC on (Parts I and II of) proposed Form SCIR could allow for greater inter-governmental and international coordination of responses to cybersecurity incidents affecting financial institutions globally because the LEI is a globally-utilized digital identifier that is not specific to the Commission. Other regulatory entities and bodies, including the CFTC, Alberta Securities Commission (Canada), European Markets and Securities Authority, and Monetary Authority of Singapore, require the use of an LEI.[912] Another benefit of the LEI is that the legal entity's identity is verified by a third party upon issuance of the LEI and upon annual renewal of the LEI. Additionally, LEIs contain "Level 2" information about the linkages between the entities being identified and their various parents and subsidiaries, which is particularly beneficial considering that some financial firms and Commission registrants have complex, interlocking relationships with affiliates and subsidiaries that can be different types of Commission-regulated firms.

A UIC requirement for Parts I and II of proposed Form SCIR would not impose additional costs on those Covered Entities that already have an LEI. For those Covered Entities that do not have an LEI, they would need to obtain one before filing either part of proposed Form SCIR. An LEI can be obtained for a $65 initial cost and a $50 per year renewal cost.[913] There also are administrative costs associated with filling out the paperwork to obtain the LEI as well as to process payments for the initial issuance of an LEI and its maintenance. The Commission expects that this cost would be small relative to the benefit that could be reaped if a significant cybersecurity incident were to occur that impacted financial institutions across multiple domestic and international jurisdictions.

---

[912] In addition, the FSB has stated that "[t]he use of the LEI in regulatory reporting can significantly improve the ability of the public sector to understand and identify the build-up of risk across multiple jurisdictions and across complex global financial processes." FSB Peer Review Report.

After considering the benefits and costs of requiring the LEI as an identifier for all Covered Entities via a UIC requirement, the Commission is proposing to require Covered Entities to identify themselves with a UIC on proposed Form SCIR only if they already have a UIC so as to minimize the burden on Covered Entities and because multiple other Commission disclosure forms also only require registrants to identify themselves with UICs if they already have UICs.[914] In conclusion, requiring Covered Entities to identify themselves on both parts of proposed Form SCIR with a CIK and with a UIC (*i.e.*, the LEI) if they already have a UIC is consistent with the existing regulatory framework

Although CIK numbers and UICs (such as in the form of LEIs) are the primary two entity standard identifiers used in Commission regulations, the Commission could instead propose to require Covered Entities to identify themselves with an alternative entity identifier other than CIK numbers and UICs for the proposed rule. For the reasons stated above, there are benefits from the use of CIK numbers (*i.e.*, CIK numbers enable EDGAR filing, which facilitates aggregation and analysis of the information) and LEIs (*i.e.*, the LEI is an affordable, international standard identifier that facilitates information sharing). Accordingly, the Commission decided against proposing to require the use of another standard entity identifier for the purposes of this proposal.

c. Require Only One Location for the Public Disclosures

Rather than requiring Covered Entities to publicly disclose their cybersecurity risks and significant cybersecurity incidents during the current or previous calendar year both on their websites and also file that information centrally on Part II of proposed Form SCIR in EDGAR, the Commission considered requiring that Covered Entities provide the public disclosures on their websites only.

---

[914] Covered Entities that do not have an LEI may obtain one if they so choose.

Requiring Covered Entities to place the cybersecurity disclosures only on their websites could provide modest, incremental reductions in the burdens associated with providing those disclosures both on Covered Entity websites and through filing Part II of proposed Form SCIR with the Commission. Additionally, the websites of Covered Entities might be the natural place for their customers, counterparties, members, registrants, or users to look for information about the Covered Entity. Alternatively, requiring Covered Entities to place their cybersecurity disclosures (Part II of Form SCIR) only in EDGAR in a structured data language also could provide modest, incremental reductions in the burdens associated with placing those disclosures on their websites.

Accordingly, the Commission is proposing to require Covered Entities to provide the information both on their websites and in EDGAR on Part II of proposed Form SCIR.[915] Publication on Covered Entity websites is advantageous because that is where many Covered Entities' customers, counterparties, members, registrants, or users will look for information about their financial intermediaries. Centralized filing of structured public disclosures of cybersecurity risks and significant cybersecurity incidents during the current or previous calendar year in EDGAR by Covered Entities would enable customers, counterparties, members, registrants, and users, as well as financial analysts—and even the Covered Entities themselves—to more efficiently discern broad trends in cybersecurity risks and incidents, which would enable Covered Entities and other market participants to more efficiently determine if they need to modify, change, or upgrade their cybersecurity defense measures in light of those trends. Accordingly, the Commission is proposing to require Covered Entities to publish the required cybersecurity disclosures on their websites and provide the information in Part II of proposed Form SCIR, which would be filed in EDGAR using a custom XML.

---

[915] The Commission is seeking comment on this topic. *See* section II.B.3.c. of this release.

d. Modify the Location of the EDGAR-Filed Public Cybersecurity Disclosures for Some Covered Entities

Rather than requiring Covered Entities to provide the public cybersecurity disclosures in EDGAR using Part II of proposed Form SCIR, the Commission considered requiring Covered Entities that currently are required to file forms in EDGAR to provide the disclosures in structured attachments to existing EDGAR-filed forms. Currently, only SBS Entities and transfer agents are required to file EDGAR forms. SBSDs and MSBSPs must file in EDGAR registration applications on Form SBSE, SBSE-A, or SBSE-BD, amendments to those Forms if the information in them is or has become inaccurate, and certifications on Form SBSE-C.[916] As discussed above, Commission regulations require SBSDRs to file Form SDR in EDGAR but the Commission temporarily relieved SBSDRs of the EDGAR-filing requirement. Transfer agents file Forms TA-1, TA-2, and TA-W in EDGAR in a custom XML.[917] The Commission considered permitting those types of Covered Entities that are not currently subject to an EDGAR-filing requirement to file the cybersecurity disclosures only on their individual firm websites (without needing to also file the disclosures in EDGAR). Therefore, rather than requiring all Covered Entities to file the cybersecurity disclosures using Part II of proposed Form SCIR, the Commission could require Covered Entities that are SBS Entities or transfer agents to provide the same information as structured attachments to Form SBSE (for SBS Entities) and Form TA-1 (for transfer agents). Likewise, the Commission could require SBSDRs to file the cybersecurity disclosures as attachments to Form SDR once the Commission temporary relief from the EDGAR-filing requirement expires.

Requiring all Covered Entities to provide the disclosures on a single, uniform form would likely be simpler (because the information would be in one location)—and thereby more

---

[916] *See* Instruction A.2 to Form SBSE, Instruction A.2 to Form SBSE-A, Instruction A.3 to Form SBSE-BD, and Instruction A.2 to Form SBSE-C.

[917] *See* Commission, Electronic Filing of Transfer Agent Forms (Nov. 14, 2007), *available at* https://www.sec.gov/info/edgar/ednews/ta-filing.htm.

efficient—for the Commission, Covered Entities, and others who might seek the information in the cybersecurity disclosures (including Covered Entities' users, members, customers, or counterparties) than putting the cybersecurity disclosures in attachments on disparate forms and (for those firms not subject to EDGAR-filing requirements) on individual Covered Entity websites.

e. Modify the Structured Data Requirement for the Public Cybersecurity Disclosures

Rather than requiring Covered Entities to file Part II of proposed Form SCIR in EDGAR using a custom XML, the Commission could either eliminate the structured data language requirement for some or all Covered Entities or require the use of a different structured data language, such as Inline XBRL.[918] For example, the Commission could eliminate the requirement that Covered Entities file Part II of proposed Form SCIR in a custom XML or in any structured data language. By eliminating the structured data requirement, the Commission would allow Covered Entities to submit the new cybersecurity disclosures in unstructured HTML or ASCII, thereby avoiding the need to put the information for Part II of proposed Form SCIR into a fillable web form that EDGAR would use to generate the custom XML filing, or instead file Part II of proposed Form SCIR directly in custom XML using the XML schema for proposed Form SCIR, as published on the Commission's website.

Another option is that the Commission could remove the structured data filing requirement for some subset of Covered Entities. For example, the Commission could instead require only certain types of Covered Entities, such as national securities exchanges or SBS Entities, to file Part II of proposed Form SCIR in a custom XML. Alternatively, the Commission could require the use of a structured data language only for those Covered Entities that exceeded

---

[918] XBRL is a structured data language that is specifically designed to handle business-related information, including financial information, entity descriptions, corporate actions, ledgers and sub-ledgers, and other summary and ledger-level information. By comparison, Inline XBRL is a structured data language that embeds XBRL data directly into an HTML document, enabling a single document to provide both human-readable and structured machine-readable data.

some threshold, be it assets or trading volumes, depending on the type of Covered Entity in question. Eliminating the requirement that Part II of proposed Form SCIR be filed in a structured data language, however, would reduce the benefits of the proposed rule because the use of a structured data language would make the information contained in Part II of proposed Form SCIR easier and more efficient for Commission staff—as well as the Covered Entity's customers, counterparties, members, registrants, or users—to assemble, review, and analyze. Financial analysts at third-party information providers also could use the public disclosures to produce analyses and reports that market participants may find useful.

The Commission could require Covered Entities to file Part II of proposed Form SCIR in Inline XBRL rather than in custom XML on the grounds that Inline XBRL is an internationally-recognized freely available industry standard for reporting business-related information and a data language that allows EDGAR filers to prepare single documents that are both human-readable and machine-readable, particularly in connection with forms containing publicly-available registrant financial statements. The Commission believes that the use of a form-specific XML would be appropriate here given the relative simplicity of Part II of proposed Form SCIR disclosures and the ability for EDGAR to provide fillable web forms for entities to comply with their custom XML requirements, leading to a lower burden of compliance for Covered Entities without Inline XBRL experience.

3. General Request for Comment

The Commission requests comment on the benefits and costs associated the alternatives outlined above.

V. PAPERWORK REDUCTION ACT ANALYSIS

Certain provisions of the proposed rule, form, and rule amendments in this release would contain a new "collection of information" within the meaning of the Paperwork Reduction Act of

1995 ("PRA").[919] The Commission is submitting the proposed rule amendments and proposed new rules to the Office of Management and Budget ("OMB") for review and approval in accordance with the PRA and its implementing regulations.[920] An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number.[921] The titles for the collections of information are:

(1) Rule 10;

(2) Form SCIR;

(3) Rule 17a-4 – Records to be preserved by certain exchange members, brokers and dealers (OMB control number 3235-0279);

(4) Rule 17ad-7 – Record retention (OMB control number 3235-0291);

(5) Rule 18a-6 – Records to be preserved by certain security-based swap dealers and major security-based swap participants (OMB control number 3235-0751); and

(6) Rule 3a71-6 – Substituted Compliance for Foreign Security-Based Swap Entities (OMB control number 3235-0715).

The burden estimates contained in this section do not include any other possible costs or economic effects beyond the burdens required to be calculated for PRA purposes.

A. Summary of Collections of Information

1. Proposed Rule 10

Proposed Rule 10 would require all Market Entities (Covered Entities and non-Covered Entities) to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks.[922] All Market Entities also, at least annually, would

---

919 *See* 44 U.S.C. 3501 *et seq.*

920 *See* 44 U.S.C. 3507; 5 CFR 1320.11.

921 *See* 5 CFR 1320.11(l).

922 *See* paragraphs (b) through (d) of proposed Rule 10 (setting forth the requirements for Market Entities that meet the definition of "covered entity"); paragraph (e)(1) of proposed Rule 10. *See also* Sections II.B.1 and II.C. of this release (discussing these proposed requirements in more detail).

be required to review and assess the design and effectiveness of their cybersecurity policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review.[923] They also would be required to prepare a report (in the case of Covered Entities) and a record (in the case of non-Covered Entities) with respect to the annual review.[924] Finally, all Market Entities would need to give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring.[925]

Market Entities that meet the definition of "covered entity" would be subject to certain additional requirements under proposed Rule 10.[926] First, their cybersecurity risk management policies and procedures would need to include the following elements:

- Periodic assessments of cybersecurity risks associated with the Covered Entity's information systems and written documentation of the risk assessments;
- Controls designed to minimize user-related risks and prevent unauthorized access to the Covered Entity's information systems;
- Measures designed to monitor the Covered Entity's information systems and protect the Covered Entity's information from unauthorized access or use, and oversight of service providers that receive, maintain, or process information, or are otherwise permitted to access the Covered Entity's information systems;
- Measures to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the Covered Entity's information systems; and

---

923 *See* paragraph (b)(2) of proposed Rule 10; paragraph (e)(1) of proposed Rule 10. *See also* Sections II.B.1.f. and II.C. of this release (discussing these proposed requirements in more detail).

924 *See* paragraph (b)(2) of proposed Rule 10; paragraph (e)(1) of proposed Rule 10. *See also* Sections II.B.1.f. and II.C. of this release (discussing these proposed requirements in more detail).

925 *See* paragraph (c)(1) of proposed Rule 10; paragraph (e)(2) of proposed Rule 10. *See also* sections II.B.2.a. and II.C. of this release (discussing these proposed requirements in more detail).

926 *See* paragraph (b) through (d) of proposed Rule 10 (setting forth the requirements for Market Entities that meet the definition of "covered entity"); paragraph (e) of proposed Rule 10 (setting forth the requirements for Market Entities that do not meet the definition of "covered entity").

- Measures to detect, respond to, and recover from a cybersecurity incident and written documentation of any cybersecurity incident and the response to and recovery from the incident.[927]

Second, Covered Entities—in addition to providing the Commission with immediate written electronic notice of a significant cybersecurity incident—would need to report and update information about the significant cybersecurity incident by filing Part I of proposed Form SCIR with the Commission through the EDGAR system.[928] The form would elicit information about the significant cybersecurity incident and the Covered Entity's efforts to respond to, and recover from, the incident.

Third, Covered Entities would need to publicly disclose summary descriptions of their cybersecurity risks and the significant cybersecurity incidents they experienced during the current or previous calendar year on Part II of proposed Form SCIR.[929] The form would need to be filed with the Commission through the EDGAR system and posted on the Covered Entity's business Internet website and, in the case of Covered Entities that are carrying or introducing broker-dealers, provided to customers at account opening and annually thereafter.

Covered Entities and Non-Covered Entities would need to preserve certain records relating to the requirements of proposed Rule 10 in accordance with amended or existing recordkeeping requirements applicable to them or, in the case of exempt clearing agencies, pursuant to conditions in relevant exemption orders.[930]

2. Form SCIR

---

927 *See* sections II.B.1.a. through II.B.1.e. of this release (discussing these proposed requirements in more detail). In the case of non-Covered Entities, as discussed in more detail below in Section II.C. of this release, the design of the cybersecurity risk management policies and procedures would need to take into account the size, business, and operations of the broker-dealer. *See* paragraph (e) of proposed Rule 10.

928 *See* sections II.B.2. and II.B.4. of this release (discussing these proposed requirements in more detail).

929 *See* sections II.B.3. and II.B.4.of this release (discussing these proposed requirements in more detail).

930 *See* sections II.B.5. and II.C. of this release (discussing these proposed requirements in more detail).

Proposed Rule 10 would require Covered Entities to: (1) report and update information about a significant cybersecurity incident;[931] and (2) publicly disclose summary descriptions of their cybersecurity risks and the significant cybersecurity incidents they experienced during the current or previous calendar year.[932] Parts I and II of proposed Form SCIR would be used by Covered Entities, respectively, to report and update information about a significant cybersecurity incident and publicly disclose summary descriptions of their cybersecurity risks and the significant cybersecurity incidents they experienced during the current or previous calendar year.

3. Rules 17a-4, 17ad-7, 18a-6 and Clearing Agency Exemption Orders

Rules 17a-4, 17ad-7, and 18a-6—which apply to broker-dealers, transfer agents, and SBS Entities, respectively—would be amended to establish preservation and maintenance requirements for the written policies and procedures, annual reports, Parts I and II of proposed Form SCIR, and records required to be made pursuant to proposed Rule 10 (*i.e.*, the Rule 10 Records).[933] The proposed amendments would specify that the Rule 10 Records must be retained for three years. In the case of the written policies and procedures to address cybersecurity risks, the record would need to be maintained until three years after the termination of the use of the policies and procedures. In addition, orders exempting certain clearing agencies from registering with the Commission would be amended to establish preservation and maintenance requirements for the Rule 10 Records that would apply to the exempt clearing agencies subject to those orders.[934] The amendments to the orders would provide that the records need to be retained for

---

931 *See* sections II.B.2. and II.B.4. of this release (discussing these proposed requirements in more detail).

932 *See* sections II.B.3. and II.B.4.of this release (discussing these proposed requirements in more detail).

933 *See* sections II.B.5. and II.C. of this release (discussing these proposed amendments in more detail). Rule 17a-4 sets forth record preservation and maintenance requirements for broker-dealers, Rule 17ad-7 sets forth record preservation and maintenance requirements for transfer agents, and Rule 18a-6 sets forth record preservation and maintenance requirements for SBS Entities.

934 *See* section II.B.5. of this release (discussing these proposed amendments in more detail).

five years (consistent with Rules 13n-7 and 17a-1).[935] In the case of the written policies and procedures to address cybersecurity risks, the record would need to be maintained until five years after the termination of the use of the policies and procedures.

4. Substituted Compliance (Rule 3a71-6)

Paragraph (d)(1) of Rule 3a71-6 would be amended to add proposed Rule 10 and Form SCIR to the list of Commission requirements eligible for a substituted compliance determination.[936] If adopted, this amendment together with existing paragraph (d)(6) of Rule 3a71-6 would permit eligible SBS Entities to file an application requesting that the Commission make a determination that compliance with specified requirements under a foreign regulatory system may satisfy the requirements of proposed Rule 10, Form SCIR, and the related record preservation requirements. As provided by Exchange Act Rule 0-13,[937] which the Commission adopted in 2014,[938] applications for substituted compliance determinations must be accompanied by supporting documentation necessary for the Commission to make the determination, including information regarding applicable requirements established by the foreign financial regulatory authority or authorities, as well as the methods used by the foreign financial regulatory authority or authorities to monitor and enforce compliance; applications should cite to and discuss applicable precedent.[939]

B. Proposed Use of Information

---

935 For the reasons discussed in section II.B.5.a. of this release, the proposal would not amend Rules 13n-7 or 17a-1. As explained in that section of the release, the existing requirements of Rule 13n-7 (which applies to SBSDRs) and Rule 17a-1 (which applies to registered clearing agencies, the MSRB, national securities associations, and national securities exchanges) will require these Market Entities to retain the Rule 10 Records for five years and, in the case of the written policies and procedures, for five years after the termination of the use of the policies and procedures.

936 *See* section II.D. of this release (discussing these proposed amendments in more detail).

937 17 CFR 240.0-13.

938 *See* SBS Entity Definitions Adopting Release, 79 FR at 47357-59.

939 *See* 17 CFR 240.0-13(e). In adopting Rule 0-13, the Commission noted that because Rule 0-13 was a procedural rule that did not provide any substituted compliance rights, "collections of information arising from substituted compliance requests, including associated control numbers, [would] be addressed in connection with any applicable substantive rulemakings that provide for substituted compliance." *See* SBS Entity Definitions Adopting Release, 79 FR at 47366 n.778.

The proposed requirements to have written policies and procedures to address cybersecurity risks, to document risk assessments and significant cybersecurity incidents, to create a report or record of the annual review of the policies and procedures, to provide immediate notification and subsequent reporting of significant cybersecurity incidents, to publicly disclose summary descriptions of cybersecurity risks and significant cybersecurity incidents, and to preserve the written policies and procedures, reports, and records would constitute collection of information requirements under the PRA. Collectively, these collections of information are designed to address cybersecurity risk and the threat it poses to Market Entities and the U.S. securities markets.

Market Entities would use the written policies and procedures, the records required to be made pursuant to those policies and procedures, and the report or record of the annual review of the policies and procedures to address the specific cybersecurity risks to which they are exposed. The Commission could use the written policies and procedures, reports, and records to review Market Entities' compliance with proposed Rule 10.

Market Entities would use the immediate written electronic notifications to notify the Commission (and, in some cases, other regulators) about significant cybersecurity incidents they experience pursuant to proposed Rule 10. The Commission could use the immediate written electronic notification to promptly begin to assess the situation by, for example, when warranted, assessing the Market Entity's operating status and engaging in discussions with the Market Entity to understand better what steps it is taking to protect its customers, counterparties, members, registrants, or users.

Covered Entities would use Part I of proposed Form SCIR to report to the Commission (and, in some cases, other regulators) significant cybersecurity incidents they experienced pursuant to proposed Rule 10. The Commission could use the reports of significant cybersecurity incidents filed using Part I of proposed Form SCIR to understand better the nature and extent of a particular significant cybersecurity incident and the efficacy of the Covered

Entity's response to mitigate the disruption and harm caused by the incident. The Commission staff could use the reports to focus on the Covered Entity's operating status and to facilitate their outreach to, and discussions with, personnel at the Covered Entity who are addressing the significant cybersecurity incident. In addition, the reporting would provide the staff with a view into the Covered Entity's understanding of the scope and impact of the significant cybersecurity incident. All of this information would be used by the Commission and its staff in assessing the significant cybersecurity incident impacting the Covered Entity. Further, the Commission would be use the database of reports to assess the potential cybersecurity risks affecting U.S. securities markets more broadly. This information could be used to address future significant cybersecurity incidents. For example, these reports could assist the Commission in identifying patterns and trends across Covered Entities, including widespread cybersecurity incidents affecting multiple Covered Entities at the same time. Further, the reports could be used to evaluate the effectiveness of various approaches to respond to and recover from a significant cybersecurity incident.

Covered Entities would use Part II of proposed Form SCIR to publicly disclose summary descriptions of their cybersecurity risks and the significant cybersecurity incidents they experienced during the current or previous calendar year pursuant to proposed Rule 10. These disclosures would be used to provide greater transparency to customers, counterparties, registrants, or members of the Covered Entity, or to users of its services, about the Covered Entity's cybersecurity risk profile. This information could be used by these persons to manage their own cybersecurity risk and, to the extent they have choice, select a Covered Entity with whom to transact or otherwise conduct business. In addition, because the reports would be filed through EDGAR, Covered Entities' customers, counterparties, members, registrants, or users would be able to run search queries to compare the disclosures of multiple Covered Entities. This would make it easier for Commission staff and others to assess the cybersecurity risk

profiles of different types of Covered Entities and could facilitate trend analysis by members of the public of significant cybersecurity incidents.

Under the proposed amendment to Rule 3a71-6, the Commission would use the information collected to evaluate requests for substituted compliance with respect to proposed Rule 10, Form SCIR, and the related record preservation requirements applicable to SBS Entities. Consistent with Exchange Act Rule 0-13(h),[940] the Commission would publish in the Federal Register a notice that a complete application had been submitted, and provide the public the opportunity to submit to the Commission any information that relates to the Commission action requested in the application, subject to appropriate requests for confidential treatment being submitted pursuant to any applicable provisions governing confidentiality under the Exchange Act.[941]

C. Respondents

The following table summarizes the estimated number of respondents that would be subject to the proposed Rule 10, Form SCIR, and recordkeeping burdens.

Type of Registrant	Number
Covered Broker-Dealers	1,541
Non-Covered Broker-Dealers	1,969
Clearing agencies and exempt clearing agencies	16
MSRB	1
National securities exchanges	24
National securities associations	1
SBS Entities	50
SBSDRs	3
Transfer agents	353
Total Covered Entities	***1,989***
Total Non-Covered Broker-Dealers	***1,969***
Total Respondents	***3,958***

The respondents subject to these collection of information requirements include the following:

---

940 17 CFR 240.0-13(h).

941 *See* section V.F of this release.

1. Broker-Dealers

Each broker-dealer registered with the Commission would be subject to proposed Rule 10 as either a Covered Entity or a Non-Covered Broker-Dealer. As of September 30, 2022, there were 3,510 broker-dealers registered with the Commission.[942] The Commission estimates that 1,541 of these broker-dealers would be Covered Entities under the proposed rule because they fit within one or more of the following categories: carrying broker-dealer; broker-dealer that introduces customer accounts to a carrying broker-dealer on a fully disclosed basis; broker-dealer with regulatory capital equal to or exceeding $50 million; broker-dealer with total assets equal to or exceeding $1 billion; broker-dealer that operates as a market maker under the securities laws; or a broker-dealer that operates as an ATS.[943] The Commission estimates that 1,969 broker-dealers (*i.e.*, the remaining broker-dealers registered with /the Commission) would be Non-Covered Broker-Dealers for purposes of the rules.

2. Clearing Agencies

With regard to clearing agencies, respondents under these rules are: (1) nine registered clearing agencies;[944] and (2) five exempt clearing agencies.[945] The Commission estimates for purposes of the PRA that two additional entities may seek to register as a clearing agency in the next three years, and so for purposes of this proposal the Commission has assumed sixteen total clearing agency and exempt clearing agency respondents.

3. The MSRB

---

942 This estimate is derived from broker-dealer FOCUS filings and ATS Form ATS-R quarterly reports as of September 30, 2022.

943 *Id*.

944 The registered and active clearing agencies are: (1) DTC; (2) FICC; (3) NSCC; (4) ICC; (5) ICEEU; (6) the Options Clearing Corp.; and (7) LCH SA. The clearing agencies that are registered with the Commission but conduct no clearance or settlement operations are: (1) BSECC; and (2) SCCP.

945 The exempt clearing agencies that provide matching services are: (1) DTCC ITP Matching U.S. LLC; (2) Bloomberg STP LLC; (3) SS&C Technologies, Inc.; (4) Euroclear Bank SA/NV; and (5) Clearstream Banking, S.A.

The sole respondent to the proposed collection of information for the MSRB is the MSRB itself.

4. National Securities Exchanges and National Securities Associations

The respondents to the proposed collections of information for national securities exchanges and national securities associations would be the 24 national securities exchanges currently registered with the Commission under section 6 of the Exchange Act,[946] and the one national securities association currently registered with the Commission under section 15A of the Exchange Act.[947]

5. SBS Entities

As of January 4, 2023, 50 SBSDs have registered with the Commission, while no MSBSPs have registered with the Commission.[948] Of the 50 SBSDs that have registered with the Commission, 7 entities are also broker-dealers.[949]

Requests for a substituted compliance determination under Rule 3a71-6 with respect to the proposed Rule 10, Form SCIR, and the related record preservation requirements may be filed by foreign financial authorities, or by non-U.S. SBSDs or MSBSPs. The Commission had previously estimated that there may be approximately 22 non-U.S. entities that may potentially

---

946 *See* 15 U.S.C. 78f. The national securities exchanges registered with the Commission are: (1) BOX Options Exchange LLC; (2) Cboe BZX Exchange, Inc.; (3) Cboe BYX Exchange, Inc.; (4) Cboe C2 Exchange, Inc.; (5) Cboe EDGA Exchange, Inc.; (6) Cboe EDGX, Inc.; (7) Cboe Exchange, Inc.; (8) Investors Exchange Inc.; (9) Long-Term Stock Exchange, Inc.; (10) MEMX, LLC; (11) Miami International Securities Exchange LLC; (12) MIAX PEARL, LLC; (13) MIAX Emerald, LLC; (14) NASDAQ BX, Inc.; (15) NASDAQ GEMX, LLC; (16) NASDAQ ISE, LLC; (17) NASDAQ MRX, LLC; (18) NASDAQ PHLX LLC; (19) The NASDAQ Stock Market LLC; (20) New York Stock Exchange LLC; (21) NYSE MKT LLC; (22) NYSE Arca, Inc.; (23) NYSE Chicago Stock Exchange, Inc.; and (24) NYSE National, Inc.

947 *See* 15 U.S.C. 78o-3. The one national securities association registered with the Commission is FINRA.

948 *See List of Registered Security-Based Swap Dealers and Major Security-Based Swap Participants*, available at: https://www.sec.gov/tm/List-of-SBS-Dealers-and-Major-SBS-Participants.

949 A Covered Entity that is both a broker-dealer and an SBS Entity (which includes all seven of these broker-dealers) will have burdens with respect to the proposed rule, Form SCIR, and recordkeeping amendments as they apply to both its broker-dealer business and its security-based swap business. Therefore, such "dual-hatted" entities will be counted as both Covered Entities that are broker-dealers and as SBS Entities for purposes of the PRA.

register as SBSDs, out of approximately 50 total entities that may register as SBSDs.[950] Potentially all non-U.S. SBSDs, or some subset thereof, may seek to rely on a substituted compliance determination in connection with the proposed cybersecurity risk management requirements.[951] However, the Commission had expected that the great majority of substituted compliance applications would be submitted by foreign authorities[952] given their expertise in connection with the relevant substantive requirements, and in connection with their supervisory and enforcement oversight with regard to SBSDs and their activities.[953] The Commission expected that very few substituted compliance requests would come from SBS Entities.[954] For purposes of PRA assessments, the Commission estimated that three SBS Entities would submit such applications.[955] Although, as of January 4, 2023, 30 entities had identified themselves as a

---

950 *See* Proposed Rule Amendments and Guidance Addressing Cross-Border Application of Certain Security-Based Swap Requirements, Exchange Act Release No. 85823 (May 10, 2019), 84 FR 24206, 24253 (May 24, 2019). *See also* Security-Based Swap Transactions Connected With a Non-U.S. Person's Dealing Activity That Are Arranged, Negotiated, or Executed by Personnel Located in a U.S. Branch or Office or in a U.S. Branch or Office of an Agent; Security-Based Swap Dealer De Minimis Exception, Exchange Act Release No. 77104 (Feb. 10, 2016), 81 FR 8597, 8605 (Feb. 19, 2016) ("SBS Entity U.S. Activity Adopting Release"); Business Conduct Standards Adopting Release, 81 FR at 30090, 30105; SBS Entity Recordkeeping and Reporting Release, 84 FR at 68607-09; and Capital, Margin, and Segregation Requirements Adopting Release, 84 FR at 43960-61.

951 Consistent with prior estimates, the Commission further believes that there may up to five MSBSPs. *See Registration Process for Security-Based Swap Dealers and Major Security-Based Swap Participants,* Exchange Act Release No. 75611 (Aug. 5, 2015), 80 FR 48963, 48990 (Aug. 14, 2015) ("SBS Entity Registration Adopting Release"); *see also* SBS Entity Business Conduct Standards Adopting Release, 81 FR at 30089, 30099. It is possible that some subset of those entities will be non-U.S. MSBSPs that will seek to rely on substituted compliance in connection with proposed Rule 10, Form SCIR, and the related record preservation requirements.

952 *See* SBS Entity Risk Mitigation Adopting Release, 85 FR at 6389. *See also* SBS Entity Business Conduct Standards Adopting Release, 81 FR at 30097; SBS Entity Trade Acknowledgement and Verification Adopting Release, 81 FR at 39832.

953 *See* SBS Entity Risk Mitigation Adopting Release, 85 FR at 6384. *See also* SBS Entity Business Conduct Standards Adopting Release, 81 FR at 30090; SBS Entity Trade Acknowledgement and Verification Adopting Release, 81 FR at 39832.

954 *See* SBS Entity Risk Mitigation Adopting Release, 85 FR at 6389. *See also* SBS Entity Business Conduct Standards Adopting Release, 81 FR at 30097, n.1582 and accompanying text; SBS Entity Trade Acknowledgement and Verification Adopting Release, 81 FR at 39832.

955 *Id. See also* SBS Entity Recordkeeping and Reporting Adopting Release, 84 FR at 68609; Capital, Margin, and Segregation Requirements Adopting Release, 84 FR at 43967.

nonresident SBSD in their application for registration with the Commission,[956] the Commission has issued only one order in response to a request for substituted compliance from potential registrants.[957] The Commission continues to believe that its estimate that three such entities will submit applications remains appropriate for purposes of this PRA assessment because applicants may file additional requests.

6. SBSDRs

Two SBSDRs are currently registered with the Commission.[958] The Commission estimates for purposes of the PRA that one additional entity may seek to register as an SBSDR in the next three years, and so for purposes of this proposal the Commission has assumed three SBSDR respondents.

7. Transfer Agents

The proposed rule would apply to every transfer agent as defined in section 3(a)(25) of the Exchange Act that is registered or required to be registered with an appropriate regulatory agency as defined in section 3(a)(34)(B) of the Exchange Act. As of December 31, 2022, there were 353 transfer agents that were either registered with the Commission through Form TA-1 or registered with other appropriate regulatory agencies.

D. Total Initial and Annual Reporting Burdens

As stated above, each requirement to disclose information, offer to provide information, or adopt policies and procedures constitutes a collection of information requirement under the

---

956 No entity has registered as an MSBSP. *See* List of Registered Security-Based Swap Dealers and Major Security-Based Swap Participants, *available at*: https://www.sec.gov/tm/List-of-SBS-Dealers-and-Major-SBS-Participants (providing the list of registered SBSDs and MSBSPs that was updated as of January 4, 2023).

957 *See* Order Granting Conditional Substituted Compliance in Connection With Certain Requirements Applicable to Non-U.S. Security-Based Swap Dealers Subject to Regulation in the Swiss Confederation, Exchange Act Release No. 93284 (Oct. 8, 2021), 86 FR 57455 (Oct. 15, 2021) (File No. S7-07-21). The Commission's other substituted compliance orders have been in response to requests from foreign authorities; *see* https://www.sec.gov/tm/Jurisdiction-Specific-Apps-Orders-and-MOU.

958 The Commission approved the registration of two SBSDRs in 2021. The two registered SBSDRs are: (1) DTCC Data Repository (U.S.), LLC; and (2) ICE Trade Vault, LLC.

PRA. The Commission discusses below the collection of information burdens associated with the proposed rule and rule amendment.

1. Proposed Rule 10

The Commission has made certain estimates of the burdens associated with the policies and procedures and review and report of the review requirements of proposed Rule 10 applicable to Covered Entities solely for the purpose of this PRA analysis.[959] Table 1 below summarizes the initial and ongoing annual burden and cost estimates associated with the policies and procedures and review and report of the review requirements.

Table 1: Rule 10 PRA Estimates – Cybersecurity Policies and Procedures and Review and Report of the Review Requirements for Covered Entities

	Internal initial burden hours	Internal annual burden hours[1]	Wage rate[2]	Internal time costs	Annual external cost burden
PROPOSED RULE 10 ESTIMATES					
Adopting and implementing policies and procedures[3]	50 hours	21.67 hours[4]	$462 (blended rate for compliance attorney and assistant general counsel)	$10,011.54	$1,488[5]
Annual review of policies and procedures and report of review	0 hours	10 hours[6]	$462 (blended rate for compliance attorney and assistant general counsel)	$4,620	$1,984[7]
Total new annual burden per Covered Entity		31.67 hours		$14,631.54	$3,472
Number of Covered Entities		× 1,989		× 1,989	× 1,989
Total new annual aggregate burden		62,991.63 hours		$29,102,133.06	$6,905,808

Notes:

1. Includes initial burden estimates annualized over a 3-year period.

2. The Commission's estimates of the relevant wage rates are based on salary information for the securities industry compiled by Securities Industry and Financial Markets Association's Office Salaries in the Securities Industry 2013, as modified by Commission staff for 2022 ("SIFMA Wage Report"). The estimated figures are modified by firm size, employee benefits, overhead, and adjusted to account for the effects of inflation.

3. These estimates are based on an average. Some firms may have a lower burden in the case they will be evaluating exiting policies and procedures with respect to any cybersecurity risks and/or incidents, while other firms may be creating new cybersecurity policies and procedures altogether.

4. Includes initial burden estimates annualized over a three-year period, plus 5 ongoing annual burden hours. The estimate of 21.67 hours is based on the following calculation: ((50 initial hours /3) + 5 additional ongoing burden hours) = 21.67 hours.

---

959 These requirements are discussed in section II.B.1. of this release.

5. This estimated burden is based on the estimated wage rate of $496/hour, for 3 hours, for outside legal services.

The Commission's estimates of the relevant wage rates for external time costs, such as outside legal services, take into account staff experience, a variety of sources including general information websites, and adjustments for inflation.

6. The Commission estimates 10 additional ongoing burden hours.

7. This estimated burden is based on the estimated wage rate of $496/hour, for 4 hours, for outside legal services. *See* note 5 (regarding wage rates with respect to external cost estimates).

The Commission has made certain estimates of the burdens associated with the policies and procedures and review and record of the review requirements of proposed Rule 10 applicable to Non-Covered Broker-Dealers solely for the purpose of this PRA analysis.[960] Table 2 below summarizes the initial and ongoing annual burden and cost estimates associated with the proposed rule's policies and procedures and review and record of the review requirements for Non-Covered Broker-Dealers.

Table 2: Rule 10 PRA Estimates – Cybersecurity Policies and Procedures and Review and Record of the Review Requirements for Non-Covered Broker-Dealers

	Internal initial burden hours	Internal annual burden hours[1]	Wage rate[2]	Internal time costs	Annual external cost burden
PROPOSED RULE 10 ESTIMATES					
Adopting and implementing policies and procedures[3]	30 hours	15 hours[4]	$462 (blended rate for compliance attorney and assistant general counsel)	$6,930	$1,488[5]
Annual review of policies and procedures and record of the review	0 hours	6 hours[6]	$462 (blended rate for compliance attorney and assistant general counsel)	$2,772	$992[7]
Total new annual burden per Non-Covered Broker-Dealer		21 hours		$9,702	$2,480
Number of Non-Covered Broker-Dealers		× 1,969		× 1,969	× 1,969
Total new annual aggregate burden		41,349 hours		$19,103,238	$4,883,120

Notes:

1. Includes initial burden estimates annualized over a 3-year period.

2. The Commission's estimates of the relevant wage rates are based on salary information for the securities industry compiled by Securities Industry and Financial Markets Association's Office Salaries in the Securities Industry 2013, as modified by Commission staff for 2022 ("SIFMA Wage Report"). The estimated figures are modified by firm size, employee benefits, overhead, and adjusted to account for the effects of inflation.

3. These estimates are based on an average. Some firms may have a lower burden in the case they will be evaluating exiting policies and

960 These requirements are discussed in section II.C. of this release.

procedures with respect to any cybersecurity risks and/or incidents, while other firms may be creating new cybersecurity policies and procedures altogether.

4. Includes initial burden estimates annualized over a three-year period, plus 5 ongoing annual burden hours. The estimate of 15 hours is based on the following calculation: ((30 initial hours /3) + 5 additional ongoing burden hours) = 15 hours.

5. This estimated burden is based on the estimated wage rate of $496/hour, for 3 hours, for outside legal services.

The Commission's estimates of the relevant wage rates for external time costs, such as outside legal services, take into account staff experience, a variety of sources including general information websites, and adjustments for inflation.

6. The Commission estimates 6 additional ongoing burden hours.

7. This estimated burden is based on the estimated wage rate of $496/hour, for 2 hours, for outside legal services. *See* note 5 (regarding wage rates with respect to external cost estimates).

The Commission has made certain estimates of the burdens associated with the notification requirement of proposed Rule 10 applicable to Market Entities solely for the purpose of this PRA analysis.[961] Table 3 below summarizes the initial and ongoing annual burden and cost estimates associated with the proposed rule's notification requirements for Market Entities.

Table 3: Rule 10 PRA Estimates – Notification Requirements for Market Entities

	Internal initial burden hours	Internal annual burden hours		Wage rate	Internal time costs	Annual external cost burden
PROPOSED RULE 10 ESTIMATES						
Making a determination of significant cybersecurity incident and immediate notice to the Commission	5 hours	4.67 hours[1]	×	$353 (blended rate for assistant general counsel, compliance manager and systems analyst)	$1,648.51	$1,488[2]
Total new annual burden per Market Entity		4.67 hours			$1,648.51	$1,488
Number of Market Entities		× 3,958			× 3,958	× 3,958
Total new aggregate annual burden		18,483.86 hours			$6,524,802.58	$5,889,504

Notes:

1. Includes initial burden estimates annualized over a three-year period, plus 3 ongoing annual burden hours. The estimate of 4.67 hours is based on the following calculation: ((5 initial hours /3) + 3 additional ongoing burden hours) = 4.67 hours.

2. This estimated burden is based on the estimated wage rate of $496/hour, for 3 hours, for outside legal services.

The Commission's estimates of the relevant wage rates for external time costs, such as outside legal services, take into account staff experience, a variety of sources including general information websites, and adjustments for inflation.

The Commission has made certain estimates of the burdens associated with the requirement of proposed Rule 10 that Covered Broker-Dealers provide the disclosures that would need to made on Part II of proposed Form SCIR requirements to their customers solely for the

961 This requirement is discussed in section II.B.2.a. of this release.

purpose of this PRA analysis.[962] Table 4 below summarizes the initial and ongoing annual burden and cost estimates associated with the requirement of proposed Rule 10 that Covered Broker-Dealers provide the disclosures that would need to made on Part II of proposed Form SCIR requirements to their customers.

Table 4: Rule 10 PRA Estimates – Additional Disclosure Requirements for Broker-Dealers that are Covered Entities

	Internal initial burden hours	Internal annual burden hours		Wage rate	Internal time costs	Annual external cost burden
PROPOSED RULE 10 ESTIMATES						
Delivery of disclosures to new customers	6.68 hours[1]	6.68 hours	×	$69 (general clerk)	$460.92	$0
Annual delivery of disclosures to existing customers	44.58 hours[2]	44.58 hours	×	$69 (general clerk)	$3,076.02	$0
Total new annual burden per broker-dealer Covered Entity		51.26 hours			$3,536.94	
Number of broker-dealer Covered Entities		×1,541			×1,541	
Total new aggregate annual burden		78,991.66 hours			$5,450,424.54	

Notes:

1. The Commission estimates that a broker-dealer that is a Covered Entity will require no more than 0.02 hours to send the broker-dealer's required disclosures to each new customer, or an annual burden of 6.68 hours per broker-dealer. (0.02 hours per customer x 334 median number of new customers per broker-dealer based on FOCUS Schedule I data as of December 31, 2022 = approximately 6.68 hours per broker-dealer.) The Commission notes that the burden for preparing disclosures to customers is already incorporated into a separate burden estimate under other broker-dealer rules promulgated by the Commission (*e.g.*, 17 CFR 240.17a-3) and FINRA rules. The Commission expects that broker-dealers subject to this new disclosure requirement will make their delivery of disclosures to new customers as part of an email or mailing they already send to new customers; therefore, the Commission estimates that the additional burden will be adding a few pages to the email attachment or mailing.

2. The Commission estimates that, with a bulk mailing or email, a broker-dealer that is a Covered Entity will require no more than 0.02 hours to send the broker-dealer's required disclosures to each existing customer, or an annual burden of 44.58 hours per broker-dealer. (0.02 hours per customer x 2,229 median number of customers per broker-dealer based on FOCUS Schedule I data as of December 31, 2022 = approximately 44.58 hours per broker-dealer.) The Commission notes that the burden for preparing disclosures to customers is already incorporated into a separate burden estimate under other broker-dealer rules promulgated by the Commission (*e.g.*, 17 CFR 240.17a-3) and FINRA rules. The Commission expects that broker-dealers subject to this new disclosure requirement will make their annual delivery to existing customers as part of an email or mailing of an account statement they already send to customers; therefore, the Commission estimates that the additional burden will be adding a few pages to the email attachment or mailing.

2. Form SCIR

The Commission has made certain estimates of the burdens associated with filing the initial and amended Part I of Form SCIR under proposed Rule 10 applicable to Covered Entities

---

962 These requirements are discussed in section II.B.3.b. of this release.

solely for the purpose of this PRA analysis.[963] Table 5 below summarizes the initial and ongoing annual burden and cost estimates associated with filing proposed Form SCIR.

Table 5: Part I of Form SCIR PRA Estimates

	Internal initial burden hours	Internal annual burden hours		Wage rate	Internal time costs	Annual external cost burden
PROPOSED PART I OF FORM SCIR ESTIMATES						
Filling out initial Part I of Form SCIR	3 hours	1.5 hours[1]	×	$431 (blended rate for assistant general counsel and compliance manager)	$646.50	$496[2]
Filing an amended Part I of Form SCIR	1 hour	1 hour	×	$431 (blended rate for assistant general counsel and compliance manager)	$431	$496[3]
Total new annual burden per Covered Entity		2.5 hours			$1077.50	$992
Number of Covered Entities		× 1,989			× 1,989	× 1,989
Total new aggregate annual burden		4,972.5 hours			$2,143,147.5	$1,973,088

Notes:

1. Includes initial burden estimates annualized over a three-year period, plus 0.5 ongoing annual burden hours. The estimate of 1.5 hours is based on the following calculation: ((3 initial hours /3) + 0.5 additional ongoing burden hours) = 1.5 hours.

2. This estimated burden is based on the estimated wage rate of $496/hour, for 1 hour, for outside legal services.

The Commission's estimates of the relevant wage rates for external time costs, such as outside legal services, takes into account staff experience, a variety of sources including general information websites, and adjustments for inflation.

3. This estimated burden is based on the estimated wage rate of $496/hour, for 1 hour, for outside legal services.

The Commission has made certain estimates of the burdens associated with filing the Part II of Form SCIR under proposed Rule 10 applicable to Covered Entities solely for the purpose of this PRA analysis.[964] Table 6 below summarizes the initial and ongoing annual burden and cost estimates associated with the proposed rule's disclosure requirements for Covered Entities.

963 These requirements are discussed in sections II.B.2. and II.B.4. of this release.

964 These requirements are discussed in sections II.B.3. and II.B.4. of this release.

Table 6: Part II of Form SCIR PRA Estimates

	Internal initial burden hours	Internal annual burden hours		Wage rate	Internal time costs	Annual external cost burden
PROPOSED PART II OF FORM SCIR ESTIMATES						
Disclosure of significant cybersecurity incidents and cybersecurity risks on Part II of Form SCIR and posting form on website	5 hours	3.67 hours[1]	×	$375.33 per hour (blended rate for assistant general counsel, senior compliance examiner and compliance manager)[3]	$1,377.46	$1,488[2]
Total new annual burden per Covered Entity		3.67 hours			$1,377.46	$1,488
Number of Covered Entities		× 1,989			× 1,989	× 1,989
Total new aggregate annual burden		7,299.63 hours			$2,739,767.94	$2,959,632

Notes:

1. Includes initial burden estimates annualized over a three-year period, plus 2 ongoing annual burden hours. The estimate of 3 hours is based on the following calculation: ((5 initial hours /3) + 2 additional ongoing burden hours) = 3.67 hours.

2. This estimated burden is based on the estimated wage rate of $496/hour, for 3 hours, for outside legal services.

The Commission's estimates of the relevant wage rates for external time costs, such as outside legal services, take into account staff experience, a variety of sources including general information websites, and adjustments for inflation.

3. The $375.33 wage rate reflects current estimates from the SIFMA Wage Report of the blended hourly rate for an assistant general counsel ($518), senior compliance examiner ($264) and a compliance manager ($344). ($518 + $264 + $344) / 3 = $375.33.

In addition, the requirement to file Form SCIR in EDGAR using a form-specific XML may impose some compliance costs. Covered Entities that are not otherwise required to file in EDGAR—for example, clearing agencies, the MSRB, national securities associations, and national securities exchanges, as well as any broker-dealer Covered Entities that choose not to file Form X-17A-5 Part III or Form 17-H through the EDGAR system, would need to complete Form ID to obtain the EDGAR-system access codes that enable entities to file documents through the EDGAR system.[965] The Commission estimates that each filer that currently does not

[965] Form ID (OMB control number 3235-0328) must be completed and filed with the Commission by all individuals, companies, and other organizations who seek access to file electronically on EDGAR. Accordingly, a filer that does not already have access to EDGAR must submit a Form ID, along with the notarized signature of an authorized individual, to obtain an EDGAR identification number and access codes to file on EDGAR. The Commission currently estimates that Form ID would take 0.30 hours to prepare, resulting in an annual industry-wide burden of 17,199 hours. *See* Supporting Statement for the Paperwork Reduction Act Information Collection Submission for Form ID (Dec. 20 2021), *available at* https://www.reginfo.gov/public/do/PRAViewDocument?ref_nbr=202112-3235-003.

have access to EDGAR would incur an initial, one-time burden of 0.30 hours to complete and submit a Form ID.[966] Therefore, the Commission believes the one-time industrywide reporting burden associated with the proposed requirements to file on EDGAR is 4.8 hours for clearing agencies,[967] 0.30 hours for the MSRB,[968] 7.5 hours for national securities exchanges and associations;[969] 0.9 hours for SBSDRs;[970] and 242.4 hours for Covered Broker-Dealers not already filing their annual audits on EDGAR.[971] In addition, the requirement to file Form SCIR using custom XML (with which a Covered Entity would be able to comply by inputting its disclosures into a fillable web form), the Commission estimates each Covered Entity would incur an internal burden of 0.5 hours per filing.[972] Accordingly, the Commission estimates that Covered Entities will collectively have an ongoing burden of 994.5 hours[973] with respect to filing Form SCIR in custom XML.

3. Rules 17a-4, 17ad-7, 18a-6, and Clearing Agency Exemption Orders (and Existing Rules 13n-7 and 17a-1)

The Commission has made certain estimates of the burdens associated with the proposed record preservation requirements solely for the purpose of this PRA analysis.[974] Table 7 below summarizes the initial and ongoing annual burden and cost estimates associated with the additional recordkeeping requirements.

---

966 The Commission does not estimate a burden for SBS Entities since these firms have already filed Form ID so they can file Form SBSE on EDGAR. Similarly, the Commission does not estimate a burden for transfer agents since these firms already file their annual report on Form TA-2 on EDGAR.

967 0.30 hours x 16 clearing agencies = 4.8 hours.

968 0.30 hours x 1 MSRB = 0.30 hours.

969 0.30 hours x (24 national securities exchanges and 1 national securities association) = 7.5 hours.

970 0.30 hours x 3 SBSRs = 0.9 hours.

971 0.30 hours x 808 Covered Broker-Dealers not already filing on EDGAR = 242.4 hours.

972 This estimate would mirror the Commission's internal burden hour estimate for a proposed custom XML requirement for Schedules 13D and 13G. *See* Modernization of Beneficial Ownership Reporting Release.

973 1,989 Covered Entities x .5 hours = 994.5 hours.

974 These requirements are discussed in sections II.B.5.a. and II.C. of this release.

Table 7: PRA Estimates – Proposed Amendments to Rules 17a-4, 18a-6, and 17ad-7 and Clearing Agency Exemption Orders (and Existing Rules 17a-1 and 13n-7)[975]

	Internal Annual Hour Burden		Wage Rate	Internal Time Costs	Annual External Cost Burden
PROPOSED ESTIMATES FOR RECORDKEEPING BURDENS					
Retention of cybersecurity policies and procedures	1	×	$73.5 (blended rate for general clerk and compliance clerk)	$73.5	$0
Total burden per Covered Entity or Non-Covered Broker-Dealer	1			$73.5	$0
Total number of affected entities	× 3,918			× 3,918	$0
Sub-total burden	3,918 hours			$287,973	$0
Retention of written report documenting annual review	1	×	$73.5 (blended rate for general clerk and compliance clerk)	$73.5	$0
Total annual burden per Covered Entity or Non-Covered Broker-Dealer	1			$73.5	$0
Total number of affected entities	× 3,918			× 3,918	$0
Sub-total burden	3,918 hours			$287,973	$0
Retention of copy of any Form SCIR or immediate notice to the Commission	1	×	$73.5 (blended rate for general clerk and compliance clerk)	$73.5	$0
Total annual burden per Covered Entity or Non-Covered Broker-Dealer	1			$73.5	$0
Total number of affected entities	× 3,918			× 3,918	$0
Sub-total burden	3,918 hours			$287,973	$0
Retention of records documenting a cybersecurity incident	1	×	$73.5 (blended rate for general clerk and compliance clerk)	$73.5	$0
Total annual burden per Covered Entity	1			$73.5	$0
Total number of affected Covered Entities	× 1,949			× 1,949	$0
Sub-total burden	1,949 hours			$143,251.50	$0
Retention of records documenting a Covered Entity's cybersecurity risk assessment	1	×	$73.5 (blended rate for general clerk and compliance clerk)	$73.5	$0

975 Given the general nature of the recordkeeping requirements for national securities exchanges, national securities associations, registered clearing agencies, and the MSRB under Rule 17a-1 (OMB control number 3235-0208, Recordkeeping Rule for National Securities Exchanges, National Securities Associations, Registered Clearing Agencies, and the Municipal Securities Rulemaking Board) and for SBSDRs under Rule 13n-7 (OMB control number 3235-0719, Security-Based Swap Data Repository Registration, Duties, and Core Principles and Form SDR), it is anticipated that the new recordkeeping requirements proposed in this release would result in a one-time nominal increase in burden per entity that would effectively be encompassed by the existing burden estimates associated with these existing rules as described in those collections of information. Below, the Commission solicits comment regarding all of the PRA estimates discussed in this release.

Total annual burden per Covered Entity	1			$73.5	$0
Total number of affected Covered Entities	× 1,949			× 1,949	$0
Sub-total burden	1,949 hours			$143,251.50	$0
Retention of copy of any public disclosures	1	×	$73.5 (blended rate for general clerk and compliance clerk)	$73.5	$0
Total annual burden per Covered Entity	1			$73.5	$0
Total number of affected Covered Entities	× 1,949			× 1,949	$0
Sub-total burden	1,949 hours			$143,251.50	$0
Total annual aggregate burden of recordkeeping obligations	**17,601 hours**			**$1,293,673.5**	$0

4. Substituted Compliance- Rule 3a71-6

Rule 3a71–6 would require submission of certain information to the Commission to the extent SBS Entities elect to request a substituted compliance determination with respect to proposed Rule 10, Form SCIR, and the related record preservation requirements. Consistent with Exchange Act Rule 0-13, such applications must be accompanied by supporting documentation necessary for the Commission to make the determination, including information regarding applicable foreign requirements, and the methods used by foreign authorities to monitor and enforce compliance. If Rule 3a71-6 is amended as proposed, the Commission expects that the majority of such requests will be made during the first year following the effective date.

The Commission expects that the great majority of substituted compliance applications will be submitted by foreign authorities, and that very few substituted compliance requests will come from SBS Entities. For purposes of this assessment, the Commission estimates that three such SBS Entities will submit such an application.[976]

---

976 *See* SBS Entity Risk Mitigation Adopting Release, 85 FR at 6389. *See also* SBS Entity Business Conduct Standards Adopting Release, 81 FR at 30097, n.1582 and accompanying text; SBS Entity Trade Acknowledgement and Verification Adopting Release, 81 FR at 39832; SBS Entity Recordkeeping and Reporting Adopting Release, 84 FR at 68609; Capital, Margin, and Segregation Requirements Adopting Release, 84 FR at 43967.

The Commission has previously estimated that the paperwork burden associated with filing a request for a substituted compliance determination related to existing business conduct, supervision, chief compliance officer, and trade acknowledgement and verification requirements described in Rule 3a71-6(d)(1)-(3) was approximately 80 hours of in-house counsel time, plus $84,000[977] for the services of outside professionals, and the paperwork burden estimate associated with making a request for a substituted compliance determination related to the existing recordkeeping and reporting requirements described in Rule 3a71-6(d)(6) was approximately 80 hours of in-house counsel time, plus $84,000[978] for the services of outside professionals.[979] To the extent that an SBS Entity files a request for a substituted compliance determination in connection with Rule 10, Form SCIR, the related record preservation requirements, and requirements currently identified in Rule 3a71-6(d) as eligible for substituted compliance determinations, the Commission believes that the paperwork burden associated with the request would be greater than that associated with a narrower request due to the need for more information regarding the comparability of the relevant rules and the adequacy of the associated supervision and enforcement practices. However, the Commission believes that its prior paperwork burden estimate is sufficient to cover a combined substituted compliance request that also seeks a determination in connection with Rule 10, Form SCIR, and the related record preservation requirements.[980]

---

977 Based on 200 hours of outside time x $420 per hour. This estimated burden also includes the burden associated with making a request for a substituted compliance determination related to the portfolio reconciliation, portfolio compression, and trading relationship documentation requirements described in Rule 3a71-6(d)(7); *see* SBS Entity Risk Mitigation Adopting Release, 85 FR at 6389.

978 Based on 200 hours of outside time x $420 per hour.

979 *See Supporting Statement for the Paperwork Reduction Act Information Collection Submission for Exchange Act Rule 3a71-6* (June 10, 2021), *available at* https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=202106-3235-008.

980 Although applicants may file requests for substituted compliance determinations related multiple eligible requirements, applicants may instead file requests for substituted compliance determinations related to individual eligible requirements. As such, the Commission's estimates reflect the total paperwork burden of requests filed by (i) applicants that would be seeking a substituted compliance determination related to Rule

Nevertheless, the Commission is revising its estimate of the hourly rate for outside professionals to $496, consistent with the other paperwork burden estimates in this release. Therefore, the Commission estimates that the total paperwork burden incurred by entities associated with preparing and submitting a request for a substituted compliance determination in connection with the proposed cybersecurity risk management requirements applicable to SBS Entities would be reflected in the estimated burden of a request for a substituted compliance determination related to the business conduct, supervision, chief compliance officer, trade acknowledgement and verification, and the portfolio reconciliation, portfolio compression, and trading relationship documentation requirements described in Rule 3a71-6(d)(1)-(3) and (7) of approximately 80 hours of in-house counsel time, plus $99,200 for the services of outside professionals,[981] and the paperwork burden associated with making a request for a substituted compliance determination related to the recordkeeping and reporting requirements described in Rule 3a71-6(d)(6) of approximately 80 hours of in-house counsel time, plus $99,200 for the services of outside professionals.[982] This estimate results in an aggregate total one-time paperwork burden associated with preparing and submitting requests for substituted compliance determinations relating to the requirements described in Rule 3a71-6(d)(1) through (3), (6) and (7), including the proposed cybersecurity risk management requirements, of approximately 480 internal hours,[983] plus $595,200 for the services of outside professionals[984] for all three requests.

E. Collection of Information is Mandatory

10, Form SCIR, and the related record preservation requirements combined with a request for a substituted compliance determination related to other eligible requirements, and (ii) applicants that previously filed requests for substituted compliance determinations related to other eligible requirements and would be seeking an additional substituted compliance determination in connection with Rule 10, Form SCIR, and the related record preservation requirements.

981 Based on 200 hours of outside time x $496 per hour.

982 Based on 200 hours of outside time x $496 per hour.

983 (80 hours related to Rule 3a71-6(d)(1) through (3), (7) plus 80 hours related to Rule 3a71-6(d)(6)) * 3 requests.

984 ($99,200 related to Rule 3a71-6(d)(1) through (3), (7) plus $99,200 related to Rule 3a71-6(d)(6)) * 3 requests.

The collections of information pursuant to proposed Rule 10, Form SCIR, and the relevant recordkeeping rules are mandatory, as applicable, for Market Entities. With respect to Rule 3a71-6, the application for substituted compliance is mandatory for all foreign financial regulatory authorities or SBS Entities that seek a substituted compliance determination.

F. Confidentiality of Responses to Collection of Information

The Commission expects to receive confidential information in connection with the collections of information. A Market Entity can request confidential treatment of the information.[985] If such confidential treatment request is made, the Commission anticipates that it will keep the information confidential subject to applicable law.[986]

With regard to Rule 3a71-6, the Commission generally will make requests for a substituted compliance determination public, including supporting documentation provided by the requesting party, subject to requests for confidential treatment being submitted pursuant to any applicable provisions governing confidentiality under the Exchange Act.[987] If confidential treatment is granted, the Commission would keep such information confidential, subject to the provisions of applicable law.[988]

G. Retention Period for Recordkeeping Requirements

Rule 17a-4, as proposed to be amended, specifies the required retention periods for records required to be made and preserved by a broker-dealer, whether electronically or otherwise.[989] Rule 17ad-7, as proposed to be amended, specifies the required retention periods

---

985 *See* 17 CFR 200.83. Information regarding requests for confidential treatment of information submitted to the Commission is available on the Commission's website at https://www.sec.gov/foia/howfo2.htm#privacy.

986 *See, e.g.,* 5 U.S.C. 552 *et seq*.; 15 U.S.C. 78x (governing the public availability of information obtained by the Commission).

987 *See, e.g.,* 17 CFR 200.83; 17 CFR 240.24b-2; *see also* SBS Entity Definitions Adopting Release, 79 FR at 47359.

988 *See, e.g.,* 5 U.S.C. 552 *et seq*.; 15 U.S.C. 78x (governing the public availability of information obtained by the Commission).

989 *See* Rule 17a-4, as proposed to be amended.

for records required to be made and preserved by transfer agents, whether electronically or otherwise.[990] Rule 18a-6, as proposed to be amended, specifies the required retention periods for records required to be made and preserved by SBSDs or MSBSPs, whether electronically or otherwise.[991] All records required of certain of the Market Entities pursuant to the proposed rule amendments must be retained for three years.[992] Existing Rule 17a-1 specifies the required retention periods for records required to be made and preserved by national securities exchanges, national securities associations, registered clearing agencies, and the MSRB, whether electronically or otherwise.[993] Under the existing provisions of Rule 17a-1, registered clearing agencies, the MSRB, national securities associations, and national securities exchanges would be required to preserve at least one copy of the Rule 10 Records for at least five years, the first two years in an easily accessible place. Existing Rule 13n-7, which is not proposed to be amended, specifies the required retention periods for records required to be made and preserved by SBSDRs, whether electronically or otherwise.[994] Rule 13n-7 provides that the SBSDR must keep the documents for a period of not less than five years, the first two years in a place that is immediately available to representatives of the Commission for inspection and examination.[995] Finally, exempt clearing agencies are generally subject to conditions that mirror certain of the recordkeeping requirements in Rule 17a-1.[996] Nonetheless, the Commission is proposing to amend the clearing agency exemption orders to add a condition that each exempt clearing agency

---

990 *See* Rule 17ad-7, as proposed to be amended.

991 *See* Rule 18a-6, as proposed to be amended.

992 *See* Rules 17a-4, 17A-d, and 18a-6, as proposed to be amended.

993 *See* Rule 17a-1.

994 *See* Rule 13n-7.

995 *See* paragraph (b)(2) of Rule 13n-7.

996 *See, e.g.,* BSTP SS&C Order, 80 FR at 75411 (conditioning BSTP's exemption by requiring BSTP to, among other things, preserve a copy or record of all trade details, allocation instructions, central trade matching results, reports and notices sent to customers, service agreements, reports regarding affirmation rates that are sent to the Commission or its designee, and any complaint received from a customer, all of which pertain to the operation of its matching service and ETC service. BSTP shall retain these records for a period of not less than five years, the first two years in an easily accessible place).

must retain the Rule 10 Records for a period of at least five years after the record is made or, in the case of the written policies and procedures to address cybersecurity risks, for at least five years after the termination of the use of the policies and procedures.

H. Request for Comment

Pursuant to 44 U.S.C. 3506(c)(2)(B), the Commission solicits comment on the proposed collections of information in order to:

- Evaluate whether the proposed collections of information are necessary for the proper performance of the functions of the Commission, including whether the information would have practical utility;
- Evaluate the accuracy of the Commission's estimates of the burden of the proposed collections of information;
- Determine whether there are ways to enhance the quality, utility, and clarity of the information to be collected; and
- Evaluate whether there are ways to minimize the burden of the collection of information on those who respond, including through the use of automated collection techniques or other forms of information technology.

Persons submitting comments on the collection of information requirements should direct them to the Office of Management and Budget, Attention: Desk Officer for the Securities and Exchange Commission, Office of Information and Regulatory Affairs, Washington, DC 20503, and should also send a copy of their comments to Vanessa A. Countryman, Secretary, Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549-1090, with reference to File Number S7-06-23. Requests for materials submitted to OMB by the Commission with regard to this collection of information should be in writing, with reference to File Number S7-06-23 and be submitted to the Securities and Exchange Commission, Office of FOIA/PA Services, 100 F Street NE., Washington, DC 20549-2736. As OMB is required to make a decision concerning the collections of information between 30 and 60 days after publication, a

comment to OMB is best assured of having its full effect if OMB receives it within 30 days of publication.

VI. INITIAL REGULATORY FLEXIBILITY ACT ANALYSIS

The RFA requires the Commission, in promulgating rules, to consider the impact of those rules on small entities.[997] Section 603(a) of the Administrative Procedure Act,[998] as amended by the RFA, generally requires the Commission to undertake a regulatory flexibility analysis of all proposed rules to determine the impact of such rulemaking on "small entities."[999] Section 605(b) of the RFA states that this requirement shall not apply to any proposed rule which, if adopted, would not have a significant economic impact on a substantial number of small entities.[1000]

The Commission has prepared the following Initial Regulatory Flexibility Analysis ("IRFA") in accordance with section 3(a) of the RFA.[1001] It relates to: (1) proposed Rule 10 under the Exchange Act; (2) proposed Form SCIR; and (3) proposed amendments to Rules 17a-4, 17ad-7, and 18a-6 under the Exchange Act.[1002]

A. Reasons for, and Objectives of, Proposed Action

The reasons for, and objectives of, the proposed rule and rule amendments are discussed above.[1003]

1. Proposed Rule 10 and Parts I and II of Proposed Form SCIR

---

997 *See* 5 U.S.C. 601 *et seq*.

998 5 U.S.C. 603(a).

999 Section 601(b) of the RFA permits agencies to formulate their own definitions of "small entities." *See* 5 U.S.C. 601(b). The Commission has adopted definitions for the term "small entity" for the purposes of rulemaking in accordance with the RFA. These definitions, as relevant to this proposed rulemaking, are set forth in Rule 0-10.

1000 *See* 5 U.S.C. 605(b).

1001 5 U.S.C. 603(a).

1002 The Commission is also certifying that that amendments to Rule 3a71-6 will not have a significant economic impact on a substantial number of small entities for purposes of the RFA. *See* section VI.C.5. of this release.

1003 *See* sections I and II of this release.

Proposed Rule 10 would require all Market Entities (Covered Entities and non-Covered Entities) to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks.[1004] All Market Entities also, at least annually, would be required to review and assess the design and effectiveness of their cybersecurity policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review.[1005] They also would be required to prepare a report (in the case of Covered Entities) and a record (in the case of non-Covered Entities) with respect to the annual review.[1006] Finally, all Market Entities would need to give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring.[1007]

Market Entities that meet the definition of "covered entity" would be subject to certain additional requirements under proposed Rule 10.[1008] First, their cybersecurity risk management policies and procedures would need to include the following elements:

- Periodic assessments of cybersecurity risks associated with the Covered Entity's information systems and written documentation of the risk assessments;
- Controls designed to minimize user-related risks and prevent unauthorized access to the Covered Entity's information systems;
- Measures designed to monitor the Covered Entity's information systems and protect the Covered Entity's information from unauthorized access or use, and oversight of

---

1004 *See* paragraphs (b) through (d) of proposed Rule 10 (setting forth the requirements for Market Entities that meet the definition of "covered entity"); paragraph (e)(1) of proposed Rule 10. *See also* sections II.B.1 and II.C. of this release (discussing these proposed requirements in more detail).

1005 *See* paragraph (b)(2) of proposed Rule 10; paragraph (e)(1) of proposed Rule 10. *See also* sections II.B.1.f. and II.C. of this release (discussing these proposed requirements in more detail).

1006 *See* paragraph (b)(2) of proposed Rule 10; paragraph (e)(1) of proposed Rule 10. *See also* sections II.B.1.f. and II.C. of this release (discussing these proposed requirements in more detail).

1007 *See* paragraph (c)(1) of proposed Rule 10; paragraph (e)(2) of proposed Rule 10. *See also* sections II.B.2.a. and II.C. of this release (discussing these proposed requirements in more detail).

1008 *See* paragraph (b) through (d) of proposed Rule 10 (setting forth the requirements for Market Entities that meet the definition of "covered entity"); paragraph (e) of proposed Rule 10 (setting forth the requirements for Market Entities that do not meet the definition of "covered entity").

service providers that receive, maintain, or process information, or are otherwise permitted to access the Covered Entity's information systems;

- Measures to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the Covered Entity's information systems; and

- Measures to detect, respond to, and recover from a cybersecurity incident and written documentation of any cybersecurity incident and the response to and recovery from the incident.[1009]

Second, Covered Entities—in addition to providing the Commission with immediate written electronic notice of a significant cybersecurity incident—would need to report and update information about the significant cybersecurity incident by filing Part I of proposed Form SCIR with the Commission through the EDGAR system.[1010] The form would elicit information about the significant cybersecurity incident and the Covered Entity's efforts to respond to, and recover from, the incident.

Third, Covered Entities would need to publicly disclose summary descriptions of their cybersecurity risks and the significant cybersecurity incidents they experienced during the current or previous calendar year on Part II of proposed Form SCIR.[1011] The form would need to be filed with the Commission through the EDGAR system and posted on the Covered Entity's business Internet website and, in the case of Covered Entities that are carrying or introducing broker-dealers, provided to customers at account opening and annually thereafter.

Covered Entities and Non-Covered Entities would need to preserve certain records relating to the requirements of proposed Rule 10 in accordance with amended or existing recordkeeping requirements applicable to them or, in the case of exempt clearing agencies, pursuant to conditions in relevant exemption orders.[1012]

[1009] *See* sections II.B.1.a. through II.B.1.e. of this release (discussing these proposed requirements in more detail). In the case of non-Covered Entities, as discussed in more detail below in section II.C. of this release, the design of the cybersecurity risk management policies and procedures would need to take into account the size, business, and operations of the broker-dealer. *See* paragraph (e) of proposed Rule 10.

[1010] *See* sections II.B.2. and II.B.4. of this release (discussing these proposed requirements in more detail).

[1011] *See* sections II.B.3. and II.B.4.of this release (discussing these proposed requirements in more detail).

[1012] *See* sections II.B.5. and II.C. of this release (discussing these proposed requirements in more detail).

Collectively, these requirements are designed to address cybersecurity risk and the threat it poses to Market Entities and the U.S. securities markets. The written policies and procedures, the records required to be made pursuant to those policies and procedures, and the report or record of the annual review of the policies and procedures would address the specific cybersecurity risks to which Market Entities are exposed. The Commission could use these written policies and procedures, reports, and records to review Market Entities' compliance with proposed Rule 10.

The Commission could use the immediate written electronic notification of significant cybersecurity incidents to promptly begin to assess the situation by, for example, when warranted, assessing the Market Entity's operating status and engaging in discussions with the Market Entity to understand better what steps it is taking to protect its customers, counterparties, members, registrants, or user. The Commission could use the subsequent reports about the significant cybersecurity incident filed by Covered Entities using Part I of proposed Form SCIR to understand better the nature and extent of a particular significant cybersecurity incident and the efficacy of the Covered Entity's response to mitigate the disruption and harm caused by the incident. The Commission staff could use the reports to focus on the Covered Entity's operating status and to facilitate their outreach to, and discussions with, personnel at the Covered Entity who are addressing the significant cybersecurity incident. In addition, the reporting would provide the staff with a view into the Covered Entity's understanding of the scope and impact of the significant cybersecurity incident. All of this information could be used by the Commission and its staff in assessing the significant cybersecurity incident impacting the Covered Entity. Further, the Commission could be use the database of reports to assess the potential cybersecurity risks affecting U.S. securities markets more broadly. This information could be used to address future significant cybersecurity incidents. For example, these reports could assist the Commission in identifying patterns and trends across Covered Entities, including widespread cybersecurity incidents affecting multiple Covered Entities at the same time. Further, the reports

could be used to evaluate the effectiveness of various approaches to respond to and recover from a significant cybersecurity incident.

The disclosures by Covered Entities on Part II of proposed Form SCIR would be used to provide greater transparency to customers, counterparties, registrants, or members of the Covered Entity, or to users of its services, about the Covered Entity's cybersecurity risk profile. This information could be used by these persons to manage their own cybersecurity risk and, to the extent they have choice, select a Covered Entity with whom to transact or otherwise conduct business. In addition, because the reports would be filed through EDGAR, Covered Entities' customers, counterparties, members, registrants, or users would be able to run search queries to compare the disclosures of multiple Covered Entities. This would make it easier for Commission staff and others to assess the cybersecurity risk profiles of different types of Covered Entities and could facilitate trend analysis by members of the public of significant cybersecurity incidents.

2. Rules 17a-4, 17ad-7, 18a-6 and Clearing Agency Exemption Orders

Rules 17a-4, 17ad-7, and 18a-6—which apply to broker-dealers, transfer agents, and SBS Entities, respectively—would be amended to establish preservation and maintenance requirements for the written policies and procedures, annual reports, Parts I and II of proposed form SCIR, and records required to be made pursuant to proposed Rule 10 (*i.e.*, the Rule 10 Records).[1013] The proposed amendments would specify that the Rule 10 Records must be retained for three years. In the case of the written policies and procedures to address cybersecurity risks, the record would need to be maintained until three years after the termination of the use of the policies and procedures.[1014] In addition, orders exempting certain clearing

---

[1013] *See* sections II.B.5. and II.C. of this release (discussing these proposed amendments in more detail). Rule 17a-4 sets forth record preservation and maintenance requirements for broker-dealers, Rule 17ad-7 sets forth record preservation and maintenance requirements for transfer agents, and Rule 18a-6 sets forth record preservation and maintenance requirements for SBS Entities.

[1014] *See* proposed amendments to Rule 17a-4.

agencies from registering with the Commission would be amended to establish preservation and maintenance requirements for the Rule 10 Records that would apply to the exempt clearing agencies subject to those orders.[1015] The amendments would provide that the records need to be retained for five years (consistent with Rules 13n-7 and 17a-1).[1016] In the case of the written policies and procedures to address cybersecurity risks, the record would need to be maintained until five years after the termination of the use of the policies and procedures. The preservation of these records would make them available for examination by the Commission and other regulators.

B. Legal Basis

The Commission is proposing Rule 10 and Form SCIR under the Exchange Act, as well as amendments to Rules 17a-4, 17ad-7, and 18a-6 under the Exchange Act, under the following authorities under the Exchange Act: (1) Sections 15, 17, and 23 for broker-dealers (15 U.S.C. 78*o*, 78q, and 78w); (2) Sections 17, 17A, and 23 for clearing agencies (15 U.S.C. 78q, 17q-1, and 78w(a)(1)); (3) Sections 15B, 17, and 23 for the MSRB (15 U.S.C. 78*o*–4, 78q(a), and 78w); (4) Sections 6(b), 11A, 15A, 17, and 23 for national securities exchanges and national securities associations (15 U.S.C. 78f, 78k-1, 78*o*-3, and 78w); (5) Sections 15F, 23, and 30(c) for SBS Entities (15 U.S.C. 78*o*-10, 78w, and 78dd(c)); (6) Sections 13 and 23 for SBSDRs (15 U.S.C. 78m and 78w); and (7) Sections 17a, 17A, and 23 for transfer agents (78q, 17q-1, and 78w).

C. Small Entities Subject to Proposed Rule, Form SCIR, and Recordkeeping Rule Amendments

As discussed above, the Commission estimates that a total of approximately 1,989 Covered Entities (consisting of 1,541 broker-dealers, 16 clearing agencies, the MSRB, 25 total

---

[1015] *See* section II.B.5. of this release (discussing these proposed amendments in more detail).

[1016] For the reasons discussed in section II.B.5.a. of this release, the proposal would not amend Rules 13n-7 or 17a-1. As explained in that section of the release, the existing requirements of Rule 13n-7 (which applies to SBSDRs) and Rule 17a-1 (which applies to registered clearing agencies, the MSRB, national securities associations, and national securities exchanges) will require these Market Entities to retain the Rule 10 Records for five years and, in the case of the written policies and procedures, for five years after the termination of the use of the policies and procedures.

national securities exchanges and national securities associations, 50 SBS Entities, 3 SBSDRs, and 353 transfer agents) and 1,969 Non-Covered Broker-Dealers would be subject to the new cybersecurity requirements and related recordkeeping requirements as a result of: (1) proposed Rule 10 under the Exchange Act; (2) proposed Form SCIR; and (3) proposed amendments to Rules 17a-4, 17ad-7, and 18a-6 under the Exchange Act. The number of these firms that may be considered "small entities" are discussed below.

1. Broker-Dealers

For purposes of Commission rulemaking, a small entity includes, when used with reference to a broker-dealer, a broker-dealer that: (1) had total capital (net worth plus subordinated liabilities) of less than $500,000 on the date in the prior fiscal year as of which its audited financial statements were prepared pursuant to Rule 17a-5(d) under the Exchange Act, or, if not required to file such statements, a broker-dealer with total capital (net worth plus subordinated liabilities) of less than $500,000 on the last day of the preceding fiscal year (or in the time that it has been in business, if shorter); and (2) is not affiliated with any person (other than a natural person) that is not a small business or small organization.[1017]

Based on FOCUS Report data, the Commission estimates that as of September 30, 2022, approximately 764 broker-dealers total (195 broker-dealers that are Covered Entities and 569 broker-dealers that are Non-Covered Broker-Dealers) that might be deemed small entities for purposes of this analysis.

2. Clearing Agencies

For the purposes of Commission rulemaking, a small entity includes, when used with reference to a clearing agency, a clearing agency that: (1) compared, cleared, and settled less than $500 million in securities transactions during the preceding fiscal year; (2) had less than $200 million of funds and securities in its custody or control at all times during the preceding

---

[1017] *See* paragraph (c) of Rule 0-10.

fiscal year (or at any time that it has been in business, if shorter); and (3) is not affiliated with any person (other than a natural person) that is not a small business or small organization.[1018]

Based on the Commission's existing information about the clearing agencies currently registered with the Commission, the Commission preliminarily believes that such entities exceed the thresholds defining "small entities" set out above. While other clearing agencies may emerge and seek to register as clearing agencies, the Commission preliminarily does not believe that any such entities would be "small entities" as defined in Exchange Act Rule 0-10. Consequently, the Commission certifies that the proposed rule and form would not, if adopted, have a significant economic impact on a substantial number of small entities.

3. The MSRB

The Commission's rules do not define "small business" or "small organization" for purposes of entities like the MSRB. The MSRB does not fit into one of the categories listed under the Commission rule that provides guidelines for a defined group of entities to qualify as a small entity for purposes of Commission rulemaking under the RFA.[1019] The RFA in turn, refers to the Small Business Administration ("SBA") in providing that the term "small business" is defined as having the same meaning as the term "small business concern" under section 3 of the Small Business Act.[1020] The SBA provides a comprehensive list of categories with accompanying size standards that outline how large a business concern can be and still qualify as a small business.[1021] The industry categorization that appears to best fit the MSRB under the SBA table is Professional Organization. The SBA defines a Professional Organization as an entity having average annual receipts of less than $15 million. Within the MSRB's 2021 Annual

---

1018 *See* paragraph (d) of Rule 0-10.

1019 *See* Rule 0-10.

1020 *See* 5 U.S.C. 601(3).

1021 *See* 13 CFR 121.201. *See also* SBA, Table of Small Business Size Standards Marched to North American Industry Classification System Codes, *available at* https://www.sba.gov/sites/default/files/files/Size_Standards_Table.pdf (outlining the list of small business size standards within 13 CFR 121.201).

Report the organization reported total revenue exceeding $35 million for fiscal year 2021.[1022] The Report also stated that the organization's total revenue for fiscal year 2020 exceeded $47 million.[1023] The Commission is using the SBA's definition of small business to define the MSRB for purposes of the RFA and has concluded that the MSRB is not a "small entity." Consequently, the Commission certifies that the proposed rule and form would not, if adopted, have a significant economic impact on a substantial number of small entities.

4. National Securities Exchanges and National Securities Associations

For the purposes of Commission rulemaking, and with respect to the national securities exchanges, the Commission has defined a "small entity" as an exchange that has been exempt from the reporting requirements of Rule 601 of Regulation NMS and is not affiliated with any person (other than a natural person) that is not a small business or small organization.[1024] None of the national securities exchanges registered under section 6 of the Exchange Act that would be subject to the proposed rule and form is a "small entity" for purposes of the RFA.

There is only one national securities association (FINRA), and the Commission has previously stated that it is not a small entity as defined by 13 CFR 121.201.[1025] Consequently, the Commission certifies that the proposed rule and form would not, if adopted, have a significant economic impact on a substantial number of small entities.

5. SBS Entities

For purposes of Commission rulemaking, a small entity includes: (1) when used with reference to an "issuer" or a "person," other than an investment company, an "issuer" or "person" that, on the last day of its most recent fiscal year, had total assets of $5 million or

---

1022 *See* MSRB, 2021 Annual Report, 16, *available at* https://msrb.org/-/media/Files/Resources/MSRB-2021-Annual-Report.ashx.

1023 *Id*.

1024 *See* paragraph (e) of Rule 0-10.

1025 *See, e.g.*, Securities Exchange Act Release No. 62174 (May 26, 2010), 75 FR 32556, 32605 n.416 (June 8, 2010) ("FINRA is not a small entity as defined by 13 CFR 121.201.").

less;[1026] or (2) a broker-dealer with total capital (net worth plus subordinated liabilities) of less than $500,000 on the date in the prior fiscal year as of which its audited financial statements were prepared pursuant to Rule 17a-5(d) under the Exchange Act,[1027] or, if not required to file such statements, a broker-dealer with total capital (net worth plus subordinated liabilities) of less than $500,000 on the last day of the preceding fiscal year (or in the time that it has been in business, if shorter); and is not affiliated with any person (other than a natural person) that is not a small business or small organization.[1028]

With respect to SBS Entities, based on feedback from market participants and our information about the security-based swap markets, and consistent with our position in prior rulemakings arising out of the Dodd-Frank Act, the Commission continues to believe that: (1) the types of entities that will engage in more than a *de minimis* amount of dealing activity involving security-based swaps—which generally would be large financial institutions—would not be "small entities" for purposes of the RFA, and (2) the types of entities that may have security-based swap positions above the level required to be MSBSPs would not be "small entities" for purposes of the RFA.[1029]

Consequently, the Commission certifies that with respect to SBS Entities the proposed rule and form (as well as the amendments to Rule 3a71-6) would not, if adopted, have a significant economic impact on a substantial number of small entities.

6. SBSDRs

1026 *See* paragraph (a) of Rule 0-10.

1027 17 CFR 240.17a-5(d).

1028 *See* paragraph (c) of Rule 0-10.

1029 *See, e.g.*, SBS Entity Risk Mitigation Adopting Release, 85 FR at 6411; SBS Entity Registration Adopting Release, 80 FR at 49013; Recordkeeping and Reporting Requirements for Security-Based Swap Dealers, Major Security-Based Swap Participants, and Broker-Dealers; Capital Rule for Certain Security-Based Swap Dealers, Exchange Act Release No. 71958 (Apr. 17, 2014), 79 FR 25193, 25296-97 and n.1441 (May 2, 2014); Further Definition Release, 77 FR at 30743.

For purposes of Commission rulemaking regarding SBSDRs, a small entity includes: (1) when used with reference to an "issuer" or a "person," other than an investment company, an "issuer" or "person" that, on the last day of its most recent fiscal year, had total assets of $5 million or less;[1030] or (2) a broker-dealer with total capital (net worth plus subordinated liabilities) of less than $500,000 on the date in the prior fiscal year as of which its audited financial statements were prepared pursuant to Rule 17a-5(d) under the Exchange Act,[1031] or, if not required to file such statements, a broker-dealer with total capital (net worth plus subordinated liabilities) of less than $500,000 on the last day of the preceding fiscal year (or in the time that it has been in business, if shorter); and is not affiliated with any person (other than a natural person) that is not a small business or small organization.[1032]

Based on the Commission's existing information about the SBSDRs currently registered with the Commission, and consistent with the Commission's prior rulemakings,[1033] the Commission preliminarily believes that such entities exceed the thresholds defining "small entities" set out above. While other SBSDRs may emerge and seek to register as SBSDRs, the Commission preliminarily does not believe that any such entities would be "small entities" as defined in Exchange Act Rule 0-10. Consequently, the Commission certifies that the proposed

---

1030 *See* paragraph (a) of Rule 0-10.

1031 17 CFR 240.17a-5(d).

1032 *See* paragraph (c) of Rule 0-10.

1033 *See, e.g.*, SBSDR Adopting Release, 80 FR at 14548-49 (stating that "[i]n the Proposing Release, the Commission stated that it did not believe that any persons that would register as SBSDRs would be considered small entities. The Commission stated that it believed that most, if not all, SBSDRs would be part of large business entities with assets in excess of $5 million and total capital in excess of $500,000. As a result, the Commission certified that the proposed rules would not have a significant impact on a substantial number of small entities and requested comments on this certification. The Commission did not receive any comments that specifically addressed whether Rules 13n–1 through 13n–12 and Form SBSDR would have a significant economic impact on small entities. Therefore, the Commission continues to believe that Rules 13n–1 through 13n–12 and Form SBSDR will not have a significant economic impact on a substantial number of small entities. Accordingly, the Commission hereby certifies that, pursuant to 5 U.S.C. 605(b), Rules 13n–1 through 13n–12, Form SBSDR will not have a significant economic impact on a substantial number of small entities").

rule and form would not, if adopted, have a significant economic impact on a substantial number of small entities.

7. Transfer Agents

For purposes of Commission rulemaking, Exchange Act Rule 0-10(h) provides that the term small business or small organization shall, when used with reference to a transfer agent, mean a transfer agent that: (1) received less than 500 items for transfer and less than 500 items for processing during the preceding six months (or in the time that it has been in business, if shorter); (2) transferred items only of issuers that would be deemed "small businesses" or "small organizations" as defined in this section; and (3) maintained master shareholder files that in the aggregate contained less than 1,000 shareholder accounts or was the named transfer agent for less than 1,000 shareholder accounts at all times during the preceding fiscal year (or in the time that it has been in business, if shorter); and (4) is not affiliated with any person (other than a natural person) that is not a small business or small organization under this section.[1034] As of March 31, 2022, the Commission estimates there were 158 transfer agents that were considered small organizations. Our estimate is based on the number of transfer agents that reported a value of fewer than 1,000 for items 4(a) and 5(a) on Form TA-2 for the 2021 annual reporting period (which was required to be filed by March 31, 2022).[1035]

D. Reporting, Recordkeeping, and Other Compliance Requirements

1. Proposed Rule 10 and Parts I and II of Proposed Form SCIR

The proposed requirements under proposed Rule 10 and Parts I and II of proposed Form SCIR, including compliance and recordkeeping requirements, are summarized in this IRFA.[1036]

1034 *See* paragraph (h) of Rule 0-10.

1035 Item 4(a) on Form TA-2 requires each transfer agent to provide the number of items received for transfer during the reporting period. Item 5(a) on Form TA-2 requires each transfer agent to provide its total number of individual securityholder accounts, including accounts in the Direct Registration System (DRS), dividend reinvestment plans and/or direct purchase plans as of December 31."

1036 *See* section VI.A. of this release. *See also* section II of this release (discussing the requirements of proposed Rule 10 and Parts I and II of proposed Form SCIR in more detail).

The burdens on respondents, including those that are small entities, are discussed above in the Commission's economic analysis and PRA analysis.[1037] They also are discussed below.

As discussed above, there are approximately 764 small entity broker-dealers. 195 of these broker-dealers would be Covered Entities and 569 of these broker-dealers would be Non-Covered Broker-Dealers under proposed Rule 10. In addition, there are approximately 158 small entity transfer agents, all of which would be Covered Entities (resulting in a total of 353 small entities that would be Covered Entities). The total number of small entity broker-dealers or transfer agents that would be subject to the requirements of proposed Rule 10 as either Covered Entities or Non-Covered Broker-Dealers is 922.

The requirements under proposed Rule 10 to implement and review certain policies and procedures would result in costs to these small entities. For Covered Entities, this would create a new annual burden of approximately 31.67 hours per firm, or 11,179.51 hours in aggregate for small entities. The Commission therefore expects the annual monetized aggregate cost to small entities to be $5,164,933.62.[1038] For Non-Covered Broker-Dealers, the requirements would create a new annual burden of approximately 21 hours per firm, or 11,949 hours in aggregate for small entities. The Commission therefore expects the annual monetized aggregate cost to small entities to be $5,520,438.[1039]

In addition, there are approximately 922 small entities that would be subject to the notification requirements of proposed Rule 10. The requirement to make a determination regarding a significant cybersecurity incident and immediate notice to the Commission would create a new annual burden of approximately 4.67 hours per Market Entity, or 4,305.74 hours in aggregate for small entities. The Commission therefore expects the annual monetized aggregate

---

1037 *See* sections IV and V of this release (setting forth the Commission's economic analysis and PRA analysis, respectively).

1038 $29,102,133.06 total cost x (353 small entities/ 1,989 total entities) = $5,164,933.62.

1039 $19,103,238 total cost x (569 small entities/ 1,969 total entities) = $5,520,438.

cost to small entities associated with the proposed notification requirement under Rule 10 to be $1,519,926.22.[1040] The 353 small entities that would be Covered Entities would also be subject to the requirements to file Part I of proposed Form SCIR. This would create a new annual burden of approximately 2.5 hours per Covered Entity, or 882.5 hours in aggregate for small entities. The Commission therefore expects the annual monetized aggregate cost to small entities associated with Part I of proposed Form SCIR to be $380,357.50.[1041]

In addition, the approximately 353 small entities that are Covered Entities would be subject to the disclosure requirements of proposed Rule 10. These 353 small entities would be required to make certain public disclosures on Part II of proposed Form SCIR. This would create a new annual burden of approximately 3.67 hours per Covered Entity, or 1,295.51 hours in aggregate for small entities. The Commission therefore expects the annual monetized aggregate cost to small entities associated with Part II of proposed Form SCIR to be $486,243.38.[1042]

Furthermore, the requirement to file Form SCIR using a form-specific XML may impose some compliance costs for entities not already required to file in EDGAR. Because all transfer agents are already required to file in EDGAR their annual reports on Form TA-2, no small entity transfer agent will incur an additional burden for filing their public disclosures in EDGAR. Assuming all 195 small broker-dealers that are Covered Entities do not already file in EDGAR, the requirement to file the public disclosures in EDGAR would create an initial, one-time burden of approximately 0.30 hours per Covered Entity, or 58.5 hours in aggregate for small entities, to complete and submit a Form ID. In addition, the requirement to file Form SCIR using custom XML (with which a Covered Entity would be able to comply by inputting its disclosures into a fillable web form) would create an ongoing burden of 0.5 hours per filing, or 176.5 hours for all small entities collectively.

[1040] $6,524,802.58 total cost x (922 small entities / 3,958 total entities) = $1,519,926.22.

[1041] $2,143,147.5 total cost x (353 small entities / 1,989 total entities) = $380,357.50.

[1042] $2,739,767.94 total cost x (353 small entities / 1,989 total entities) = $486,243.38.

As discussed above, there are approximately 195 small entity broker-dealers that would be subject to the additional disclosure requirements under proposed Rule 10 for customers of Covered Broker-Dealers. This would create a new annual burden of approximately 51.26 hours per Covered Entity, or 9,995.7 hours in aggregate for small entities. The Commission therefore expects the annual monetized aggregate cost to small entities associated with the proposed disclosure requirements for Covered Broker-Dealers to be $689,703.30.[1043]

2. Rules 17a-4, 17ad-7, and 18a-6

The proposed amendments to Rules 17a-4, 17ad-7, and 18a-6 would impose certain recordkeeping requirements, which—with respect to 17a-4 and 17ad-7—includes requirements for those that are small entities.[1044] The proposed amendments are discussed above in detail,[1045] and the requirements and the burdens on respondents, including those that are small entities, are discussed above in the economic analysis and PRA, respectively.[1046]

There are approximately 353 small entities that would be subject to the proposed amendments to Rules 17a-4 and 17ad-7 as Covered Entities. As discussed above in the PRA analysis in section V, the proposed amendments to Rules 17a-4 and 17ad-7 would require Market Entities to retain certain copies of documents required under proposed Rule 10, and would create a new annual burden of approximately 6 hours per entity, or 2,118 hours in aggregate for small entities. The Commission therefore expects the annual monetized aggregate cost to small entities associated with the proposed amendments would be $155,673.[1047]

As discussed above, there are approximately 569 small entity broker-dealers that would be subject to the proposed amendments to Rule 17a-4 as Non-Covered Broker-Dealers. As

---

1043 $5,450,424.54 total cost x (195 small entities / 1,541 total entities) = $689,703.30.

1044 *See* section VI.A.3. of this release.

1045 *See* sections II.B.5. and II.C. of this release

1046 *See* sections IV and V of the release.

1047 $877,149 total cost x (353 small entities / 1,989 total entities) = $155,673.

discussed above in the PRA analysis, in section V, the proposed amendments to Rule 17a-4 would require Market Entities to retain certain copies of documents required under proposed Rule 10, which would create a new annual burden of approximately 3 hours per entity, or 1,707 hours in aggregate for small entities. The Commission therefore expects the annual monetized aggregate cost to small entities associated with the proposed amendments would be $125,464.50.[1048]

E. Duplicative, Overlapping, or Conflicting Federal Rules

1. Proposed Rule 10 and Parts I and II of Proposed Form SCIR

As discussed above certain broker-dealers—including an operator of an ATS—and transfer agents would be small entities. Proposed Rule 10 would require all Market Entities to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks, and, at least annually, review and assess the design and effectiveness of these policies and procedures.[1049] As discussed earlier, broker-dealers are subject to Regulation S-P and Regulation S-ID.[1050] In addition, ATSs that trade certain stocks exceeding specific volume thresholds are subject to Regulation SCI. Further, an ATS is subject to Regulation ATS. Transfer agents registered with the Commission (but not transfer agents registered with another appropriate regulatory agency) are subject to the Regulation S-P Disposal Rule.[1051] Transfer agents also may be subject to Regulation S-ID if they are "financial institutions" or "creditors."[1052]

1048 $434,164.50 total cost x (569 small entities / 1,969 total entities) = $125,464.50.

1049 *See* paragraphs (b)(1) and (e)(1) of proposed Rule 10 (requiring Covered Entities and Non-Covered Broker-Dealers, respectively, to have policies and procedures to address their cybersecurity risks); sections II.B.1. and II.C.1. of this release (discussing the requirements of paragraphs (b)(1) and (e)(1) of proposed Rule 10 in more detail).

1050 *See* section IV.C.1.b.i. of this release (discussing current relevant regulations applicable to broker-dealers).

1051 *See* section IV.C.1.b.v. of this release (discussing current relevant regulations applicable to transfer agents).

1052 *See* 17 CFR 248.201 and 202. The scope of Regulation S-ID includes any financial institution or creditor, as defined in the Fair Credit Reporting Act (15 U.S.C. 1681) that is required to be "registered under the Securities Exchange Act of 1934." *See* 17 CFR 248.201(a).

As discussed earlier, these other regulations have provisions that require policies and procedures that address certain cybersecurity risks.[1053] However, the policies and procedures requirements of proposed Rule 10 are intended to differ in scope and purpose from those other regulations, and because the policies and procedures required under proposed Rule 10 are consistent with the existing and proposed requirements of those other regulations that pertain to cybersecurity.

Proposed Rule 10 would require all Market Entities to give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring.[1054] Covered Entities—in addition to providing the Commission with immediate written electronic notice of a significant cybersecurity incident—would need to report and update information about the significant cybersecurity incident by filing Part I of proposed Form SCIR with the Commission.[1055] Recently, the OCC, Federal Reserve Board, and FDIC adopted a new rule that would require certain banking organizations to notify the appropriate banking regulator of any cybersecurity incidents within 36 hours of discovering an incident.[1056] Certain transfer agents are banking organizations and, therefore, may be required to provide notification to the Commission and other regulators under proposed Rule 10 and to their banking regulator under this new rule if they experience a significant cybersecurity incident.[1057] However, the burdens of providing these notices are minor and each requirement is designed to alert separate regulators who have

---

1053 *See* section II.F.1.c. of this release.

1054 *See* paragraph (c)(1) of proposed Rule 10; paragraph (e)(2) of proposed Rule 10. *See also* sections II.B.2.a. and II.C. of this release (discussing these proposed requirements in more detail).

1055 *See* sections II.B.2. and II.B.4. of this release (discussing these proposed requirements in more detail).

1056 *See* section IV.C.1.d. of this release (discussing this requirement in more detail).

1057 Similarly, to the extent that a Covered Entity is subject to NFA rules, there may be overlapping notification requirements. *See* NFA Interpretive Notice 9070 - NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs (effective March 1, 2016; April 1, 2019 and September 30, 2019) *available at* https://www.nfa.futures.org/rulebook/rules.aspx?RuleID=9070&Section=9.

oversight responsibilities with respect to transfer agents about cybersecurity incidents that could adversely impact the transfer agent.

Proposed Rule 10 would require a Covered Entity to make two types of public disclosures relating to cybersecurity on Part II of proposed Form SCIR.[1058] Covered Entities would be required to make the disclosures by filing Part II of proposed Form SCIR on EDGAR and posting a copy of the filing on their business Internet websites.[1059] In addition, a Covered Entity that is either a carrying or introducing broker-dealer would be required to provide a copy of the most recently filed Part II of Form SCIR to a customer as part of the account opening process. Thereafter, the carrying or introducing broker-dealer would need to provide the customer with the most recently filed form annually. Regulation SCI requires that SCI entities disseminate information to their members, participants, or customers (as applicable) regarding SCI events, including systems intrusions.[1060]

Consequently, a Covered Entity would, if it experiences a "significant cybersecurity incident," be required to make updated disclosures under proposed Rule 10 by filing Part II of proposed Form SCIR on EDGAR, posting a copy of the form on its business Internet website, and, in the case of a carrying or introducing broker-dealer, by sending the disclosure to its customers using the same means that the customer elects to receive account statements. Moreover, if Covered Entity is an SCI entity and the significant cybersecurity incident is or would be an SCI event under the current or proposed requirements of Regulation SCI, the Covered Entity also could be required to disseminate certain information about the SCI event to certain of its members, participants, or customers (as applicable).

As discussed above, proposed Rule 10 and Regulation SCI require different types of information to be disclosed. In addition, the disclosures, for the most part, would be made to

---

1058 *See* paragraph (d)(1) of proposed Rule 10.

1059 *See* section II.B.3.b. of this release (discussing these proposed requirements in more detail).

1060 *See* 17 CFR 242.1002(c).

different persons: (1) the public at large in the case of proposed Rule 10;[1061] and (2) affected members, participants, or customers (as applicable) of the SCI entity in the case of Regulation SCI. For these reasons, the Commission proposes to apply the disclosure requirements of proposed Rule 10 to Covered Entities even if they would be subject to the disclosure requirements of Regulation SCI.

2. Rules 17a-4, 17ad-7, 18a-6 and Clearing Agency Exemption Orders

As part of proposed Rule 10, the Commission is proposing corresponding amendments to the books and records rules for Market Entities. There are no duplicative, overlapping, or conflicting Federal rules with respect to the proposed amendments to Rules 17a-4, 17ad-7, 18a-6 and clearing agency exemption orders.

F. Significant Alternatives

The RFA directs the Commission to consider significant alternatives that would accomplish our stated objectives, while minimizing any significant adverse effect on small entities.

1. Broker-Dealers

As discussed above, the proposal would apply to all registered broker-dealers. Under the proposal, the following broker-dealers would be Covered Entities: (1) broker-dealers that maintain custody of securities and cash for customers or other broker-dealers (*i.e.*, carrying broker-dealers); (2) broker-dealers that introduce their customer accounts to a carrying broker-dealer on a fully disclosed basis (*i.e.*, introducing broker-dealers); (3) broker-dealers with regulatory capital equal to or exceeding $50 million; (4) broker-dealers with total assets equal to or exceeding $1 billion; (5) broker-dealers that operate as market makers; and (6) broker-dealers that operate an ATS. Broker-dealers that do not fit into at least one of these categories would not

---

[1061] A carrying broker-dealer would be required to make the disclosures to its customers as well through the means by which they receive account statements.

be Covered Entities (*i.e.*, they would be Non-Covered Broker-Dealers). As discussed earlier, Covered Entities would be subject to additional requirements under proposed Rule 10.[1062]

Of the 1,541 broker-dealers that would be Covered Entities, approximately 195 are considered small entities. All but one of these small entities are broker-dealers that introduce their customer accounts to a carrying broker-dealer on a fully disclosed basis. The remaining small entity broker-dealer is an operator of an ATS. The Commission considered the following alternatives for small entities that are Covered Broker-Dealers in relation to the proposal: (1) differing compliance or reporting requirements that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the proposed rule for such small entities; (3) the use of design rather than performance standards; and (4) an exemption from coverage of the proposed rule, or any part thereof, for such small entities.

Regarding the first and fourth alternatives, the Commission decided not to include differing requirements or exemptions for introducing broker-dealers, regardless of size, and therefore, they would be Covered Entities under the proposed rule. This decision was based on a number of considerations.[1063] For example, introducing broker-dealers are a conduit to their customers' accounts at the carrying broker-dealer and have access to information and trading systems of the carrying broker-dealer. Consequently, a cybersecurity incident at an introducing firm could directly harm the introducing firm's customers to the extent it causes them to lose access to the systems allowing them to view and transact in their securities accounts at the carrying broker-dealer. Further, a significant cybersecurity incident at an introducing broker-dealer could spread to the carrying broker-dealer given the information systems that connect the

---

[1062] *See* paragraphs (b), (c), and (d) of proposed Rule 10 (setting forth the requirements for Covered Entities); paragraph (e) of proposed Rule 10 (setting forth the requirements for Non-Covered Broker-Dealers).

[1063] *See* section II.A.1.b. of this release (discussing why introducing broker-dealers would be Covered Entities in more detail).

two firms. These connections also may make introducing broker-dealers attractive targets for threat actors seeking to access the information systems of the carrying broker-dealer to which the introducing broker-dealer is connected. In addition, introducing broker-dealers may store personal information about their customers on their information systems or be able to access this information on the carrying broker-dealer's information systems. If this information is accessed or stolen by unauthorized users, it could result in harm (*e.g.*, identity theft or conversion of financial assets) to many individuals, including retail investors.

The Commission decided not to include differing requirements or exemptions for broker-dealers that operate an ATS, regardless of size, and therefore, they would be Covered Entities under the proposed rule. This decision was based on a number of considerations.[1064] The Commission also decided to include all broker-dealers, regardless of size, that operate an ATS as Covered Entities in the proposed rule because ATSs have become increasingly important venues for trading securities in a fast and automated manner. ATSs perform exchange functions to bring together buyers and sellers using limit order books and order types. These developments have made ATSs significant sources of orders and trading interest for securities. ATSs use data feeds, algorithms, and connectivity to perform their functions. In this regard, ATSs rely heavily on information systems, including to connect to other Market Entities such as other broker-dealers and principal trading firms. A significant cyber security incident that disrupts a broker-dealer that operates as an ATS could negatively impact the ability of investors to liquidate or purchase certain securities at favorable or predictable prices or in a timely manner to the extent the ATS provides liquidity to the market for those securities. Further, a significant cybersecurity incident at an ATS could provide a gateway for threat actors to attack other Market Entities that connect to it through information systems and networks of interconnected information systems. This

---

[1064] *See* section II.A.1.b. of this release (discussing why broker-dealers that operate an ATS would be Covered Entities in more detail).

could cause a cascading effect where a significant cybersecurity incident initially impacting an ATS spreads to other Market Entities causing major disruptions to the U.S. securities markets. In addition, ATS are connected to a number of different Market Entities through information systems, including national securities exchanges and other broker-dealers. Therefore, they create and are exposed to cybersecurity risk through the channels of these information systems.

Regarding the second alternative, the Commission believes the current proposal is clear and that further clarification, consolidation, or simplification of the compliance requirements is not necessary for small entities that are introducing broker-dealers or broker-dealers that operate as ATSs. As discussed above, proposed Rule 10 would require Covered Entities to establish, maintain, and enforce written cybersecurity policies and procedures that are reasonably designed to address their cybersecurity risks and that specifically address: (1) risk assessment; (2) user security and access; (3) information protection; (4) cybersecurity threat and vulnerability management; and (5) cybersecurity incident response and recovery.[1065] It also would require Covered Entities to conduct an annual review and assessment of these policies and procedures and produce a report documenting the review and assessment. Further, the proposed rule would require them to provide immediate notification and subsequent reporting of significant cybersecurity incidents and to publicly disclose summary descriptions of their cybersecurity risks and, if applicable, summary descriptions of their significant cybersecurity incidents.[1066] The proposed rule would provide clarity in the existing regulatory framework regarding cybersecurity and serve as an explicit requirement for firms to establish, maintain, and enforce comprehensive cybersecurity programs to their address cybersecurity risks, provide information to the

---

[1065] *See* paragraph (b) of proposed Rule 10. *See also* section II.B.1. of this release (discussing these requirements in more detail).

[1066] *See* paragraphs (c) and (d) of proposed Rule 10. *See also* sections II.B.2. through II.B.4. of this release (discussing these requirements in more detail).

Commission about the significant cybersecurity incidents they experience, and publicly disclose information about their cybersecurity risks and significant cybersecurity incidents.

Regarding the third alternative, the Commission determined to use performance standards rather than design standards. Although the proposed rule requires Covered Entities to implement policies and procedures that are reasonably designed and that must include certain elements, the Commission does not place certain conditions or restrictions on how to establish, maintain, and enforce such policies and procedures. The general elements required to be included in the policies and procedures are designed to enumerate the core areas that firms would need to address when adopting, implementing, reassessing and updating their cybersecurity policies and procedures.

The policies and procedures that would be required by proposed Rule 10—because they would need to address the Covered Entity's cybersecurity risks—generally should be tailored to the nature and scope of the Covered Entity's business and address the Covered Entity's specific cybersecurity risks. Thus, proposed Rule 10 is not intended to impose a one-size-fits-all approach to addressing cybersecurity risks. In addition, cybersecurity threats are constantly evolving and measures to address those threats continue to evolve. Therefore, proposed Rule 10 is designed to provide Covered Entities with the flexibility to update and modify their policies and procedures as needed so that that they continue to be reasonably designed to address the Covered Entity's cybersecurity risks over time.

The remaining 569 small entity broker-dealers registered would not be Covered Entities. These firms are not conduits to their customer accounts at a carrying broker-dealer. These firms also do not perform exchange-like functions such as offering limit order books and other order types, like an ATS would. As such, these firms are subject to differing compliance, reporting, and disclosure requirements that take into account the resources available to the entities. For example, these firms are subject to simplified requirements concerning their cybersecurity

policies and procedures and annual review.[1067] In addition, these firms are exempted from the cybersecurity reporting and disclosure requirements that apply to Covered Entities.

2. Clearing Agencies

For the reasons stated above, this requirement is not applicable to clearing agencies.

3. The MSRB

For the reasons stated above, this requirement is not applicable to the MSRB.

4. National Securities Exchanges and National Securities Associations

For the reasons stated above, this requirement is not applicable to national securities exchanges and national securities associations.

5. SBS Entities

For the reasons stated above, this requirement is not applicable to SBS Entities.

6. SBSDRs

For the reasons stated above, this requirement is not applicable to SBSDRs.

7. Transfer Agents

The proposed rule would apply to every transfer agent as defined in section 3(a)(25) of the Exchange Act that is registered or required to be registered with an appropriate regulatory agency as defined in section 3(a)(34)(B) of the Exchange Act. As of December 31, 2022, there were 353 transfer agents that were either registered with the Commission through Form TA-1 or registered with other appropriate regulatory agencies through Form TA-2. As of March 31, 2022, the Commission estimates there were 158 transfer agents that were considered small organizations.

[1067] Non-Covered Broker-Dealers that are small entities are not, however, altogether exempted from the policies and procedures requirements because having appropriate cybersecurity policies and procedures in place would help address any cybersecurity risks and incidents that occur at the broker-dealer and help protect broker-dealers and their customers from greater risk of harm. The Commission anticipates that these benefits should apply to customers of smaller firms as well as larger firms. Non-Covered Broker-Dealers are also not exempted from the requirement to provide the Commission with immediate written electronic notice of a significant cybersecurity incident affecting the entity.

The Commission considered the following alternatives for small organizations that are transfer agents in relation to the proposal: (1) differing compliance or reporting requirements that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the proposed rule for such small entities; (3) the use of design rather than performance standards; and (4) an exemption from coverage of the proposed rule, or any part thereof, for such small entities.

Regarding the first and fourth alternatives, the Commission decided not to include differing requirements or exemptions for transfer agents, regardless of size, and therefore, they would be Covered Entities under the proposed rule. This decision was based on a number of considerations.[1068] A transfer agents engage on behalf of an issuer of securities or on behalf of itself as an issuer of securities in (among other functions): (1) tracking, recording, and maintaining the official record of ownership of each issuer's securities; (2) canceling old certificates, issuing new ones, and performing other processing and recordkeeping functions that facilitate the issuance, cancellation, and transfer of those securities; (3) facilitating communications between issuers and registered securityholders; and (4) making dividend, principal, interest, and other distributions to securityholders. Their core recordkeeping systems provide a direct conduit to their issuer clients' master records that document and, in many instances provide the legal underpinning for, registered securityholders' ownership of the issuer's securities. If these functions were disrupted, investors might not be able to transfer ownership of their securities or receive dividends and interest due on their securities positions.

Transfer agents store proprietary information about securities ownership and corporate actions. A significant cybersecurity incident at a transfer agent could lead to the improper use of this information to harm securities holders (*e.g.*, public exposure of confidential financial

---

[1068] *See* section II.A.1.c. of this release (discussing why transfer agents would be Covered Entities in more detail).

information) or provide the unauthorized user with an unfair advantage over other market participants (*e.g.*, trading based on confidential business information). Transfer agents also may store personal information including names, addresses, phone numbers, email addresses, employers, employment history, bank and specific account information, credit card information, transaction histories, securities holdings, and other detailed and individualized information related to the transfer agents' recordkeeping and transaction processing on behalf of issuers. Threat actors breaching the transfer agent's information systems could use this information to steal identities or financial assets of the persons to whom this information pertains. They also could sell it to other threat actors.

Regarding the second alternative, the Commission is not proposing further clarification, consolidation, or simplification of the compliance requirements for small organizations that are transfer agents. As discussed above, proposed Rule 10 would require Covered Entities to establish, maintain, and enforce written cybersecurity policies and procedures that are reasonably designed to address their cybersecurity risks and that specifically address: (1) risk assessment; (2) user security and access; (3) information protection; (4) cybersecurity threat and vulnerability management; and (5) cybersecurity incident response and recovery.[1069] It also would require Covered Entities to conduct an annual review and assessment of these policies and procedures and produce a report documenting the review and assessment. Further, the proposed rule would require them to provide immediate notification and subsequent reporting of significant cybersecurity incidents and to publicly disclose summary descriptions of their cybersecurity risks and, if applicable, summary descriptions of their significant cybersecurity incidents.[1070] The proposed rule would provide clarity in the existing regulatory framework regarding cybersecurity

---

[1069] *See* paragraph (b) of proposed Rule 10. *See also* section II.B.1. of this release (discussing these requirements in more detail).

[1070] *See* paragraphs (c) and (d) of proposed Rule 10. *See also* sections II.B.2. through II.B.4. of this release (discussing these requirements in more detail).

and serve as an explicit requirement for firms to establish, maintain, and enforce comprehensive cybersecurity programs to their address cybersecurity risks, provide information to the Commission about the significant cybersecurity incidents they experience, and publicly disclose information about their cybersecurity risks and significant cybersecurity incidents.

Regarding the third alternative, the proposed rule requires Covered Entities to implement policies and procedures that are reasonably designed and that must include certain elements. However, the proposed rule does not place certain conditions or restrictions on how to establish, maintain, and enforce such policies and procedures. The general elements required to be included in the policies and procedures are designed to enumerate the core areas that firms would need to address when adopting, implementing, reassessing and updating their cybersecurity policies and procedures.

The policies and procedures that would be required by proposed Rule 10—because they would need to address the Covered Entity's cybersecurity risks—generally should be tailored to the nature and scope of the Covered Entity's business and address the Covered Entity's specific cybersecurity risks. Thus, proposed Rule 10 is not intended to impose a one-size-fits-all approach to addressing cybersecurity risks. In addition, cybersecurity threats are constantly evolving and measures to address those threats continue to evolve. Therefore, proposed Rule 10 is designed to provide Covered Entities with the flexibility to update and modify their policies and procedures as needed so that that they continue to be reasonably designed to address the Covered Entity's cybersecurity risks over time.

G. Request for Comment

The Commission encourages written comments on the matters discussed in this IRFA. The Commission solicits comment on the number of small entities subject to the proposed Rule 10, Form SCIR, and proposed amendments to Rules 3a71-6, 17a-4, 18a-6, and 17ad-7. The Commission also solicits comment on the potential effects discussed in this analysis; and whether this proposal could have an effect on small entities that have not been considered. The

Commission requests that commenters describe the nature of any effect on small entities and provide empirical data to support the extent of such effect. Such comments will be placed in the same public file as comments on the proposed rule and form and associated amendments. Persons wishing to submit written comments should refer to the instructions for submitting comments located at the front of this release.

VII. SMALL BUSINESS REGULATORY ENFORCEMENT FAIRNESS ACT

For purposes of the Small Business Regulatory Enforcement Fairness Act of 1996, or "SBREFA," the Commission must advise OMB whether a proposed regulation constitutes a "major" rule. Under SBREFA, a rule is considered "major" where, if adopted, it results in or is likely to result in (1) an annual effect on the economy of $100 million or more; (2) a major increase in costs or prices for consumers or individual industries; or (3) significant adverse effects on competition, investment or innovation. The Commission requests comment on the potential effect of the proposed amendments on the U.S. economy on an annual basis; any potential increase in costs or prices for consumers or individual industries; and any potential effect on competition, investment or innovation. Commenters are requested to provide empirical data and other factual support for their views to the extent possible.

VIII. STATUTORY AUTHORITY

The Commission is proposing new Rule 10 (17 CFR 242.10) and Form SCIR (17 CFR 249.624) and amending Regulation S-T (17 CFR 232.101), Rule 3a71-6 (17 CFR 240.3a71-6), Rule 17a-4 (17 CFR 240.17a-4), Rule 17ad-7 (17 CFR 240.17ad-7), Rule 18a-6 (17 CFR 18a-6), and Rule 18a-10 (17 CFR 240.18a-10) under the Commission's rulemaking authority set forth in the following sections of the Exchange Act: (1) sections 15, 17, and 23 for broker-dealers (15 U.S.C. 78*o*, 78q, and 78w); (2) sections 17, 17A, and 23 for clearing agencies (15 U.S.C. 78q, 17q-1, and 78w(a)(1)); (3) sections 15B, 17 and 23 for the MSRB (15 U.S.C. 78*o*–4, 78q(a), and 78w); (4) sections 6(b), 11A, 15A, 17, and 23 for national securities exchanges and national securities associations (15 U.S.C. 78f, 78k-1, 78*o*-3, and 78w); (5) sections 15F, 23, and 30(c)

for SBS Entities (15 U.S.C. 78*o*-10, 78w, and 78dd(c)); (6) sections 13 and 23 for SBSDRs (15 U.S.C. 78m and 78w); and (7) sections 17a, 17A, and 23 for transfer agents (78q, 17q-1, and 78w).

List of Subjects in 17 CFR Part 232, 240, 242 and 249

Brokers, Confidential business information, Reporting and recordkeeping requirements, Securities, Security-based swaps, Security-based swap dealers, Major security-based swap participants.

Text of Proposed Rules and Rule Amendments

For the reasons set out in the preamble, the Commission is proposing to amend title 17, chapter II of the Code of Federal Regulations as follows:

PART 232 – REGULATION S-T – GENERAL RULES AND REGULATIONS FOR ELECTRONIC FILINGS

1. The general authority citation for part 232 is revised to read as follows:

Authority: 15 U.S.C. 77c, 77f, 77g, 77h, 77j, 77s(a), 77z-3, 77sss(a), 78c(b), 78*l*, 78m, 78n, 78o(d), 78o-10, 78w(a), 78*ll*, 80a-6(c), 80a-8, 80a-29, 80a-30, 80a-37, 80b-4, 80b-10, 80b-11, 7201 *et seq.*; and 18 U.S.C. 1350, unless otherwise noted.

* * * * *

2. Section § 232.101 is amended by revising paragraph (a)(1)(xxx) and adding paragraph (a)(1)(xxxi) to read as follows:

§ 232.101 Mandated electronic submissions and exceptions.

(a) * * *

(1) * * *

(xxx) Documents filed with the Commission pursuant to section 33 of the Investment Company Act (15 U.S.C. 80a-32); and

(xxxi) Form SCIR (§ 249.624 of this chapter).

* * * * *

PART 240 – GENERAL RULES AND REGULATIONS, SECURITIES EXCHANGE ACT OF 1934

3. The authority citation for part 240 continues to read, in part, as follows:

Authority: 15 U.S.C. 77c, 77d, 77g, 77j, 77s, 77z-2, 77z-3, 77eee, 77ggg, 77nnn, 77sss, 77ttt, 78c, 78c-3, 78c-5, 78d, 78e, 78f, 78g, 78i, 78j, 78j-1, 78k, 78k-1, 78l, 78m, 78n, 78n-1, 78o, 78o-4, 78o-10, 78p, 78q, 78q-1, 78s, 78u-5, 78w, 78x, 78ll, 78mm, 80a-20, 80a-23, 80a-29, 80a-37, 80b-3, 80b-4, 80b-11, and 7201 et. seq., and 8302; 7 U.S.C. 2(c)(2)(E); 12 U.S.C. 5221(e)(3); 18 U.S.C. 1350; Pub. L. 111-203, 939A, 124 Stat. 1376 (2010); and Pub. L. 112-106, sec. 503 and 602, 126 Stat. 326 (2012), unless otherwise noted.

* * * * *

4. Section 240.3a71-6 is amended by revising paragraph (d)(1) to read as follows:

§ 240.3a71–6 Substituted compliance for security-based swap dealers and major security-based swap participants.

* * * * *

(d) * * *

(1) *Business conduct, supervision, and risk management.* The business conduct and supervision requirements of sections 15F(h) and (j) of the Act (15 U.S.C. 78o-10(h) and (j)) and §§ 240.15Fh-3 through 15Fh-6 (other than the antifraud provisions of section 15F(h)(4)(A) of the Act and § 240.15Fh-4(a), and other than the provisions of sections 15F(j)(3) and 15F(j)(4)(B) of the Act), and the requirements of § 242.10 of this chapter and Form SCIR (§ 249.624 of this chapter); provided, however, that prior to making such a substituted compliance determination the Commission intends to consider whether the information that is required to be provided to counterparties pursuant to the requirements of the foreign financial regulatory system, the counterparty protections under the requirements of the foreign financial regulatory system, the mandates for supervisory systems under the requirements of the foreign financial regulatory system, and the duties imposed by the foreign financial regulatory system, are comparable to

those associated with the applicable provisions arising under the Act and its rules and regulations.

* * * * *

5. Section 240.17a-4 is amended by adding paragraph (e)(13) to read as follows:

§ 240.17a-4 Records to be preserved by certain exchange members, brokers and dealers.

* * * * *

(e) * * *

(13)(i) The written policies and procedures required to be adopted and implemented pursuant to § 242.10(b)(1) or § 242.10(e)(1) of this chapter until three years after the termination of the use of the policies and procedures;

(ii) The written documentation of any risk assessment pursuant to § 242.10(b)(1)(i)(B) of this chapter for three years;

(iii) The written documentation of the occurrence of a cybersecurity incident pursuant to § 242.10(b)(1)(v)(B) of this chapter, including any documentation related to any response and recovery from such an incident, for three years;

(iv) The written report of the annual review required to be prepared pursuant to § 242.10(b)(2)(ii) of this chapter or the record of the annual review required pursuant to § 240.10(e)(1) for three years;

(v) A copy of any notice transmitted to the Commission pursuant to § 242.10(c)(1) or § 240.10(e)(2) of this chapter or any Part I of Form SCIR filed with the Commission pursuant to § 242.10(c)(2) of this chapter for three years; and

(vi) A copy of any Part II of Form SCIR filed with the Commission pursuant to § 242.10(d) of this chapter for three years.

* * * * *

6. Redesignate § 240.17Ad-7 as § 240.17ad-7.

7. Newly redesignated § 240.17ad-7 is amended by revising the section heading, and adding paragraph (j) to read as follows:

§ 240.17ad-7 (Rule 17Ad-7) Record retention.

* * * * *

(j)(1) The written policies and procedures required to be adopted and implemented pursuant to § 242.10(b)(1) of this chapter until three years after the termination of the use of the policies and procedures;

(2) The written documentation of any risk assessment pursuant to § 242.10(b)(1)(i)(B) of this chapter for three years;

(3) The written documentation of the occurrence of a cybersecurity incident pursuant to § 242.10(b)(1)(v)(B) of this chapter, including any documentation related to any response and recovery from such an incident, for three years;

(4) The written report of the annual review required to be prepared pursuant to § 242.10(b)(2)(ii) of this chapter for three years;

(5) A copy of any notice transmitted to the Commission and any ARA pursuant to § 242.10(c)(1) of this chapter or any Part I of Form SCIR filed with the Commission pursuant to § 240.2.10(c)(2) for three years; and

(6) A copy of any Part II of Form SCIR filed with the Commission pursuant to § 240.2.10(d) for three years.

8. Section 240.18a-6 is amended by adding paragraph (d)(6) to read as follows:

§ 240.18a-6 Records to be preserved by certain security-based swap dealers and major security-based swap participants

* * * * *

(d) * * *

(6)(i) The written policies and procedures required to be adopted and implemented pursuant to § 242.10(b)(1) of this chapter until three years after the termination of the use of the policies and procedures;

(ii) The written documentation of any risk assessment pursuant to § 242.10(b)(1)(i)(B) of this chapter for three years;

(iii) The written documentation of the occurrence of a cybersecurity incident pursuant to § 242.10(b)(1)(v)(B) of this chapter, including any documentation related to any response and recovery from such an incident, for three years;

(iv) The written report of the annual review required to be prepared pursuant to § 242.10(b)(2)(ii) of this chapter for three years;

(v) A copy of any notice transmitted to the Commission pursuant to § 242.10(c)(1) of this chapter or any Part I of Form SCIR filed with the Commission pursuant to § 242.10(c)(2) of this chapter for three years; and

(vi) A copy of any Part II of Form SCIR filed with the Commission pursuant to § 242.10(d) of this chapter for three years.

* * * * *

9. Section 240.18a-10 is amended by adding paragraph (g) to read as follows:

§ 240.18a-10 Alternative compliance mechanism for security-based swap dealers that are registered as swap dealers and have limited security-based swap activities

* * * * *

(g) The provisions of this section do not apply to the record maintenance and preservation requirements § 240.18a-6(d)(6)(i) through (vi).

PART 242 - REGULATIONS M, SHO, ATS, AC, NMS, AND SBSR AND CUSTOMER MARGIN REQUIREMENTS FOR SECURITY FUTURES

10. The general authority citation for part 242 is revised to read as follows:

Authority: 15 U.S.C. 77g, 77q(a), 77s(a), 78b, 78c, 78g(c)(2), 78i(a), 78j, 78k-1(c), 78l, 78m, 78n, 78o(b), 78o(c), 78o(g), 78o-10, 78q(a), 78q(b), 78q(h), 78w(a), 78dd-1, 78mm, 80a-23, 80a-29, and 80a-37.

11. Section 242.10 is added to read as follows:

§ 242.10 Cybersecurity requirements.

(a) *Definitions*: For purposes of this section:

(1) *Covered entity* means:

(i) A broker or dealer registered with the Commission that:

(A) Maintains custody of cash and securities for customers or other brokers or dealers and is not exempt from the requirements of § 240.15c3-3 of this chapter;

(B) Introduces customer accounts on a fully disclosed basis to another broker or dealer described in paragraph (a)(1)(i)(A) of this section;

(C) Has regulatory capital equal to or exceeding $50 million;

(D) Has total assets equal to or exceeding $1 billion;

(E) Is a market maker under the Securities Exchange Act of 1934 (15 U.S.C. 78a, *et seq*.) ("Act") or the rules thereunder (which includes a broker or dealer that operates pursuant to § 240.15c3-1(a)(6) of this chapter) or is a market maker under the rules of a self-regulatory organization of which the broker or dealer is a member; or

(F) operates an alternative trading system as defined in § 242.300(a) or operates an NMS Stock ATS as defined in § 242.300(k).

(ii) A clearing agency (registered or exempt) under section 3(a)(23)(A) of the Act.

(iii) A major security-based swap participant registered pursuant to section 15F(b) of the Act.

(iv) The Municipal Securities Rulemaking Board.

(v) A national securities association registered under section 15A of the Act.

(vi) A national securities exchange registered under section 6 of the Act.

(vii) A security-based swap data repository under section 3(a)(75) of the Act.

(viii) A security-based swap dealer registered pursuant to section 15F(b) of the Act.

(ix) A transfer agent as defined in section 3(a)(25) of the Act that is registered or required to be registered with an appropriate regulatory agency as defined in section 3(a)(34)(B) of the Act (hereinafter also "ARA").

(2) *Cybersecurity incident* means an unauthorized occurrence on or conducted through a market entity's information systems that jeopardizes the confidentiality, integrity, or availability of the information systems or any information residing on those systems.

(3) *Cybersecurity risk* means financial, operational, legal, reputational, and other adverse consequences that could result from cybersecurity incidents, cybersecurity threats, and cybersecurity vulnerabilities.

(4) *Cybersecurity threat* means any potential occurrence that may result in an unauthorized effort to affect adversely the confidentiality, integrity, or availability of a market entity's information systems or any information residing on those systems.

(5) *Cybersecurity vulnerability* means a vulnerability in a market entity's information systems, information system security procedures, or internal controls, including, for example, vulnerabilities in their design, configuration, maintenance, or implementation that, if exploited, could result in a cybersecurity incident.

(6) *Information* means any records or data related to the market entity's business residing on the market entity's information systems, including, for example, personal information received, maintained, created, or processed by the market entity.

(7) *Information systems* means the information resources owned or used by the market entity, including, for example, physical or virtual infrastructure controlled by the information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the covered entity's information to maintain or support the covered entity's operations.

(8) *Market Entity* means a "covered entity" as defined in this section and a broker or dealer registered with the Commission that is not a "covered entity" as defined in this section.

(9) *Personal information* means any information that can be used, alone or in conjunction with any other information, to identify a person, including, but not limited to, name, date of birth, place of birth, telephone number, street address, mother's maiden name, Social Security number,

government passport number, driver's license number, electronic mail address, account number, account password, biometric records, or other non-public authentication information.

(10) *Significant cybersecurity incident* means a cybersecurity incident, or a group of related cybersecurity incidents, that:

(i) Significantly disrupts or degrades the ability of the market entity to maintain critical operations; or

(ii) Leads to the unauthorized access or use of the information or information systems of the market entity, where the unauthorized access or use of such information or information systems results in or is reasonably likely to result in:

(A) Substantial harm to the market entity; or

(B) Substantial harm to a customer, counterparty, member, registrant, or user of the market entity, or to any other person that interacts with the market entity.

(b)(1) *Cybersecurity policies and procedures*. A covered entity must establish, maintain, and enforce written policies and procedures that are reasonably designed to address the covered entity's cybersecurity risks, including policies and procedures that:

(i)(A) *Risk assessment*. Require periodic assessments of cybersecurity risks associated with the covered entity's information systems and information residing on those systems, including requiring the covered entity to:

(*1*) Categorize and prioritize cybersecurity risks based on an inventory of the components of the covered entity's information systems and information residing on those systems and the potential effect of a cybersecurity incident on the covered entity; and

(*2*) Identify the covered entity's service providers that receive, maintain, or process information, or are otherwise permitted to access the covered entity's information systems and any of the covered entity's information residing on those systems, and assess the cybersecurity risks associated with the covered entity's use of these service providers.

(B) Require written documentation of the risk assessments.

(ii) *User security and access*. Require controls designed to minimize user-related risks and prevent unauthorized access to the covered entity's information systems and the information residing on those systems, including:

(A) Requiring standards of behavior for individuals authorized to access the covered entity's information systems and the information residing on those systems, such as an acceptable use policy;

(B) Identifying and authenticating individual users, including but not limited to implementing authentication measures that require users to present a combination of two or more credentials for access verification;

(C) Establishing procedures for the timely distribution, replacement, and revocation of passwords or methods of authentication;

(D) Restricting access to specific information systems of the covered entity or components thereof and the information residing on those systems solely to individuals requiring access to the systems and information as is necessary for them to perform their responsibilities and functions on behalf of the covered entity; and

(E) Securing remote access technologies.

(iii) *Information protection*. (A) Require measures designed to monitor the covered entity's information systems and protect the information residing on those systems from unauthorized access or use, based on a periodic assessment of the covered entity's information systems and the information that resides on the systems that takes into account:

(*1*) The sensitivity level and importance of the information to the covered entity's business operations;

(*2*) Whether any of the information is personal information;

(*3*) Where and how the information is accessed, stored and transmitted, including the monitoring of information in transmission;

(*4*) The information systems' access controls and malware protection; and

(5) The potential effect a cybersecurity incident involving the information could have on the covered entity and its customers, counterparties, members, or users, including the potential to cause a significant cybersecurity incident.

(B) Require oversight of service providers that receive, maintain, or process the covered entity's information, or are otherwise permitted to access the covered entity's information systems and the information residing on those systems, pursuant to a written contract between the covered entity and the service provider, through which the service providers are required to implement and maintain appropriate measures, including the practices described in paragraphs (b)(1)(i) through (v) of this section, that are designed to protect the covered entity's information systems and information residing on those systems.

(iv) *Cybersecurity threat and vulnerability management*. Require measures designed to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to the covered entity's information systems and the information residing on those systems;

(v) *Cybersecurity incident response and recovery*. (A) Require measures designed to detect, respond to, and recover from a cybersecurity incident, including policies and procedures that are reasonably designed to ensure:

(*1*) The continued operations of the covered entity;

(*2*) The protection of the covered entity's information systems and the information residing on those systems;

(*3*) External and internal cybersecurity incident information sharing and communications; and

(*4*) The reporting of significant cybersecurity incidents pursuant to paragraph (c) of this section.

(B) Require written documentation of any cybersecurity incident, including the covered entity's response to and recovery from the cybersecurity incident.

(2) *Annual Review*. A covered entity must, at least annually:

(i) Review and assess the design and effectiveness of the cybersecurity policies and procedures required by paragraph (b)(1) of this section, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review; and

(ii) Prepare a written report that describes the review, the assessment, and any control tests performed, explains their results, documents any cybersecurity incident that occurred since the date of the last report, and discusses any material changes to the policies and procedures since the date of the last report.

(c) *Notification and reporting of significant cybersecurity incidents*—(1) *Immediate notice*. A covered entity must give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring. The notice must identify the covered entity, state that the notice is being given to alert the Commission of a significant cybersecurity incident impacting the covered entity, and provide the name and contact information of an employee of the covered entity who can provide further details about the significant cybersecurity incident. The notice also must be given to:

(i) In the case of a broker or dealer, the examining authority of the broker or dealer; and

(ii) In the case of a transfer agent, the ARA of the transfer agent.

(2) *Report*. (i) A covered entity must report a significant cybersecurity incident, promptly, but no later than 48 hours, upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring by filing Part I of Form SCIR with the Commission electronically through the Electronic Data Gathering, Analysis, and Retrieval System ("EDGAR system") in accordance with the EDGAR Filer Manual, as defined in Rule 11 of Regulation S-T (17 CFR 232.11), and Part I of Form SCIR must be filed in accordance with the requirements of Regulation S-T.

(ii) A covered entity must file an amended Part I of Form SCIR with the Commission electronically through the EDGAR system in accordance with the EDGAR Filer Manual, as

defined in Rule 11 of Regulation S-T (17 CFR 232.11), and Part I of Form SCIR must be filed in accordance with the requirements of Regulation S-T promptly, but no later than 48 hours after each of the following circumstances:

(A) Any information previously reported to the Commission on Part I of Form SCIR pertaining to a significant cybersecurity incident becoming materially inaccurate;

(B) Any new material information pertaining to a significant cybersecurity incident previously reported to the Commission on Part I of Form SCIR being discovered;

(C) A significant cybersecurity incident is resolved; or

(D) An internal investigation pertaining to a significant cybersecurity incident is closed.

(iii)(A) If the covered entity is a broker or dealer, it must promptly transmit a copy of each Part I of Form SCIR it files with the Commission to its examining authority; and

(B) If the covered entity is a transfer agent, it must promptly transmit a copy of each Part I of Form SCIR it files with the Commission to its ARA.

(d) *Disclosure of cybersecurity risks and incidents*—(1) *Content of the disclosure*—(i) *Cybersecurity risks*. A covered entity must provide a summary description of the cybersecurity risks that could materially affect the covered entity's business and operations and how the covered entity assesses, prioritizes, and addresses those cybersecurity risks.

(ii) *Significant cybersecurity incidents*. A covered entity must provide a summary description of each significant cybersecurity incident that has occurred during the current or previous calendar year. The description of each significant cybersecurity incident must include the following information to the extent known:

(A) The person or persons affected;

(B) The date the incident was discovered and whether it is ongoing;

(C) Whether any data was stolen, altered, or accessed or used for any other unauthorized purpose;

(D) The effect of the incident on the covered entity's operations; and

(E) Whether the covered entity, or service provider, has remediated or is currently remediating the incident.

(2) *Methods of disclosure*. A covered entity must make the disclosures required pursuant to paragraph (d)(1) of this section by:

(i) Filing Part II of Form SCIR with the Commission electronically through the EDGAR system in accordance with the EDGAR Filer Manual, as defined in Rule 11 of Regulation S-T (17 CFR 232.11), and in accordance with the requirements of Regulation S-T; and

(ii) Posting a copy of the Part II of Form SCIR most recently filed pursuant to paragraph (d)(2)(i) of this section on an easily accessible portion of its business Internet website that can be viewed by the public without the need of entering a password or making any type of payment or providing any other consideration.

(3) *Additional methods of disclosure required for certain brokers or dealers*. In addition to the method of disclosure required by paragraph (d)(2) of this section, a broker or dealer described in paragraph (a)(1)(i) or (ii) of this section must provide a copy of the Part II of Form SCIR most recently filed pursuant to paragraph (d)(2)(i) of this section to a customer as part of the account opening process and, thereafter, annually and as required by paragraph (d)(4) of this section using the same means that the customer elects to receive account statements.

(4) *Disclosure updates*. The covered entity must promptly provide an updated disclosure through the methods required by paragraphs (d)(2) and (3) of this section if the information required to be disclosed pursuant to paragraphs (d)(1)(i) or (ii) of this section materially changes, including, in the case of paragraph (d)(1)(ii) of this section, after the occurrence of a new significant cybersecurity incident or when information about a previously disclosed significant cybersecurity incident materially changes.

(e) *Requirements for brokers or dealers that are not covered entities*. (1) A broker or dealer that is not a "covered entity" as defined in this section must establish, maintain, and enforce written policies and procedures that are reasonably designed to address the cybersecurity

risks of the broker or dealer taking into account the size, business, and operations of the broker or dealer. The broker or dealer must annually review and assess the design and effectiveness of the cybersecurity policies and procedures, including whether the policies and procedures reflect changes in cybersecurity risk over the time period covered by the review. The broker or dealer must make a written record that documents the steps taken in performing the annual review and the conclusions of the annual review.

(2) A broker or dealer that is not a "covered entity" as defined in this section must give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred or is occurring. The notice must identify the broker or dealer, state that the notice is being given to alert the Commission of a significant cybersecurity incident impacting the broker or dealer, and provide the name and contact information of an employee of the broker or dealer who can provide further details about the significant cybersecurity incident. The notice also must be given to the examining authority of the broker or dealer.

* * * * *

PART 249 – FORMS, SECURITIES EXCHANGE ACT OF 1934

12. The authority citation for part 249 continues to read, in part, as follows:

Authority: 15 U.S.C. 78a, *et seq*., unless otherwise noted.

* * * * *

13. Section 249.624 is added to read as follows:

§ 249.624 Form SCIR.

Form SCIR shall be filed by a covered entity to report a significant cybersecurity incident pursuant to the requirements of 17 CFR 242.10.

By the Commission.

Dated: March 15, 2023.

J. Matthew DeLesDernier,

Deputy Secretary.

Note: The following appendix will not appear in the Code of Federal Regulations.

Form SCIR

Significant Cybersecurity Incidents and Risks

OMB Approval	
OMB Number:	[•]
Expires:	[•]
Estimated average burden hours per response:	[•]
per amendment:	[•]

FORM SCIR INSTRUCTIONS

A. GENERAL INSTRUCTIONS

1. **FORM** – Part I of Form SCIR must be used by a covered entity to confidentially report a cybersecurity incident pursuant to the requirements of 17 CFR 242.10. Part II of Form SCIR must be used to publicly disclose cybersecurity risks and significant cybersecurity incidents pursuant to the requirements of 17 CFR 242.10.

2. **ELECTRONIC FILING** - A covered entity must file Parts I and II of Form SCIR through the EDGAR system, and must utilize the EDGAR Filer Manual (as defined in 17 CFR 232.11) to file Parts I and II of Form SCIR electronically to assure the timely acceptance and processing of the filing. Refer to 17 CFR 242.10 for other requirements with respect to filing Part I of Form SCIR with other regulators and for other requirements with respect to publicly disclosing Part II of Form SCIR.

3. **FEDERAL INFORMATION LAW AND REQUIREMENTS** - An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid control number. Sections 15F, 17(a), 17A, and 23(a) of the Exchange Act authorize the U.S. Securities and Exchange Commission ("Commission") to collect the information on Form SCIR from covered entities. *See* 15 U.S.C. §§78o-10, 78q and 78w. Filing of Parts I and II Form SCIR is mandatory. The principal purpose of Part I of Form SCIR is to report information about a significant cybersecurity incident impacting a covered entity so the Commission can respond to the incident, evaluate the operating status of the covered entity, and assess the impact the significant cybersecurity incident may have on other participants in the U.S. securities markets. The principal purpose of Part II of Form SCIR is to publicly disclose summary descriptions of the cybersecurity risks of the covered entity and summary descriptions of each significant cybersecurity incident that covered entity has experienced in the current or previous calendar year (if applicable). Any member of the public may direct to the Commission any comments concerning the accuracy of the burden estimate on this form, and any suggestions for reducing this burden. This collection of information has been reviewed by the Office of Management and Budget in accordance with the clearance requirements of 44 U.S.C. §3507. The information contained in this form is part of a system of records subject to the Privacy Act of 1974, as amended. The Commission has published in the Federal Register the Privacy Act Systems of Records Notice for these records.

4. **FORMAT**

   a. All Items must be answered and all fields requiring a response must be completed before the filing will be accepted.

   b. A covered entity must complete the execution screen certifying that Form SCIR has been executed properly and that the information contained in the form is accurate and complete before the filing will be accepted.

   c. A paper copy, with original signatures, of Part I and Part II of Form SCIR must be retained by the covered entity and be made available for inspection upon a regulatory request.

5. **EXPLANATION OF TERMS**

   a. **COVERED ENTITY** – The term "covered entity" has the same meaning as that term is defined in 17 CFR 242.10 and, as used in Form SCIR, also refers to the person filing the Form.

   b. **CYBERSECURITY INCIDENT –** The term "cybersecurity incident" has the same meaning as that term is defined in 17 CFR 242.10.

   c. **CYBERSECURITY RISK** – The term "cybersecurity risk" has the same meaning as that term is defined in 17 CFR 242.10.

   d. **INTERNAL INVESTIGATION** – The term "internal investigation" means a formal investigation of the significant cybersecurity incident by internal personnel of the covered entity or external personnel hired by the covered entity that seeks to determine any of the following: the cause of the significant cybersecurity incident; whether there was a failure to adhere to the covered entity's policies and procedures to address cybersecurity risk; or whether the covered entity's policies and procedures to address cybersecurity risk are effective.

e. **PERSONAL INFORMATION** – The term "personal information" has the same meaning as that term is defined in 17 CFR 242.10].

f. **SIGNIFICANT CYBERSECURITY INCIDENT** – The term "significant cybersecurity incident" has the same meaning as that term is defined in 17 CFR 242.10.

g. **UNIQUE IDENTIFICATION CODE** – The term "unique identification code" means a unique identification code assigned to a person by an internationally recognized standards-setting system that is recognized by the Commission pursuant to Rule 903(a) of Regulation SBSR (17 CFR 242.903(a)).

B. INSTRUCTIONS TO PART I OF FORM SCIR

1. **INITIAL REPORT** - Pursuant to the requirements of 17 CFR 242.10, a covered entity must file an initial report on Part I of Form SCIR with respect to a significant cybersecurity incident upon having a reasonable basis to conclude that the incident has occurred or is occurring.

2. **AMENDED REPORT** - Pursuant to the requirements of 17 CFR 242.10, a covered entity must file an amended report on Part I of Form SCIR with respect to a significant cybersecurity incident after each of the following circumstances:

   - Any information on a previously filed Part I of Form SCIR pertaining to the significant cybersecurity incident becomes materially inaccurate;
   - Any new material information pertaining to a significant cybersecurity incident previously reported to the Commission on Part I of Form SCIR being discovered;
   - A significant cybersecurity incident is resolved; or
   - An internal investigation pertaining to a significant cybersecurity incident is closed.

3. **FINAL REPORT** - A covered entity filing a final report on Part I of Form SCIR must indicate on the final notification if: (i) the Part I of Form SCIR is being filed because the significant cybersecurity incident has been resolved and either no internal investigation pertaining the significant cybersecurity incident is being or will be conducted or an internal investigation pertaining to the significant cybersecurity incident has been closed prior to the resolution of the incident; or (ii) the Part I of Form SCIR is being filed to report that an internal investigation pertaining to the significant cybersecurity incident has been closed and the significant cybersecurity incident is resolved. If a covered entity files a final report on Part I of Form SCIR with respect to a significant cybersecurity incident, and, thereafter, conducts an internal investigation pertaining to the significant cybersecurity incident, it must file another final report on Part I of Form SCIR when the investigation is closed pursuant to the requirements of 17 CFR 242.10.

4. **CONTACT EMPLOYEE** - The individual listed as the contact employee must be authorized by the covered entity to provide the Commission with information about the significant cybersecurity incident, and make information about the significant cybersecurity incident available to the Commission.

5. **LINE ITEMS**

   a. **Line 2** – Provide the date the covered entity had a reasonable basis to conclude that the significant cybersecurity incident had occurred or was occurring. This can be based on, for example, reviewing or receiving a record, alert, log, or notice about the incident.

   b. **Line 3.C.** – Provide the approximate date that the Covered Entity was no longer undergoing a significant cybersecurity incident.

C. INSTRUCTIONS TO PART II OF FORM SCIR

1. **PUBLIC DISSEMINATION** – Part II of Form SCIR will be publicly disseminated upon filing it with the Commission.

2. **DISCLOSURE UPDATES** - Pursuant to the requirements of 17 CFR 242.10, a covered entity must promptly provide an updated disclosure through the methods required by 17 CFR 242.10 if the information required to be disclosed pursuant to 17 CFR 242.10 materially changes, including after the occurrence of a new significant cybersecurity incident or when information about a previously disclosed significant cybersecurity incident materially changes.

The mailing address for questions and correspondence is:

The Securities and Exchange Commission
Washington, DC 20549

FORM SCIR PART I Page 1 (Execution Page)	**SIGNIFICANT CYBERSECURITY INCIDENTS** Date:_____ SEC Filer No: _____	**Official Use**	Official Use Only

WARNING	Failure to file Form SCIR as required by 17 CFR 242.10 would violate the Federal securities laws and may result in disciplinary, administrative, injunctive or criminal action. **INTENTIONAL MISSTATEMENTS OR OMISSIONS OF FACTS MAY CONSTITUTE FEDERAL CRIMINAL VIOLATIONS.** *See* 18 U.S.C. 1001 and 15 U.S.C. 78ff(a)

INITIAL REPORT ☐ **AMENDED REPORT** ☐ **FINAL AMENDED REPORT** ☐

Check the reason for filing the Final Amended Report

Incident Resolved ☐
Investigation Closed ☐

1. Information about the *covered entity:*

A. i. Full legal name:

ii. Business name if different than legal name:

B. Tax Identification No.: Covered Entity's UIC # (if any): Covered Entity's CIK #:

C. Main Address: (Do not use a P.O. Box)

Number and Street 1: Number and Street 2:

City: State: Country: Zip/Postal Code:

D. Contact Employee

Name: Phone Number: Email:

E. Type of *Covered Entity* (Check all the apply):

Broker or dealer ☐ Clearing Agency ☐ Major Security-Based Swap Participant ☐
Municipal Securities Rulemaking Board ☐ National Securities Association ☐ National Securities Exchange ☐
Security-Based Swap Dealer ☐ Security-Based Swap Data Repository ☐ Transfer Agent ☐

EXECUTION:

The undersigned certifies that this form was executed on behalf of, and with the authority of, the *covered entity*. The undersigned and *covered entity* represent that the information and statements contained herein are current, true and complete. The undersigned and *covered entity* further represent that to the extent any information previously submitted is not amended such information is current, true, and complete.

Date (MM/DD/YYYY) Full Legal Name of Covered Entity

By: Signature Name and Title of Person Signing on Covered Entity's behalf

This page must always be completed in full.

DO NOT WRITE BELOW THIS LINE – FOR OFFICIAL USE ONLY

FORM SCIR PART I Page 2	*Covered Entity* Name: _____ Date:_____ SEC Filer No: _____	**Official Use**	Official Use Only

2. The approximate date the significant cybersecurity incident was discovered: DD | MM | YYYY

3. The approximate duration of the significant cybersecurity incident:
   A. Is the incident ongoing: Yes ☐ No ☐ Unknown ☐
   B. Approximate start date of incident: DD | MM | YYYY Unknown ☐
   C. Approximate date incident was resolved: DD | MM | YYYY

4. The status of an internal investigation pertaining to the significant cybersecurity incident:
   A. Is an internal investigation being conducted: Yes ☐ No ☐
   B. If are yes, approximate date the internal investigation was closed: DD | MM | YYYY

5. Has a law enforcement or government agency (other than the Commission) been notified of the significant cybersecurity incident: Yes ☐ No ☐

   If yes, identify each law enforcement or government agency:_____

6. Describe the nature and scope of the significant cybersecurity incident, including the information systems affected by the incident and any effect on the covered entity's critical operations:

7. A. Has the threat actor(s) causing the significant cybersecurity incident been identified: Yes ☐ No ☐
   If yes, identify the threat actor(s):_____

   B. Has there been communication(s) from or with the threat actor that caused or claims to have caused the significant cyber security incident (answer even if the actor(s) has not been identified): Yes ☐ No ☐
   If yes, describe the communications:

FORM SCIR PART I Page 3	*Covered Entity* Name: _____ Date:_____ SEC Filer No: _____	**Official Use**	Official Use Only

8. Describe the actions taken or planned to respond to and recover from the significant cybersecurity incident:_____

9. Was any data stolen, altered, or accessed or used for any other unauthorized purpose: Yes ☐ No ☐ Unknown ☐
If yes, describe the nature and scope of the data:_____

10. A. Was any personal information lost, stolen, modified, deleted, destroyed, or accessed without authorization as a result of the significant cybersecurity incident: Yes ☐ No ☐ Unknown ☐

If yes, describe the nature and scope of the information:_____

B. i. If yes, has notification been provided to persons whose personal information was lost, stolen, modified, deleted, destroyed, or accessed without authorization: Yes ☐ No ☐

ii. If no, is notification planned: Yes ☐ No ☐

FORM SCIR PART I Page 4	*Covered Entity* Name: _____ Date:_____ SEC Filer No: _____	**Official Use**	Official Use Only

11. Were any assets of the covered entity lost or stolen as a result of the significant cybersecurity incident:
    Yes ☐ No ☐ Unknown ☐

    If yes, describe the types of assets that were lost or stolen and include an approximate estimate of their value, if known:__
    _____
    _____
    _____
    _____
    _____

12. A. Were any assets of the covered entity's customers, counterparties, members, registrants, or users lost or stolen as a result of the significant cybersecurity incident: Yes ☐ No ☐ Unknown ☐

    If yes, describe the types of assets that were lost or stolen and include an approximate estimate of their value, if known:_____
    _____
    _____
    _____
    _____

    B. i. If yes, has notification been provided to persons whose assets were lost or stolen: Yes ☐ No ☐
    ii. If no, is notification planned: Yes ☐ No ☐

13. Has the significant cybersecurity incident been disclosed in accordance with 17 CFR 242.10:
    A. On EDGAR: Yes ☐ No ☐ If yes, disclosure date: DD MM YYYY
    B. On business Internet website: Yes ☐ No ☐ If yes, disclosure date: DD MM YYYY
    C. If applicable, to the covered entity's customers: Yes ☐ No ☐

    If 12.A, 12.B, and/or 12C. are no, explain why the disclosures have not been made:_____
    _____
    _____
    _____
    _____

14. A. Is the significant cybersecurity incident covered by an insurance policy of the covered entity: Yes ☐ No ☐ Unknown ☐
    B. If yes, has the insurance company been contacted: Yes ☐ No ☐

15. Provide any additional information or comments:_____
    _____
    _____
    _____
    _____

FORM SCIR PART II Page 1 (Execution Page)	CYBERSECURITY RISKS AND SIGNIFICANT CYBERSECURITY INCIDENTS Date:_____ SEC File No: _____	Official Use	Official Use Only

WARNING	Failure to file Form SCIR as required by 17 CFR 242.10 would violate the Federal securities laws and may result in disciplinary, administrative, injunctive or criminal action. **INTENTIONAL MISSTATEMENTS OR OMISSIONS OF FACTS MAY CONSTITUTE FEDERAL CRIMINAL VIOLATIONS.** See 18 U.S.C. 1001 and 15 U.S.C. 78ff(a)

1. Information about the *covered entity:*

A. i. Full legal name:

ii. Business name if different than legal name:

B. Covered Entity's UIC # (if any): Covered Entity's CIK #:

C. Main Address: (Do not use a P.O. Box)

Number and Street 1: Number and Street 2:

City: State: Country: Zip/Postal Code:

D. Type of *Covered Entity* (Check all the apply):

Broker or dealer ☐ Clearing Agency ☐ Major Security-Based Swap Participant ☐

Municipal Securities Rulemaking Board ☐ National Securities Association ☐ National Securities Exchange ☐

Security-Based Swap Dealer ☐ Security-Based Swap Data Repository ☐ Transfer Agent ☐

EXECUTION:

The undersigned certifies that this form was executed on behalf of, and with the authority of, the *covered entity*. The undersigned and *covered entity* represent that the information and statements contained herein are current, true and complete. The undersigned and *covered entity* further represent that to the extent any information previously submitted is not amended such information is current, true, and complete.

Date (MM/DD/YYYY) Full Legal Name of Covered Entity

By: Signature Name and Title of Person Signing on Covered Entity's behalf

This page must always be completed in full.

DO NOT WRITE BELOW THIS LINE – FOR OFFICIAL USE ONLY

FORM SCIR PART II Page 2	*Covered Entity* Name: _____ Date:_____ SEC File No: _____	Official Use	Official Use Only

2. "Cybersecurity risk" means financial, operational, legal, reputational, and other adverse consequences that could result from cybersecurity incidents, cybersecurity threats, and cybersecurity vulnerabilities. "Cybersecurity incident" means an unauthorized occurrence on or conducted through a covered entity's information systems that jeopardizes the confidentiality, integrity, or availability of the information systems or any information residing on those systems. "Cybersecurity threat" means any potential occurrence that may result in an unauthorized effort to affect adversely the confidentiality, integrity, or availability of a covered entity's information systems or any information residing on those systems. "Cybersecurity vulnerability" means a vulnerability in a covered entity's information systems, information system security procedures, or internal controls, including, for example, vulnerabilities in their design, configuration, maintenance, or implementation that, if exploited, could result in a cybersecurity incident.

   Provide a summary description of the cybersecurity risks that could materially affect the covered entity's business and operations and how the covered entity assesses, prioritizes, and addresses those cybersecurity risks.

   _____
   _____
   _____
   _____
   _____

3. A "significant cybersecurity incident" means a cybersecurity incident, or a group of related cybersecurity incidents, that:
   (1) significantly disrupts or degrades the ability of the covered entity to maintain critical operations; or
   (2) leads to the unauthorized access or use of the information or information systems of the covered entity, where the unauthorized access or use of such information or information systems results in or is reasonably likely to result in:
   (A) substantial harm to the covered entity; or (B) substantial harm to a customer, counterparty, member, registrant, or user of the covered entity, or to any other person that interacts with the covered entity.

   Has the covered entity experienced one or more significant cybersecurity incidents during the current or previous calendar year: Yes ☐ No ☐

   If yes, provide a summary description of each significant cybersecurity incident during that period. The description of <u>each</u> significant cybersecurity must include, at a minimum, the following information to the extent known:

   The person or persons affected;
   The date the incident was discovered and whether it is ongoing;
   Whether any data was stolen, altered, or accessed or used for any other authorized purpose;
   The effect of the incident on the covered entity's operations; and
   Whether the covered entity, or service provider, has remediated or is currently remediating the incident.

   _____
   _____
   _____
   _____
   _____
   _____
   _____

[FR Doc. 2023-05767 Filed: 4/4/2023 8:45 am; Publication Date: 4/5/2023]