February 22, 2016

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 the CFTC's request for public comment on the System Safeguards Testing Requirements Proposed Rulemaking for the above listed proposed rules, as published in the December 23, 2015 Federal Register Vol. 80, No. 246.

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 appreciates efforts the Commission has put forth to address the growing risk that cyber threats pose to trading markets and organizations such as MGEX. MGEX acknowledges the threats that DCMs, DCOs and other organizations in the commodities industry face in the current environment. Cyber-attacks, cyber threats, hacking, and, in some cases, state sponsored attacks, have become a real threat to larger institutions. MGEX understands the impetus for the CFTC to act and address these threats.

MGEX supports the concept of System Safeguards and the CFTC's efforts to address cyber threats. MGEX has carefully reviewed both RIN 3038–AE29 ("DCO Rulemaking") and RIN 3038–AE30 ("DCM Rulemaking") (collectively the "Rulemakings"). MGEX supports many of the component parts of the Rulemakings. There are a couple of areas that MGEX does have comments for the Commission to consider. Specifically, MGEX remarks: that there are inconsistent approaches between the DCO and DCM Rulemakings; that there are scalability concerns; that some of the specific sections are overly prescriptive in nature; and that the cost of compliance with this rulemaking is too high compared to the benefits it would produce.

## Inconsistent Approaches

MGEX recognizes the importance to have both the Division of Market Oversight ("DMO") and the Division of Clearing and Risk ("DCR") engage in the rulemaking process on the

topic of System Safeguards as cyber threats are a potential issue to both. While both resulting Rulemakings are important, the lack of consistency between them is problematic for entities like MGEX.

At a high level, the Rulemakings discuss many of the same subjects and propose comparable rules. However, upon examination the lack of consistency between the two Rulemakings 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 Rulemakings.

MGEX is both a DCM and DCO and it is important that the Commission's final Rulemakings account for such a combined structure. It is crucial that combined entities are not subject to rules for DCMs and DCOs that conflict or result in unintended, irreconcilable requirements. It is also important that conceptually the Rulemakings align with each other. Because MGEX is a combined entity it will have to comply with the highest common denominator between the two Rulemakings. If one Rulemaking has a carve-out, exception, or clarification that the other does not have an entity like MGEX cannot rely on it.

***Inconsistent Application of the 5% Threshold***

Currently, the DCM Rulemaking creates the concept of a "Covered Designated Contract Market" ("Covered DCM") whereby DCMs below 5% of trade volume 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

[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."

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***

In addition to the 5% threshold there are other notable inconsistencies between the rulemakings. At the onset there are some seemingly innocuous inconsistencies. For example, both Rulemakings call for a "program of risk analysis and oversight." While not a defined term, both Rulemakings refer to this same program. The problem is that the two Rulemakings differ in their interpretations of what should be in their given programs. The DCM Rulemaking calls for seven component parts[2] of the program while the DCO Rulemaking call for six component parts.[3] The "program(s) of risk analysis and oversight" are key components of both Rulemakings and having differences between the two have ramifications in several other key parts of the two Rulemakings. The lack of consistency is problematic and increases the compliance burden of a combined DCO and DCM entity.

Specifically, the DCO Rulemaking 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 Rulemaking 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 Rulemakings. 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.

---

[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"

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 will be great, particularly in the context of future rule enforcement reviews initiated by the DMO and the DCR. Varying component parts and different interpretations by the two divisions could cause significant confusion for combined entities and will most certainly increase the cost of compliance.

Additionally, throughout its cost-benefit analysis the Commission makes reference to the fact that the Commission is merely clarifying existing requirements and any new costs are "attributable to compliance with the existing regulation and not to the proposed rules.[9]" MGEX inquires whether the Commission itself has fully elucidated the precise component parts of a program of risk analysis and oversight. The two Rulemakings do not agree and this topic appears to be unsettled within the industry. As such, MGEX believes that the Commission should examine the requirements for a program of risk analysis and oversight and modify the requirements to be more principles based in order to facilitate consistent application. Also, 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, as outlined in the Rulemakings, are preexisting requirements that all entities should already be in full compliance with and that do not have a cost of compliance.

***Coordination of BCDR Plans and Testing***

Another area where there are inconsistencies relates to the coordination of business continuity and disaster recovery ("BCDR") plans and testing. Both the DCO and DCM Rulemakings[10] articulate the need to coordinate with other entities in the BCDR context. MGEX commends the Commission's decision to articulate these requirements in the context of "to the extent practicable."[11]

However, MGEX is concerned that the DCR and the DMO may have differing expectations for this coordination. The two Rulemakings differ on the parties an entity is expected to coordinate with. On the DCM side, coordination is expected with "member and other market participants upon whom [the DCM] depends upon to provide liquidity." While the DCO Rulemaking calls for coordination with "its clearing members." MGEX requests that these two plans for coordination be harmonized and provide for coordination with other entities deemed appropriate by an organization. MGEX is concerned that if clearing members or other participants are required to coordinate extensively with DCMs or DCOs there will be an incentive to work with fewer organizations. Placing increased regulatory burden and creating obstacles for smaller entities to participate is something MGEX is particularly sensitive to.

Both the DCO and DCM regulations also call for taking "into account the business continuity-disaster recovery plans of its telecommunications, power, and other essential service providers."[12] MGEX wants to ensure that this requirement is interpreted

[9] See Federal Register, Vol. 80, No. 246 pg. 80167-80176
[10] See §39.18(c)(3) and §38.1051(i)(1)
[11] §39.18(c)(3)
[12] §38.1051(i)(2); See Also, §39.18(c)(3)(iii) "Ensure that its business continuity and disaster recovery plan takes into account the plans of its providers of essential services, including telecommunications, power, and water."

consistently by both the DCR and DMO. MGEX is concerned that much of the information needed about telecommunication, power, and water providers is not readily or publically available. Particularly, independent or smaller organizations neither have the bargaining power to demand information from all providers of essential services nor have the ability to change or modify the essential providers' approach to BCDR.

***Inconsistencies***

Overall, MGEX requests that the Commission work to eliminate inconsistencies between the two Rulemakings. In addition to the topics discussed, MGEX has identified inconsistencies in how the Rulemakings handle: notice requirements,[13] BCDR,[14] and outsourcing.[15] Particularly in light of combined entities, consistency is vital to an effective compliance program. In particular, MGEX advocates for the 5% threshold established by the DMO be included in the DCO Rulemakings. Such an addition will serve the public interest by ensuring entities are not barred entry into the market and will defend against continued market consolidation.

## Scalability

In addition to issues of inconsistency, MGEX is also concerned about the one-size-fits-all approach being promulgated in the Rulemakings. MGEX supports having a scaled approach to rulemaking. Having a scaled approach is key to fostering an environment of both oversight and commercial viability. Different organizations are situated differently in the industry, have different exposure to threats, are faced with different problems and have different strengths. A one-size-fits-all approach cannot succeed in ensuring a healthy commodities industry.

If a one-size approach is used the CFTC can actually put the industry in worse shape than with their Rulemaking. This can occur by forcing smaller or independent institutions out of the market. It can also occur by creating barriers for entry for new organizations. When this happens the market consolidates into a handful of entities. These large conglomerate organizations have a disproportionate amount of market risk. MGEX feels that as one of the only independent organizations left it is our responsibility to bring up the risks that a one-size approach can lead to.

Developing regulatory controls and oversight is the function of the CFTC. The CFTC also has a mandate from Congress to enact rules to address concerns. That being said, the CFTC can and should rightly exercise its discretion to have phased, scaled, and dynamic rulemakings that allow development of the controls and oversight necessary while preserving the commercial viability of individual organizations.

MGEX applauds the CFTC's approach in the DCM Rulemaking that established a distinction for "covered" and DCM's not covered by certain components of the Rulemaking. This 5% volume distinction is conceptually exactly the type of scaled approach that MGEX would like to see.

[13] §38.1051(e) and §39.18(g)
[14] §38.1051(i)(2) and §39.18(c)(3)(ii)
[15] §39.18(d) and §38.1051(d)(2)

***Becoming a Covered DCM***

One example of an area where MGEX supports adding a scaled approach is regarding the 5% threshold. As noted above, MGEX supports the DMO's decision to create a 5% threshold or cut-off regarding the application of certain requirements. However, while §38.1051(h)(1) does articulate a way in which an organization may move from being a covered entity to being a DCM not covered, there is no such process for how an entity may be treated if it is becoming a Covered DCM.

MGEX requests that the CFTC articulate a meaningful and phased approach for how organizations move above and below the 5% total volume mark. MGEX supports a formal transition or ramp-up period for organizations that may be moving from below the 5% mark one year to above the 5% mark the next.

***Systems Development***

Another example where a scaled approach is needed is in §39.18(b)(2)(v) concerning systems development.[16] This requirement appears to anticipate significant systems development that may or may not be applicable to every organization. Some entities are actively and sometimes even prolifically developing and modifying their systems. Other organizations have different exposure and more static systems where this section may not be relevant to their activities.

MGEX supports modification of this language to include language that specifies "to the extent practicable," "as needed," or "as is reasonable." It is probably not the Commission's intent to require such requirements for entities who may not need them.

***Independent Contractors***

Another component part of scalability is the independent contractor/independent professional/employee who is not responsible for development or operation of systems and capabilities being tested.

The DCO Rulemaking establishes vulnerability testing requirements.[17] This provision requires two tests to be conducted by independent contractors and two tests by employees who are not responsible for the development or operation of systems and capabilities being tested. This is a prime example where a distinction should be made between DCOs and SIDCOs or "covered DCOs". Large and systemically important organizations employ thousands and have the resources to dedicate an IT employee to exclusively work on independent testing requirements. In fact, it would not be surprising if SIDCOs were to employee multiple dedicated employees. However, an organization like MGEX is smaller and more nimble. As such, smaller organizations like MGEX may not have qualified individuals outside of the IT Department who would meet the needed background and skill set while also meeting the level of independence which the

[16] "Systems development and quality assurance, including, but not limited to, requirements development; preproduction and regression testing; change management procedures and approvals; outsourcing and vendor management; training in secure coding practices; and any other elements of systems development and quality assurance included in generally accepted best practices;"
[17] §39.18(e)(2)(iii)

Commission is proposing.

Therefore, an entity like MGEX would be forced to either bear significant cost to hire dedicated employees exclusively for regulatory testing compliance or bear significant cost to have independent contractors perform all four tests. This approach gives larger and concentrated organizations a significant competitive advance and further incentivizes market consolidation. It is also important to note that the rigorous frequent testing that the MGEX team already engages in does not count towards this proposed DCO Rulemaking. There is a disconnect between what MGEX is doing and what this Rulemaking calls for. MGEX performs vulnerability testing in excess of what is called for but because of the prescriptive nature of this Rulemaking significantly less frequent but more costly testing is considered superior.

MGEX supports applying the 5% threshold and therefore exempting smaller DCOs from the requirements of frequency and independence. The Commission has already created a carve-out for larger organizations who may choose to have an employee not responsible for development or operation of the systems to perform certain required tests. It is a matter of fundamental fairness that smaller organizations' concerns are also addressed by establishing a 5% threshold for certain requirements. Alternatively, MGEX supports reducing the number and/or nature of the testing required.

***Scalability***

MGEX supports the Commission modifying the current Rulemakings to better account for different types and sizes of entities. MGEX believes that many of the issues related to scalability would be resolved by establishing a 5% threshold and exempting certain entities from certain requirements. Alternatively MGEX supports modifying the Rulemakings in their current form to provide needed flexibility that accounts for different organizations and the risk (or lack thereof) they present to the industry.

## Overly Prescriptive Nature of Rulemakings

In addition to resolving the inconsistencies and scalability issues in the Rulemakings, MGEX requests that the Commission address the overly prescriptive nature of the Rulemakings. MGEX believes that having in place robust system safeguards can be a valuable and essential tool to prevent and handle cyber security issues. Because of the importance of system safeguards MGEX already has an internal program and team dedicated to cyber security. MGEX takes Core Principle 20[18] and Core Principle I[19]

[18] §38.1050 Core Principle 20.Each designated contract market shall: (a) 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; (b) Establish and maintain emergency procedures, backup facilities, and a plan for disaster recovery that allow for the timely recovery and resumption of operations and the fulfillment of the responsibilities and obligations of the board of trade; and (c) Periodically conduct tests to verify that backup resources are sufficient to ensure continued order processing and trade matching, transmission of matched orders to a designated clearing organization for clearing, price reporting, market surveillance, and maintenance of a comprehensive and accurate audit trail.

[19] 7 U.S. Code § 7a–1 (I) System safeguards. Each derivatives clearing organization shall—(i) 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 automated systems, that are reliable, secure, and have adequate scalable capacity; (ii) establish and maintain emergency procedures, backup facilities, and a plan for disaster

(collectively the "Core Principles") seriously and has a program to fulfill the requirements outlined in the Core Principles. The requirements of the Core Principles along with the current regulations relating to System Safeguards have been interpreted by MGEX and other industry organizations in ways unique and tailored to each organization.

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.

MGEX comments and requests that the CFTC make changes to the current proposed Rulemakings to better allow for organizational and industry flexibility.

***Program of Risk Analysis and Oversight***

A principles based approach is preferred; therefore, MGEX applauds the CFTC's efforts to draft regulations that are principles based. One specific example exemplifying this approach is in the DCO Rulemaking. §39.18(b)(1) articulates general principles that governs a System Safeguards program of risk analysis and oversight.[20] MGEX appreciates this approach and would encourage the CFTC to modify other sections to conform to it.

However, many sections depart from this principles based approach. For example, §39.18 (b)(2) and §38.1051(a) both articulate an overly prescriptive standard. §39.18(b)(2) has six component parts that outline the following topics: (i) information security, (ii) business continuity and disaster recovery ("BCDR"), (iii) capacity and performance, (iv) systems operations, (v) system development and quality assurance, and (vi) physical security and environmental controls. Similarly, §38.1051(a) outlines the six components mentioned above and Enterprise Risk Management and Governance. MGEX takes no issue with these general areas/topics and support their general inclusion of these topics in the Rulemaking. But, the specific and itemized content of some of these sections are overly prescriptive.

***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.[21] This laundry list approach to

---

recovery that allows for— (I) the timely recovery and resumption of operations of the derivatives clearing organization; and (II) the fulfillment of each obligation and responsibility of the derivatives clearing organization; and (iii) periodically conduct tests to verify that the backup resources of the derivatives clearing organization are sufficient to ensure daily processing, clearing, and settlement.

[20] §39.18(b)(1)

[21] "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

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 base 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 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[22] 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.

***Internal Reporting and Review***

In addition to the overly prescriptive nature articulated for the program of risk analysis and oversight as well as the information security controls, MGEX is concerned about the requirement for internal reporting and review.[23] MGEX believes that system safeguards and cyber security are topics that senior management and the Board of Directors should be kept up to date on. Currently, MGEX regularly updates management, the executive

integrity monitoring); vulnerability management; penetration testing; security incident response and management; and any other elements of information security included in generally accepted best practices."

[22] §39.18(e)(5)

[23] §39.18(e)(9) and §38.1051(l)

team, and Board of Directors on cyber related topics, including: system upgrades, personnel, education/awareness, policies, changes, and testing. At a high level, MGEX supports the principle that management and the Board are kept informed.

That said, the ramifications of the current reporting requirements of the DCO Rulemaking[24] would only hinder active Board engagement on system safeguards and cyber security. Under this provision, management and the Board shall "receive and review reports setting forth the results of the testing and assessments required by this section."

This is an expansive requirement being put on the Board of Directors in light of the extensive laundry list of items included in this Rulemaking. For example, just under §39.18(b) there are six discrete items which may not seem like much until one realizes that just (i) has 26 separate controls that are all required to be tested by independent contractors. If the Board of Directors has to review all results from all tests and assessments, reviewing complex IT testing reports could become a full-time job.[25]

MGEX requests that the laundry list of prescriptive requirements be converted into principle based regulation.

Additionally and alternatively that §39.18(e)(9) be modified to provide for the Board of Directors to be kept informed about testing and receive summaries and compilations of testing results at regularly scheduled Board meetings. MGEX suggests that the Board of Directors be allowed to delegate review of specific reports to management.

***Vulnerability v. Penetration Testing Frequency***

Moreover, another topic where the Rulemakings are overly prescriptive is the requirements for vulnerability and penetration testing. One illustrative example of this concerns the frequency of testing. The Rulemaking calls for quarterly vulnerability testing[26] and for, effectively, two annual penetration tests.[27] Well before this Rulemaking was issued MGEX developed its own program for vulnerability and penetration testing. MGEX currently performs vulnerability tests more frequently than quarterly. Additionally, MGEX has not identified a need to have two annual penetration tests and is currently scheduling penetration tests on a different and variable schedule depending on security developments and cyber threats.

This illustrates that in some areas MGEX already exceeds the minimum requirements while in other areas MGEX may not need the minimums being set. MGEX is in the best position to gauge exposure to vulnerabilities and set organizational specific standards. MGEX has limited external facing systems particularly in comparison to SIDCOs or larger

[24] §39.18(e)(9)

[25] See Also a comparable provision in the DCM Rulemaking §38.1051(l). MGEX shares the same concerns with the same analysis to this section.

[26] §39.18(e)(2)(i)

[27] §39.18(e)(3) and (4)

organizations and therefore need more infrequent penetration testing.

Also, MGEX's internal architecture is more limited in scope than other organizations which means that MGEX can engage in a higher volume of vulnerability scanning than may be practical or useful at larger entities. Overall, the take-away is that organizations are different and prescriptive, static requirements have limited use and may not be an effective use of resources. Frequency of testing should be determined by the frequency of systems changing and the scope of exposure and should not be reduced to a static minimum.

This is another example of why a threshold or carve out is needed for smaller DCOs. Because while MGEX would be considered a DCM not covered[28] by the all of the frequency requirements[29] of the DCM Rulemaking, the fact that MGEX is a combined DCO and DCM means that this carve out is effectively negated by the DCO Rulemaking. MGEX strongly supports the addition of the 5% threshold be added to the DCO Rulemaking and provide for adequate ramp-up and ramp-down periods for organizations moving above or below this threshold.

MGEX requests that the frequency of both vulnerability and penetration testing be left up to the organizations themselves. In particular, allowing combined DCO and DCM entities to establish their own frequencies based on network architecture, exposure of systems, and cyber risk.

***Independence***

Another topic where the two Rulemakings are overly prescriptive is the concept of "independence." Having independent testing performed is a key feature of this Rulemaking and is probably the most costly component to comply with. Moreover, MGEX is also concerned about the breadth and volume of proprietary information that vendors would have access to in order to perform the testing required. Having vast quantities of industry information in the hands of vendors may actually cause greater harm as vendors may be at greater risk of a cyber incident.

Specifically, both the DCM and DCO Rulemakings make numerous references to requirements for independent contractor testing at various intervals. For example, in the DCM Rulemaking, vulnerability testing for a newly defined "covered DCM[30]" is to be conducted by an independent contractor for two out of its four quarterly vulnerability tests.[31] 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.

MGEX suggests that the Commission examine the foundation of the sections requiring

[28] §38.1051(h)(1)

[29] 38.1051(h)(2)

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

[31] §38.1051 (h)(2)(iii)

independent contractors. The Rulemakings utilize three potentially conflicting and overlapping terms that also are 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.

The requirements around the use of independent contractors/professionals/employees is another example of a situation that puts smaller entities at a distinct disadvantage. In the interests of fundamental fairness, MGEX requests that the Commission adopt the 5% threshold in the DCO Rulemaking and allow smaller entities a more appropriate standard to correlate with the significantly diminished risk they pose.

**Cost of Compliance**

In order for an organization to comply with these Rulemakings there will be a significant amount of cost. Throughout both the DCO and DCM Rulemakings the Commission articulates that many of the requirements will not have additional costs or if there are costs these costs are "attributable to compliance with the existing regulations and not to the proposed rules." The Commission relies on the fact that existing rules require compliance with "generally accepted standards and industry best practices.

This cost-benefit analysis articulated in the Rulemakings does not effectively take into account the realities of these Rulemakings for all entities. MGEX has defined and implemented a system safeguards structure that it believes conforms to industry best practices. Even if this structure is compatible with the Rulemakings there is still a cost of compliance. Unless each organization's program/structure is identical to the CFTC's Rulemakings there will be a cost of compliance because conforming to different (even if comparable) standards has financial ramifications.

One example that will have a high cost of compliance concerns the requirement that DCOs coordinate their BCDR plans with clearing members, members, market participants, and service providers.[32] Initially, there are the practical barriers to comprehensively coordinating BCDR plans with clearing members and service providers. Then, after plans are coordinated there is the ongoing responsibility to update, modify, and coordinate with each clearing member and service provider moving forward in time. Therefore, every single time that one of these parties changes their BCDR plan or approach, MGEX is going to have to dedicate resources to not only evaluate these changes but also determine if MGEX needs to make a change and then implement this change.

It is possible that this exercise is valuable or necessary; however, it is important that the CFTC acknowledge the resources of personnel, time, and money that will have to go into complying with this requirement. Whether on the topic of BCDR coordination or any of the other requirements set forth in the Rulemaking there will be a significant cost of compliance. This cost of compliance includes significant staff time, including significant use of legal resources. The Commission does concede that "entities may incur some minor costs as a result of the need to establish and implement internal policies and

[32] §39.18(c)(3)(i) and (iii) and §38.1051(i)(2).

procedures that are reasonably designed to address the work flow associated with the"[33] requirements including: "cooperation between the entity and independent contractor, communication and cooperation between the entity's legal, business, technology, and compliance departments, appropriate authorization to remediate deficiencies identified by the independent contractor, implementation of the measures to address such deficiencies, and verification that these measures are effective and appropriate."[34]

MGEX agrees that the Commission has articulated many of the things that an entity will have to do in order to be in compliance with the regulations. However, MGEX would argue that calling these costs "minor" is inaccurate. Implementation on the scale required by this Rulemaking will include significant personnel and non-personnel resources. MGEX has already increased its overall costs to address cyber security and system safeguards by approximately 30%. These additional costs include: IT and operations personnel costs, software and hardware, legal and compliance costs, as well as third party testing vendors. MGEX anticipates that its costs will go up two or three times if the Rulemakings are made final in their current form. Specifically, MGEX anticipates that the following areas will see increases: internal IT personnel, external vendors/contractors, software, IT infrastructure, legal and compliance, operational resources, and affiliated costs. By far the highest cost of compliance would be the hiring of independent contractors/professionals.

Even though the Commission has not allocated costs for many key components of compliance, the Commission has articulated that an estimated $8,383,222[35] average annual cost of compliance. This number is very worrisome for MGEX because it does not even include many of the real and tangible costs of compliance. The over $8 million cost of compliance only includes: independent vulnerability testing, $143,000 annually;[36] general vulnerability testing, $3,495,000 annually;[37] external penetration testing, $244,625 annually;[38] internal penetration testing $410,625 annually;[39] controls testing, $2,742,000 annually;[40] enterprise technology risk assessment testing, $1,347,950 annually;[41] and cost of volume reporting, $22.00 annually.[42] While not every organization will necessarily bare all of these costs equally it is apparent that there is a significant and potentially burdensome cost of compliance. While $8,383,222 may not be a lot for SIDCOs or other larger organizations it is excessively punitive for smaller entities. Organizations like MGEX cannot bear costs like this and should not have to as they have lower overall risk to the industry and have dramatically smaller exposure to vulnerabilities.

This $8 million number does not even capture all of the costs and therefore constitutes a significant bar to entry. There are only a handful of DCOs left, in large part because many smaller organizations were driven from the industry by regulatory costs. It is important

[33] See Federal Register, Vol. 80, No. 246 pg. 80173
[34] See Federal Register, Vol. 80, No. 246 pg. 80173
[35] See Federal Register, Vol. 80, No. 246 pg. 80168-80177
[36] See Federal Register, Vol. 80, No. 246 pg. 80168
[37] See Federal Register, Vol. 80, No. 246 pg. 80168
[38] See Federal Register, Vol. 80, No. 246 pg. 80170
[39] See Federal Register, Vol. 80, No. 246 pg. 80171
[40] See Federal Register, Vol. 80, No. 246 pg. 80172
[41] See Federal Register, Vol. 80, No. 246 pg. 80175
[42] See Federal Register, Vol. 80, No. 246 pg. 80177

for the Commission to recognize this history and modify these Rulemakings to prevent further market consolidation. MGEX believes the most effective route for the Commission to take would be to establish a 5% threshold or cut-off in both the DCO and DCM Rulemakings. Such a modification will enhance the desired goal of this Rulemaking by establishing greater system safeguard requirements while also preserving the ability for smaller entities to exist in a commercially viable way.

**Conclusion**

MGEX appreciates the opportunity to comment on the Rulemakings being proposed by the Commission. MGEX understands and appreciates the Commissions time in developing these Rulemakings and the impetus for them. MGEX respectfully requests that the Commission address: the inconsistent approaches between the Rulemakings, the lack of scalability, the overly prescriptive nature of the proposed Rulemakings, and the high cost of compliance.

If you have any questions or concerns regarding this letter, please feel free to contact Emily Spott at (612) 321-7188 or espott@mgex.com. Thank you for your attention to this matter.

Sincerely,

Emily Spott
Assistant Corporate Counsel

cc: Mark G. Bagan, CEO, MGEX
James D. Facente, Jr., Director of Market Operations, Clearing and IT, MGEX
Chairman Timothy G. Massad, CFTC
Commissioner Sharon Y. Bowen, CFTC
Commissioner J. Christopher Giancarlo, CFTC