September 29, 2017

Mr. Christopher J. Kirkpatrick
Secretary of the Commission
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street NW
Washington, DC 20581

VIA ONLINE SUBMISSION

Re: System Safeguards Testing Requirements, RIN 3038–AE29 and RIN 3038–AE30

Dear Secretary Kirkpatrick:

The Minneapolis Grain Exchange, Inc. ("MGEX") would like to thank the Commodity Futures Trading Commission ("CFTC" or "Commission") for the opportunity to respond to comment as a part of the CFTC's KISS initiative. MGEX is both a Subpart C Derivatives Clearing Organization ("DCO") and a Designated Contract Market ("DCM"), and has been the primary marketplace for North American Hard Red Spring Wheat ("HRSW") since its inception in 1881. MGEX supports the Commissions effort to simplify, modernize, and reduce the cost of compliance. System safeguards and cyber security are important issues to the industry as a whole and are topics MGEX takes very seriously. MGEX has previously submitted comments on system safeguards by a letter dated February 22, 2016.

Since that time the two rulemakings in question (RIN 3038-AE29 and RIN 3038-AR30) have become final rules. Overall, there are three main comments that MGEX would like to make regarding system safeguards. First, that as a DCM and DCO, MGEX is very concerned about the inconsistencies between the DCM and DCO rules that remain in the final rules on system safeguards. Second, the final rules and the Commissions interpretation of those rules is still too prescriptive. Third, cost of compliance with the final rules is high and growing.

Inconsistent Approaches

The DCM and DCO final rules on system safeguards lack consistency in drafting which for DCM/DCO entities makes compliance more difficult to achieve. Moreover, MGEX is concerned that during future rule enforcement reviews (RERs) by different CFTC divisions will lead to opinions, recommendations, interpretations, and application of these final rules resulting in an even greater divide between the two sets of final rules.

At a high level, the rules discuss many of the same subject; however, upon examination the lack of consistency between the two sets of rules is significant and will impact MGEX's ability to maintain a consistent and cohesive system safeguards programs that

simultaneously satisfies the DCO and the DCM final rules.

Inconsistent Application of the 5% Threshold

MGEX is most effected by the inconsistent treatment of smaller entities by the DCM and DCO rules. Under the DCM framework, entities with trade volume lower than 5% are exempt from certain requirements.[1] MGEX appreciates the thoughtful carve out this provision creates. The distinction between a Covered DCM and a DCM that is not covered is a valuable concept that MGEX believes should be applied to the DCO Rulemaking. As it stands, a smaller entity such as MGEX that is a combined DCM and DCO would not be able to take advantage of this reasonable and thoughtful carve out. As proposed, MGEX would be in a position where it needs to meet the highest common denominator of the two Rulemakings – completely eliminating the Commission's intended benefits for smaller entities. MGEX requests that the Commission create a similar carve out for smaller organizations in the DCO Rulemaking.

Specifically, the DCM Rulemaking modifies minimum testing requirements and independent contractor requirements. MGEX believes that the DCO Rulemaking should use the same 5% of combined annual total trading (clearing) volume standard when classifying DCOs, and provide the exact same final carve outs for "Covered Derivatives Clearing Organizations" and DCOs not covered.

In doing so, the Commission would be further recognizing what it has already stated to be an important distinction: the inherent lower systemic market risk posed by smaller organizations and that regulatory requirements should be prescribed with that lower risk in mind. Moreover, if volume is a reliable factor to determine exposure, risk, and regulatory status on the DCM side it follows that volume would be a reliable factor to determine the same on the DCO side.

Such a change would ensure smaller DCOs are appropriately considered and that burdensome requirements are not imposed onto such entities. If burdensome requirements are placed on smaller entities, competitive advantage for big conglomerates will necessarily result. Such competitive advantage would foster industry consolidation which, in turn, concentrates market risk and could lead to creating entities that are too big to fail while simultaneously limiting the entry of others.

Program of Risk Analysis and Oversight

One example of an area of inconsistency is in the program of risk analysis and oversight. At the onset there are some seemingly innocuous inconsistencies. For example, both final rules call for a "program of risk analysis and oversight." While not a defined term, both final rules refer to this same program. The problem is that the two final rules differ in their interpretations of what should be in their given programs. The DCM rules calls for

[1] Defined as "a designated contract market whose annual total trading volume in calendar year 2015, or in any subsequent calendar year, is five percent (5%) or more of the combined annual total trading volume of all designated contract markets regulated by the Commission for the year in question, based on annual total trading volume information provided to the Commission by each designated contract market pursuant to the procedure set forth in this chapter."

seven component parts[2] of the program while the DCO rules call for six component parts.[3] The "program(s) of risk analysis and oversight" are key components of both final rules and having differences between the two have ramifications in several other key parts of the two final rules. The lack of consistency is problematic and increases the compliance burden of a combined DCO and DCM entity.

Specifically, the DCO version of the program is included in additional sections related to DCOs: outsourcing and retention of responsibility,[4] requirements for resources, [5] and controls testing.[6] While in the DCM version, the program is an underlying requirement for additional sections related to a DCMs: standards for development and operations of system[7] and controls testing.[8]

It is not a mere drafting or semantic difference between the DCO and DCM rules. Having inconsistent approaches, language, and components creates confusion and has rippling effects for combined entities. The program of risk analysis and oversight requirement is an important part of a cyber security framework and MGEX understands the need to ensure such a program exists. Yet, even though this program is important, consistency between the regulatory branches of the Commission is equally as important. DCMs and DCOs work closely together and in some organizations, like MGEX, are inextricably linked. The cost and burden to comply with divergent regulatory schemes is great.

MGEX has also noted in other KISS comment letters that there is a troubling trend of the Commission engaging in edification and policy making through RERs, as opposed to reviewing compliance with core principles. In future separate or combined RERs on system safeguards, MGEX is worried of divergent or even conflicting messages from the division of clearing and risk and the division of market oversight as they are examining compliance with inconsistent rules. It is also important to note that as two divisions of the CFTC do not agree on the component parts of a program of risk analysis and oversight it is difficult to conclude that these programs have a precise meaning in the industry. MGEX strongly urges the Commission to implement practice and policy to harmonize these rules and the respective RERs examining compliance with them.

Overly Prescriptive Nature of Rulemakings

---

[2] §38.1051 (a) (1)-(7)

[3] §39.18 (b)(2)(i)-(vi)

[4] §39.18(d)(2)

[5] §39.18(b)(4)

[6] §39.18 (e)(5): In particular this subsection outlines a requirement that "each control included in its program of risk analysis and oversight…[be tested] no less frequently than every two years"

[7] §38.1051 (b): "In addressing the categories of risk analysis and oversight required…[a DCM] shall follow generally accepted standards and best practices with respect to the development, operation, reliability, security, and capacity of automated systems."

[8] §38.1051(h)(3): In particular this subsection required "testing of each control included in the designated contract market's program of risk analysis and oversight"

In addition to the inconsistencies in the rules MGXEX has continued concerns about the overly prescriptive nature of the system safeguards framework. MGEX has implemented a robust system safeguards program tailored to MGEX's organizational needs. This organizational tailoring is a key attribute of the current System Safeguards framework throughout the industry. Moreover, having a flexible, dynamic, and adaptable approach is crucial to the success of any cyber security or System Safeguard rulemaking. One of the challenges faced by the CFTC, MGEX, and other organizations is the ever-changing nature of cyber threats. Overall, MGEX supports and recommends that the CFTC reduce its reliance on static lists of requirements in favor of defined principles that can guide and support the industry.

Information Security Controls

One example of an overly prescriptive component of §39.18 (b)(2) and §38.1051(a)(2) is the Information Security subsections which call for information security and articulates an extensive laundry list of information security controls.[9] This laundry list approach to information security controls has a number of problems.

Initially, effectively monitoring and supporting information security cannot be reduced to a set of check-the-box items. Information security is a multi-faceted concept and more importantly it is a concept that is changing. MGEX believes that setting a static list of controls is perhaps not the most functional approach for the industry long-term. The industry has already categorized and itemized the information security controls applicable to their own organizations. Organizations, based on the realities of their specific business may have things that are on this list but they also may lack certain discrete elements that are not applicable to their business, network architecture, or external facing exposure. It is also important to note that organizations may have controls that are vital to their operations that are not included in this laundry list of controls.

The principle of information security is a valuable one but this overly prescriptive approach is not helpful for the CFTC or the industry. Having a check-the-box approach to information security controls may assist the DCR and DMO during rule enforcement reviews but they do not foster industry led development of controls. If regulatory approval can be met by satisfying this list there will be less incentive for organizations to apply a critical eye to their own infrastructure and develop their own controls and tools. Industry and organizational development of controls and tools is also a better gauge of "industry best practices" than a static list of requirements. In particular, the very nature of cyber threats is they are hard to define and hard to anticipate. Static lists are unlikely to be able to respond and adapt as issues facing the industry change over time. A principles based approach is better suited to the topic of cyber security.

Moreover, having an itemized list may give the CFTC and organizations a false sense of security. Just because there are appreciable answers to this list of controls does not

[9] "Access to systems and data (e.g., 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 (e.g., network port control, boundary defenses, encryption); system and information integrity (e.g., 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."

inherently mean that informational security controls are adequately addressing the concerns of an organization, the industry, or the CFTC. It is also important to note that exactly what is in any prescriptive list matters. Under the Controls testing requirements[10] in this Rulemaking, all of these controls must be tested on a rolling basis by independent contractors every two years.

MGEX recommends and requests that the CFTC modify §39.18 (b)(2) to reflect a more principle based approach by removing the laundry list of controls itemized in subsections (i) – (v) while keeping the main concepts intact.

Cost of Compliance

There are extensive costs to complying with the system safeguards rules. Many of these costs are intrinsic to running a business in the current cyber security environment. However, many costs and many of the new costs stem from the overly prescriptive regulatory framework that has been enacted. The Commission has also failed to account for entities of different sizes which disproportionately effects entities like MGEX and is an almost insurmountable bar to entry for new entities.

Independence

One specific area where the cost of compliance is unnecessarily high is the various requirements to have independent testing done. Both the DCM and DCO rules make numerous references to requirements for independent contractor testing at various intervals. For example, in the DCM rules, vulnerability testing for a newly defined "covered DCM[11]" is to be conducted by an independent contractor for two out of its four quarterly vulnerability tests.[12] While the other two quarterly vulnerability tests may be conducted by employees "who are not responsible for development or operation of the systems or capabilities being tested." In contrast, a newly defined DCM that is "not covered" shall have its vulnerability testing performed by an independent professional.

These rules utilize three potentially conflicting and overlapping terms (for independence) that are also overly burdensome to smaller combined entities. In the current approach, larger entities that have greater amounts of cyber-risk are allowed to utilize their own staff for many requirements. Meanwhile, smaller entities that cannot support full-time testing staff are penalized by the independence requirements.

Conclusion

MGEX appreciates the opportunity to comment on system safeguards as a part of the KISS initiative. Efforts to simplify the implementation and interpretation of rules is precisely what is needed to address some of the flaws in the system safeguards rule framework.

---

[10] §39.18(e)(5)

[11] See §39.1051 (h)(1) for definition of covered designate contract market

[12] §38.1051 (h)(2)(iii)

Thank you again for the opportunity to comment, and please feel free to contact MGEX with any further questions.

Sincerely,

Emily Spott
Associate Corporate Counsel

cc: Mark G. Bagan, CEO, MGEX
James D. Facente, Jr., Director of Market Operations, Clearing and IT, MGEX
Layne G. Carlson, Chief Regulatory Officer, MGEX