



U.S. COMMODITY FUTURES TRADING COMMISSION

Three Lafayette Centre
1155 21st Street, NW, Washington, DC 20581
Telephone: (202) 418-5110

TO: Heath P. Tarbert, Chairman
Brian D. Quintenz, Commissioner
Rostin Behnam, Commissioner
Dawn Stump, Commissioner
Dan Berkovitz, Commissioner

FROM: Miguel A. Castillo, *CPA, CRMA*
Assistant Inspector General for Auditing

DATE: September 8, 2020

SUBJECT: Performance Audit: CFTC's Policies and Procedures Regarding Oversight of Cybersecurity Safeguards by Registered Entities

The Office of the Inspector General (OIG) engaged an independent public accountant (IPA) to perform a performance audit to review existing CFTC policies, procedures and cybersecurity safeguard oversight of certain CFTC registrants. The two divisions reviewed were Division of Clearing and Risk (DCR) and Division of Market Oversight (DMO). We required the audit to be performed in accordance with U.S. Generally Accepted Government Auditing Standards (GAGAS).

In its audit, the IPA (InteliPath) concluded that DCR and DMO have developed sufficient and adequate policies and procedures to address proper cybersecurity safeguards at CFTC registrants. CFTC has established its own regulations that it follows, but also follows relevant legislation and industry best practices for monitoring registrants' measures for reducing cybersecurity risks. InteliPath identified opportunities to improve policies and procedures to reduce cybersecurity risks for registrants, and offered four recommendations on how the CFTC can do so. The recommendations correlate to CFTC's strategic goal 2.4; increase protections for customer assets and information.¹ They are as follows:

¹ Goal 2.4 states "The Commission works vigilantly to protect customer assets and information. We are identifying potential rule revisions and orders that promote asset and information protection." Source: [CFTC Strategic Plan 2020-2024](#), May 2020.

1. Increase the number of dedicated employees to the Divisions' System Safeguard Examination teams, in order to continuously assess cybersecurity risks at CFTC registrants;
2. Conduct more thorough and in-depth testing [examinations] of registrants in order to validate that their cybersecurity policies and procedures are being adhered to;
3. Implement better data tracking and data analytics tools in order to use available registrant's incident data to analyze and predict trends of potential cybersecurity threats, and to keep track of registrant communication with CFTC personnel; and
4. Emphasize to CFTC registrants usage of information sharing facilities so as to promote rapid awareness of emerging cyber threats.

We provided the draft IntelliPath report to the Chairman on August 3, 2020. The Chairman, speaking for the Commission, subsequently provided comments to the Inspector General that expressed full agreement with the recommendations, and described CFTC's planned actions. In reference to recommendation 1, the Chairman recognized the need for more specialized Systems Risk Analysts to conduct System Safeguards Examinations and committed to implementing this recommendation consistent with other budgetary needs and position allocations.

In response to recommendation 2, the Chairman also recognized that improved and consistent tracking of cybersecurity incident reports from registered entities would enhance the Divisions' oversight of system safeguards. For this purpose, the Divisions plan to enhance their risk assessment procedures and request additional information from all registered entities, including the results of their mandatory cybersecurity tests.

To address recommendation 3, the Divisions will work with technology staff to implement an improved method to track all incident reports and provide notification of significant incidents to management and explore sharing appropriately anonymized cybersecurity information with other registered entities where such anonymization is possible.

Lastly, as it pertains to recommendation 4, the Chairman recognized that emphasizing the use of information sharing facilities by registered entities to stay informed about current cyber threats is important. To implement this recommendation, the Divisions plan to send a joint communication to all registered entities urging them to sign up for alerts available from (1) the Department of the Treasury's Financial Sector Cyber Information Group and (2) the Department of Homeland Security Cybersecurity and Infrastructure Security Agency. In addition, the Divisions also plan to remind registered

entities that FS-ISAC has an information-sharing sub-group dedicated to derivatives markets and clearing organizations. They will further note that exchanges and clearing organizations have also established their own information-sharing organization known as the Clearing House and Exchange Forum whose members actively communicate with each other about current threats.

The OIG considers the Chairman's comments and planned actions responsive to IntelliPath's recommendations.

In connection with the contract, the OIG reviewed IntelliPath's report and related documentation and inquired of its representatives. Our review, as differentiated from an audit in accordance with GAGAS, was not intended to enable us to provide assurance of the report's conclusions. IntelliPath is responsible for the attached auditor's report dated March 29, 2020 and the conclusions expressed therein. However, our review disclosed no instances where IntelliPath did not comply, in all material respects, with GAGAS. The report with comments will be published on OIG's webpage and a summary will be presented in our September 2020 semiannual report to Congress.

The Chairman's comments and IntelliPath's report follows.

Cc:

Jamie Klima, Chief of Staff
Kevin S. Webb, Chief of Staff
John Dunfee, Chief of Staff
Daniel Bucsa, Chief of Staff
Erik Remmler, Chief of Staff
Dorothy DeWitt, Director DMO
Clark Hutchison, Director DCR
Anthony C. Thompson, Chief Administrative Officer
Melissa Jurgens, Chief, Executive Secretariat Branch
A. Roy Lavik, Inspector General
Judith A. Ringle, Deputy Inspector General and Chief Counsel

CFTC's Policies and Procedures Regarding Oversight of Cybersecurity Safeguards by Registered Entities



March 29, 2020

Contents

EXECUTIVE SUMMARY	2
RECOMMENDATIONS.....	3
Summary.....	3
Discussion	3
BACKGROUND	6
CFTC Mission.....	6
Management Objectives	6
CFTC Functions & Divisions	10
Relevant CFTC Regulations.....	10
Audit Objective, Scope, and Methodology.....	11
Entities Registered with CFTC	12
Best Practices.....	13

EXECUTIVE SUMMARY

This report prepared for the Commodity Futures Trading Commission (CFTC or Commission) Office of the Inspector General (OIG) reflects the study and analysis of CFTC’s existing policies and procedures toward reducing cybersecurity risks of CFTC registrants. Specifically, we reviewed the Division of Clearing and Risk (DCR), and Division of Market Oversight (DMO), and system safeguard reviews. Due to unforeseen events we did not review Division of Swap Dealer and Intermediary Oversight (DSIO)¹ actions on this topic. The objective of this performance audit was to review existing CFTC policies and procedures toward reducing cybersecurity risks of CFTC registrants, as conducted by CFTC’s oversight divisions.

The audit was conducted from October 01, 2019 through March 31, 2020 and was conducted in accordance with generally accepted government auditing standards (GAGAS), as stated in the Government Accountability Office’s Government Auditing Standards, [2018 revision](#). The scope of the audit was to conduct an independent audit of CFTC’s performance in reviewing cybersecurity system safeguards in place at entities subject to CFTC regulatory oversight. The scope of our audit covered the 2016 through 2019 fiscal years. This audit is a new initiative by the CFTC OIG to ensure that adequate monitoring of Registrants’ cybersecurity safeguards are in place.

¹ Due to unanticipated and unforeseen event (COVID-19) we were unable to undertake our intended review of DSIO.

We concluded that CFTC and its oversight divisions have developed sufficient and adequate policies and procedures to address proper cybersecurity safeguards at CFTC registrants. CFTC has established its own regulations that it adheres to, but also follows relevant legislation and industry best practices for monitoring registrants' measures for reducing Cybersecurity risk. Our performance audit identified four areas where the CFTC could improve its policies and procedures toward reducing cybersecurity risks of registrants and offers four recommendations on how the Commission can do so.

RECOMMENDATIONS

Summary

1. Increase the number of dedicated employees to the divisions' System Safeguard Examination (SSE) teams, in order to continuously assess cybersecurity risks at CFTC registrants.
2. Conduct more thorough and in-depth testing of registrants in order to validate that their cybersecurity policies and procedures are being adhered to.
3. Implement better data tracking and data analytics tools in order to use available registrant's incident data to analyze and predict trends of potential cybersecurity threats, and to keep track of registrant communication with CFTC personnel.
4. Emphasize to CFTC registrants usage of information sharing facilities so as to promote rapid awareness of emerging cyber threats.

Discussion

CFR Rule [39.18](#), - System Safeguards Testing Requirements for Derivatives Clearing Organizations and 17 Code of Federal Regulations (CFR) [37](#), [38](#), and [49](#) establishes cybersecurity safeguard testing requirements for the majority of CFTC registrants. The CFTC divisions responsible for their respective registrants evaluate different components, based on the markets that the registrants are a part of. Overall, we provided four recommendations to all CFTC divisions with cybersecurity oversight responsibilities.

The audit team developed the four recommendations based on interviews, walkthroughs, review of policies and procedures, and review of incident report logs obtained from divisions' databases. Testing requirements vary by industry segment and divisions responsible for oversight, but there are similarities that are shared when it comes to cybersecurity safeguard evaluations. The audit team evaluated supporting documentation received as evidence to support the commission's adherence to cybersecurity regulations. An important measure evaluated was responsiveness to self-reported incidents by the registrants. Timely responses in order to mitigate risks related to potential cybersecurity threats are crucial to an effective oversight program.

The four recommendations below will assist the CFTC to strengthen their cybersecurity oversight:

1. Increase the number of dedicated employees to the divisions' System Safeguard Examination (SSE) teams, in order to more appropriately assess cybersecurity oversight over CFTC registrants

In order to fully assess every registrant's ability to adhere to their own cybersecurity policies and procedures, the CFTC needs to consider increasing their resources when it comes to evaluating cybersecurity safeguards at registrant entities. Additionally, CFTC needs to consider solely designate personnel to its cybersecurity oversight initiatives, to allow for appropriate time and dedication towards the effort. Developing and increasing more specialized employees will help the CFTC establish a more robust SSE process and continually improve the entire cybersecurity safeguard testing process as well. By increasing the amount of dedicated staff, the CFTC can better achieve its Information Technology (IT) strategic goal #3: Provide a stable, scalable and secure IT environment to ensure continuous operations. Increasing staff can lower the risk that deficient cybersecurity operations exist in the registrant environments.

Incident report logs received from two divisions demonstrate that not all responses to self-reported cybersecurity incidents were timely or consistent. All communication received from registrants should be received and acknowledged from CFTC personnel immediately, in order to assess whether action needs to be taken. By increasing the number of personnel, the CFTC can better ensure that all incidents will be tracked more consistently and addressed in a timely manner. Increasing personnel staff will also allow the commission to conduct timely, thorough, and in-depth examination process.

2. Conduct more thorough and in-depth testing of registrants in order to validate that their cybersecurity policies and procedures are being adhered to.

Although our assessment found that current CFTC policies and procedures appropriately provide oversight over its registrants, there could be more operational examinations across all CFTC divisions. Often, the CFTC divisions did not examine certain registrants based on information from registrants (such as no major changes to the cybersecurity infrastructure and/or incidents from prior year) that were not indicative of deficient cybersecurity policies and procedures. Even though it is the registrant's responsibility to self-report any cybersecurity-related incident to the CFTC, there is still a possibility that not all information will be communicated to the CFTC. By requesting more robust and independent testing of registrants, CFTC will be able to validate that registrants are adhering to their policies and procedures. Additionally, conducting more localized on-site, in-depth testing will provide the CFTC with more information on how registrants conduct their cybersecurity safeguard testing. With this knowledge, the CFTC will be able to accumulate more industry specific cybersecurity risk information. Cataloging registrants' cybersecurity risks will enable CFTC to disseminate useable information to reduce cybersecurity risk among CFTC registrants.

The CFTC does perform ad-hoc testing for certain registrants, but those registrants who undergo testing usually fall into a "high-risk" category. The risk assessment used for determining risk level is based off metrics that the commission utilizes. Often times, many registrants who are not deemed "high-risk" by the commission will not undergo a full SSE. This leaves the possibility that some registrants may be in violation of regulations. The division staff does provide a sound methodology for which registrants to

test every year, but without validating a greater sample of registrants regardless of risk level, the CFTC cannot reduce the risk of non-compliant registrants. Lastly, some registrants may not undergo full SSEs for many years, leaving the opportunity for a potential cybersecurity threat to go undetected for long periods of time.

3. Implement better data tracking and data analytics tools in order to use available registrant's incident data to analyze and develop trends of potential cybersecurity threats, and to keep track of registrant communication with CFTC personnel.

CFTC designates a dedicated CFTC portal through which registrants can freely communicate any cybersecurity-related incident. Communication of that information across CFTC personnel could be improved, however. When a CFTC employee with oversight over a certain registrant receives communication, other CFTC employees might not have that information in real time. If imminent and current cybersecurity threats are happening in real time, all appropriate CFTC employees need to be made aware so that senior leadership could decide on how to communicate those threats to other registrants in that market. Dissemination of information received from registrants could be more formalized to establish protocols and efficient processes to ensure relevant stakeholders (internal and external) receive information in a timely manner.

As information and data are communicated from registrants, the CFTC logs that information mainly for recordation purposes. By implementing a data analytics tool or enhanced dashboards, CFTC personnel could leverage the existing data to help analyze trends, predict certain risks, and to overall be better equipped to utilize the data in an effort to alert registrants of emerging cybersecurity threats.

4. Emphasize to CFTC registrants usage of information sharing facilities so as to promote rapid awareness of emerging cyber threats.

The CFTC currently encourages its registrants to report any potential threat in their market to the Financial Services Information Sharing and Analysis Center (FS-ISAC). This allows registrants to report any major incident anonymously so that all other financial industry entities are aware of potential issues that may affect them. However, it would be more beneficial for CFTC registrants to have a dedicated anonymous sharing platform within the financial derivatives markets, so that registrants can be made immediately aware if an incident occurs in one of their markets. Since the CFTC has their own regulatory measures that registrants must abide by, an information-sharing program dedicated to CFTC-related registrants can alert those registrants and better anticipate potential disruptions and changes. Moreover, it can ensure that CFTC meets its strategic goal #1 and #2, noted below.

Our recommendations were developed considering the regulatory requirements in place to articulate best practices within the federal government. Recommendations take into account industry best practices and CFTC ability to readily implement aforementioned recommendations.

BACKGROUND

The CFTC regulates commodity futures and options markets in the United States. CFTC's mission is to foster open, transparent, competitive, and financially sound markets, to avoid systemic risk, and to protect the market users and their funds, consumers, and the public from fraud, manipulation, and abusive practices related to derivatives and other products subject to the Commodity Exchange Act (CEA). The CFTC protects market participants against manipulation, abusive trade practices and fraud.

The Commission historically has been charged by the CEA with regulatory authority over the commodity futures markets. These markets have existed since the 1860s, beginning with agricultural commodities, such as cotton, corn, and wheat. Over time, the markets regulated by the Commission have grown to include contracts on metals and energy, such as silver, gold, copper, gasoline, heating oil, and crude oil, and contracts on financial products, such as interest rates, stock indexes and foreign currency. Maturation of these markets brings along concomitant need to enhance Cybersecurity oversight.

CFTC Mission

The CFTC's mission can be broken into three key themes (the Marketplace, Avoidance of Systemic Risk, and Market Users) that are supported by four strategic goals: (1) Market Integrity and Transparency; (2) Financial Integrity and Avoidance of Systemic Risk; (3) Comprehensive Enforcement; and (4) Domestic and International Cooperation and Coordination. The foundation for accomplishing these strategic goals lies with management objectives focused towards achieving Commission-wide excellence.

Management Objectives

To advance its mission goals and objectives, the CFTC will achieve Commission-wide excellence by empowering strong, enterprise-focused leaders, maintaining a high-performing and engaged workforce, and ensuring effective stewardship of resources. The CFTC will build and maintain a high-performing, diverse and engaged workforce through implementing innovative recruitment and retention programs, promoting transparent and clear communication, and developing and equipping leaders at all levels of the organization. The CFTC will also achieve Commission-wide excellence by managing resources effectively. The Commission will expand internal controls, governance, and planning processes and ensure that staff has the knowledge, data and technology, and other tools to work effectively.

The most recent CFTC strategic and IT strategic goals are noted below²:

CFTC Strategic Plan 2014 - 2018	
Goal 1: Market Integrity and Transparency	The focus of <i>Market Integrity and Transparency</i> is to recognize that derivatives markets provide a means for market users to offset price risks inherent in their businesses and to serve as a public price discovery mechanism. This means that markets should be free of fraud, manipulation, and other abusive practices; and users should be confident that they will not be victimized. Market integrity is supported by a strong self-regulatory framework overseen by substantial registration administration, product and rule analysis, a

CFTC Strategic Plan 2014 - 2018

	strong surveillance program, and comprehensive examination process. In addition, appropriate information relevant to the markets must be widely and publicly distributed and applicable rules and trading structures must be sound, effective, and accessible to participants.
Goal 2: Financial integrity and Avoidance of Systematic Risk	The focus of Financial Integrity and Avoidance of Systemic Risk is to strive to ensure that Commission-registered derivatives clearing organizations (DCOs), swap dealers (SDs), major swap participants (MSPs), and futures commission merchants (FCMs) have the financial resources, risk management systems and procedures, internal controls, customer protection systems, and other controls necessary to meet their obligations so as to minimize the risk that the financial difficulty of any of these registrants, or any of their customers has systemic implications.
Goal 3: Comprehensive Enforcement	Through the goal of Comprehensive Enforcement, the CFTC enforces the CEA and Commission regulations, and works to promote awareness of and compliance with these laws. Enforcement strives to expeditiously assess tips, complaints, and referrals regarding suspicious activities and potential violations; rigorously and thoroughly investigate such alleged wrongdoings; and effectively prosecute violations and seek imposition of appropriate sanctions.
Goal 4: Domestic and International Cooperation and Coordination	Domestic and International Cooperation and Coordination focuses on how the Commission interacts with domestic and international regulatory authorities, market participants, and others affected by the Commission's regulatory policies and practices. Through domestic and international cooperation and coordination, the Commission is able to identify regulatory concerns, to develop solutions, and to address activities that cut across the jurisdiction of multiple authorities. The Commission's cooperative work promotes internationally accepted standards of best practice, enhanced global regulatory practices, and robust enforcement efforts.

CFTC IT Strategic Plan Goals 2014 – 2018

Goal 1: Deliver IT services aligned with core mission functions of the CFTC

A key driver of the information technology program is the delivery of technology platforms, systems, and services to support CFTC mission and support functions. It is a priority to meet business needs first by empowering users with self-service technology platforms for data analysis, then by enterprise-focused automation services. Accordingly, the self-service technology platforms, including business intelligence software and collaboration software, empower CFTC staff to quickly and iteratively develop analytical work products (e.g., surveillance reports) and share information without being hampered by a dependence on technologists to build solutions. If requirements are such that self-service is not practical and packaged solutions are available in the market, then CFTC will buy, configure, and integrate the appropriate solutions to meet the business need. Given the unique nature of CFTC requirements, if a solution is not available in the marketplace then many of the same technology platforms mentioned previously are leveraged to build custom mission systems.

Goal 2: Facilitate availability and enhance understanding of data to improve regulatory effectiveness

The CFTC increasingly and unavoidably relies on its understanding of data to ensure that it can perform its regulatory and public policy functions effectively. As the markets and participants it oversees overwhelmingly turn electronic, engage in faster and more automated trading, and transact in products that are more and more complex, the CFTC increasingly needs to be a regulator that understands, aggregates, processes, summarizes, and acts on data in a timely manner for surveillance, enforcement and transparency reporting. The markets and participants that CFTC regulates generate and report to the CFTC a large quantity of information from multiple industry sources across multiple markets. Increasing speed, volume, and complexity in these products and markets require the CFTC to develop an increasingly sophisticated ability to validate and pre-digest the reported data so that front-line regulatory functions such as surveillance and enforcement can more effectively use that data. In addition, since the CFTC's regulatory regime has expanded to include swaps, it needs to ensure that the integration of swaps oversight into existing program initiatives includes upgrades to keep up with new techniques and technologies. Thus, data management is essential to all of the CFTC's regulatory initiatives, particularly as swaps oversight is integrated into

CFTC IT Strategic Plan Goals 2014 – 2018

	existing program initiatives.
Goal 3: Provide a stable, scalable and secure IT environment to ensure continuous operations	As the scope of CFTC oversight increases, expands, and as the markets and related data grow increasingly complex, the Commission must continue to provide a stable, scalable and secure IT infrastructure to meet demand. The CFTC's IT infrastructure is the combination of hardware, software, network resources, facilities, and services that are common across the CFTC regardless of mission, program, or project and are the foundation of the CFTC's IT environment. This infrastructure supports the development, testing, delivery, monitoring, control, and support of IT resources.
Goal 4: Manage resources to achieve ODT's strategic Priorities	To continue supporting improved business outcomes IT management processes will continue to be integrated into the CFTC's planning and governance processes. The degree to which IT management leverages best practices, CFTC processes, and proven tools to achieve efficiency of operations will help define its success in fully supporting the CFTC's regulatory mission and mission support activities.

² The audit team did not have access to the CFTC's 2020-2024 strategic plan.

Although the agency has yet to implement an updated strategic plan for FY19 and beyond, there are still notable efforts being taken to ensure that cybersecurity remains a top priority for the agency. The existing strategic goals noted here remain largely unchanged, while the focus on strengthening cybersecurity continues to grow. Demonstrative efforts are noted in the FY20 CFTC President's budget, which explains the agency's ongoing commitment in making cybersecurity oversight an area of utmost importance.

While not specifically called out, the oversight related to registrants' cyber testing and sharing of information is embedded in Goal 2 - "Financial Integrity and Avoidance of Systematic Risk". Goal 2 ensures that the registered entities being referred are properly being managed and adhering to laws and regulations. Goal 3 - "Comprehensive Enforcement" ensures that violations and standards are properly being enforced and that compliance with the Commodity Exchange Act (CEA) is adhered to. Aside from having overall agency-wide strategic goals, the agency also has IT-specific strategic goals. While all IT strategic goals support cybersecurity oversight in general, Goal 3 - "Provide a stable, scalable and secure IT environment to ensure continuous operations" directly supports the agency's mission in strengthening cybersecurity oversight. Collectively, the 8 strategic goals work together to achieve

management's objectives. The specific goals related to cybersecurity and system safeguard oversight shows the agency's willingness to keep cybersecurity at the forefront of agency priorities.

CFTC Functions & Background

To promote market integrity, the CFTC polices the derivatives markets for various abuses. It also seeks to lower the risk of the futures and swaps markets to the economy and the public.

The agency oversees a variety of individuals and organizations. These include swap execution facilities, derivatives clearing organizations, designated contract markets, swap data repositories, swap dealers, futures commission merchants, commodity pool operators, and other entities.

The agency also oversees Designated Contracts Markets (DCMs) for financial products such as interest rates, stock indexes, and foreign currency. With passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act ([Dodd-Frank Act](#)), the agency also oversees the more than \$400 trillion swaps market, which is about twelve times the size of the futures market. The futures and swaps markets are essential to our economy and the way that businesses and investors manage risk. Farmers, ranchers, producers, commercial companies, municipalities, pension funds, and others use these markets to lock in a price or a rate. The CFTC works to ensure these hedgers and other market participants can use markets with confidence.

The CEA regulates the trading of commodity futures in the United States. Passed in 1936, it has been amended several times since then. The CEA establishes the statutory framework under which the CFTC operates. Under this Act, the CFTC has authority to establish regulations that are published in title 17 of the Code of Federal Regulations (CFR). The CFR serves as the CFTC's main source of authoritative regulations when it comes to cybersecurity and safeguard oversight of the agency's registrants. One of the CFTC's main responsibilities is to ensure that their registrants are adhering to these regulations.

The following office and divisions manage the cybersecurity oversight for registrants at CFTC:

1. Division of Clearing and Risk
2. Division of Market Oversight
3. Division of Swap Dealer and Intermediary Oversight (DSIO)-not discussed in this report

The two CFTC divisions in this report oversee Designated Contract Markets (DCMs), Swap Data Repositories (SDRs)², Swap Execution Facilities (SEFs)³, and Derivatives Clearing Organizations (DCOs).

Relevant CFTC Regulations

At the national level, flowing from Presidential Directives, the US Department of the Treasury (Treasury) developed a [framework](#) for cyber protection goals for the financial services industry. CFTC and the Securities and Exchange Commission (SEC), the two major derivatives regulators, each have established their approach to cyber resiliency at their respective regulated entities.

The following are rules and regulations that apply to the CFTC and its registrants:

² <https://www.cftc.gov/IndustryOversight/DataRepositories/index.htm>

³ <https://www.cftc.gov/IndustryOversight/TradingOrganizations/SEF2/sefhowto.html>

<i>Division</i>	<i>Registrants</i>	<i>Applicable Regulation(s)</i>
<i>DMO</i>	<i>SDRs</i>	CFR Rule 49.24 , 17 CFR Part 49 (<i>Swap Data Repositories</i>), § 49.24 (<i>System Safeguards</i>)
<i>DMO</i>	<i>SEFs</i>	CFR Rules 37.1400 and 37.1401 , 17 CFR Part 37 (<i>Swap Execution Facilities</i>), §§ 37.1400 (<i>Core Principle 14 – System Safeguards</i>) and 37.1401 (<i>Requirements</i>)
<i>DMO</i>	<i>DCMs</i>	CFR Rules 38.1050 and 38.1051 , 17 CFR Part 38 (<i>Designated Contract Markets</i>), Subpart U (<i>System Safeguards</i>), §§ 38.1050 (<i>Core Principle 20</i>) and 38.1051 (<i>General Requirements</i>).
<i>DCR</i>	<i>DCOs</i>	CFR Rule 39.18 , 17 CFR Part 39 (<i>Derivatives Clearing Organizations</i>), Subpart B (<i>Compliance with Core Principles</i>), § 39.18 (<i>System Safeguards</i>).

Audit Objective, Scope, and Methodology

The objective of this performance audit was to review existing CFTC policies and procedures to determine their level of cybersecurity safeguard oversight over the registrants in their market. The two divisions we reviewed were DCR and DMO.

The scope of the audit was to assess CFTC’s performance in reviewing cybersecurity safeguards in place at entities subject to CFTC regulatory oversight. The scope of this audit covered fiscal years 2016 through 2019. During this performance audit, we relied on information and data provided by CFTC, as well as applicable industry references. Professional judgment was applied to determine the audit scope and methodology needed to address the audit objective and in evaluating whether sufficient, appropriate evidence was obtained to address the audit objective.

The audit methodology for the performance audit consisted of:

1. Planning;
2. Evaluating CFTC’s policies and procedures for reviewing registrants’ cybersecurity policies (registrants’ cyber-related internal controls);
3. Assessing CFTC’s methods for identifying and documenting cybersecurity risks in order to provide guidance and respond to cybersecurity breaches at CFTC registrants;
4. Reviewing DCR and DMO registrant incident logs;
5. Reporting audit assessments to CFTC OIG;
6. Issuing a draft report;
7. Obtaining management comments on the draft report;
8. And issuing a final report.

Entities Registered with CFTC

Below captures the entities that were registered with the CFTC as of September 30, 2019:

Registrant Type	Number of Registrants	Oversight Division	Total DCR Registrants	Total DMO Registrants
DCO	16	DCR	16	N/A
DCM	15	DMO	N/A	15
SEF	20	DMO	N/A	20
		Totals	16	35

Best Practices

The best practices below were utilized by the audit team to determine the most applicable best practices for CFTC registrants:

Entity	Best practices
Securities and Exchange Commission (SEC)	<p>17 CFR Parts 229 and 249 Commission Statement and Guidance on Public Company Cybersecurity Disclosures</p> <p>17 CFR Parts 240, 242, and 249 Regulation Systems Compliance and Integrity</p> <p>17 CFR Parts 232, 240, and 249 Security-Based Swap Data Repository Registration, Duties, and Core Principles</p> <p>17 CFR Part 248 (<i>Regulations S-P, S-AM, and S-ID</i>), § 248.30 (<i>Procedures to Safeguard Customer Records and Information; Disposal of Consumer Report Information</i>) and § 248.201 (<i>Duties regarding the detection, prevention, and mitigation of identity theft</i>).</p> <p>CF Disclosure Guidance: Topic No. 2</p> <p>OCIE August 2017 – Observations from Cybersecurity Examinations</p> <p>OCIE May 2017 – Cybersecurity: Ransomware Alert</p> <p>OCIE September 2015 – Cybersecurity Examination Initiative</p> <p>OCIE Summary of 2014 – Cybersecurity Examination Sweep</p>
National Institute of Standards and Technology (NIST)	<p>National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1</p> <p>NIST's Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations</p>
National Futures Association (NFA)	<p>9070 – NFA Compliance Rules 2-9, 2-36 and 2 49: Information Systems Security Programs</p>
Financial Industry Regulatory Authority (FINRA)	<p>FINRA Small Firm Cybersecurity Checklist</p> <p>FINRA Report on Selected Cybersecurity practices 2018</p>
The Federal Financial Institutions Examination Council	<p>FFIEC Information Technology Examination Handbook Information Security SEPTEMBER 2016</p>




U.S. Commodity Futures Trading Commission
Three Lafayette Centre, 1155 21st Street, NW, Washington, DC 20581
www.cftc.gov

Heath P. Tarbert
Chairman and Chief Executive

(202) 418-5030
Chairman@cftc.gov

MEMORANDUM

TO: A. Roy Lavik, Inspector General

FROM: Heath P. Tarbert, Chairman and Chief Executive 

DATE: August 31, 2020

SUBJECT: Management Response to Performance Audit: CFTC's Policies and Procedures Regarding Oversight of Cybersecurity Safeguard by Registrants¹

On behalf of the Commission, I appreciate the opportunity to respond to the audit report prepared for the CFTC Office of the Inspector General ("OIG") by IntelliPath concerning the Divisions of Market Oversight ("DMO") and Clearing and Risk ("DCR") (collectively, "the Divisions") policies and procedures for conducting system safeguards reviews of the Designated Contract Markets ("DCMs"), Derivatives Clearing Organizations ("DCOs"), Swap Execution Facilities ("SEFs"), and Swap Data Repositories ("SDRs") regulated by the CFTC (collectively, the "registered entities"). DMO and DCR use their system safeguards oversight programs as tools for maintaining and improving registered entity cybersecurity and system safeguards. The Commission therefore welcomes OIG's recommendations for enhancing the effectiveness of these programs.

The Commission is pleased IntelliPath's audit concluded that CFTC and the Divisions have developed adequate policies and procedures to address proper cybersecurity safeguards at the registered entities, following relevant legislation and industry best practices for monitoring entity

¹ The term "registered entities" is used for the DCMs, SEFs, SDRs, and DCOs for which DMO and DCR conduct system safeguards oversight. The term "registrants" refers to the futures commission merchants, swap dealers, introducing brokers, and other market participants for which DSIO conducts oversight. Because this Report addresses DMO and DCR oversight, but not DSIO oversight, the Commission suggests changing the title of the Report to say "Registered Entities."

measures for reducing cybersecurity risk. The IntelliPath audit identified four areas where the Divisions could further improve their policies and procedures toward reducing entity cybersecurity risks, and made four related recommendations. The individual recommendations and the Divisions' plans for implementing them are discussed below.

1. Increase the number of dedicated employees to the Divisions' System Safeguard Examination (SSE) teams, in order to continuously assess cybersecurity risks at CFTC registrants.

In order to fully assess every registrant's ability to adhere to their own cybersecurity policies and procedures, the CFTC needs to consider increasing their resources when it comes to evaluating cybersecurity safeguards at registrant entities. Additionally, CFTC needs to consider solely designate personnel to its cybersecurity oversight initiatives, to allow for appropriate time and dedication towards the effort. Developing and increasing more specialized employees will help the CFTC establish a more robust SSE process and continually improve the entire cybersecurity safeguard testing process as well. By increasing the amount of dedicated staff, the CFTC can better achieve its Information Technology (IT) strategic goal #3: Provide a stable, scalable and secure IT environment to ensure continuous operations. Increasing staff can lower the risk that deficient cybersecurity operations exist in the registrant environments. Incident report logs received from two divisions demonstrate that not all responses to self-reported cybersecurity incidents were timely or consistent. All communication received from registrants should be received and acknowledged from CFTC personnel immediately, in order to assess whether action needs to be taken. By increasing the number of personnel, the CFTC can better ensure that all incidents will be tracked more consistently and addressed in a timely manner. Increasing personnel staff will also allow the commission to conduct timely, thorough, and in-depth examination process[es].

Number of Systems Risk Analysts and Frequency of Examinations

Both DMO and DCR agree that additional resources could allow for more and broader examinations of cybersecurity safeguards at registrant entities. And so do I. In particular, more specialized Systems Risk Analysts could conduct System Safeguards Examinations ("SSEs") and other supervisory activities for all registered entities at a frequency commensurate with the level of risk present in today's cybersecurity environment.

To that end, I stated in my keynote address to the joint meeting of the Financial and Banking Information Infrastructure Committee and the Financial Services Sector Coordinating Council on July 21, 2020 that cybersecurity is the biggest threat facing the financial sector today. This means the work of the Divisions' Systems Risk Analysts is essential to fulfilling the system safeguards aspect of the CFTC's mission. The automated systems of the registered entities play a critical role in today's predominantly electronic derivatives trading and clearing environment, as do their corresponding business continuity and disaster recovery plans. The importance of CFTC's system safeguards oversight is highlighted by the fact that it would present unacceptable risks to the U.S. financial system and the world economy should certain DCOs, DCMs, SEFs, or SDRs become inoperative—even for a relatively short period of time.

Systems Risk Analysts conduct SSEs and other supervisory activities that constitute the Divisions' system safeguards programs. As recognized in IntelliPath's audit report, these analysts also respond to notifications from registered entities concerning cybersecurity incidents, hardware or software malfunctions, cyber threats, and activations of business continuity or disaster recovery plans. Other duties include reviewing the system safeguards aspects of applications for designation or registration as a DCM, DCO, SEF, or SDR; providing system safeguards-related advice to Commissioners and senior CFTC staff, and contributing technical advice to CFTC staff when drafting regulations, conducting international comparability determinations, or preparing for legal actions.

At present, DMO conducts system safeguards oversight of a total of 38 registered entities, including 16 DCMs, 19 SEFs, and three SDRs. Of these, seven entities are considered systemically critical. It is vital that these entities be examined at least annually, via an SSE or other targeted oversight activity, as indicated by appropriate risk analysis in light of current circumstances. While the remaining 31 entities may have less potential to disrupt the nation's financial system if their operations are disrupted, they may also be somewhat more likely to experience catastrophic system failures or security breaches. Thus, DMO has determined these entities should be examined on at least a biennial basis.

DCR conducts system safeguards oversight of a total of 15 DCOs. Of these, two have been designated as Systemically Important Derivatives Clearing Organizations ("SIDCOs") by the Financial Stability Oversight Council. DCR is legally required to examine SIDCOs annually.² As relevant here, the Dodd-Frank Act has defined systemic importance as a situation where the failure of or a disruption to the functioning of a designated DCO could create, or increase, the risk of significant liquidity or credit problems which could spread and threaten the stability of the financial system of the United States.³ Given the potential consequences posed by emerging operational risks (e.g. crypto clearing operations) or, in a worst-case scenario, an actual disruption at a DCO, DCR employs a risk-based methodology to determine which DCOs require examination.

For this work, DMO presently has one Associate Director and three full-time System Safeguards Analysts and DCR has one Associate Director and six System Safeguards Analysts.⁴ Given these staffing levels, it would be extremely challenging for either Division to expand its oversight to examine the system safeguards of each registered entity for which it conducts oversight on a more frequent basis. Accordingly, as noted in the IntelliPath report, the Divisions have focused their examination activity on the most systemically important registered entities as well as those entities which each Division considers to pose a heightened level of risk.

I believe that today's level of cybersecurity threat makes system safeguards oversight of registered entities a critical priority. I know my fellow Commissioners do as well. On behalf of

² See Dodd-Frank Wall Street Reform and Consumer Protection Act, Title VIII, § 807(a).

³ See Dodd-Frank Wall Street Reform and Consumer Protection Act, Title VIII, § 803.

⁴ Staff participated in other supervisory activities in addition to the supervisory activities associated with system safeguards. During the review period several systems risk analysts were not available for assignments due to extended or short-term military deployments or exercises.

the Commission, I agree with the recommendation that we should consider increasing Systems Risk Analyst staff resources in both Divisions, specifically to enable more frequent and comprehensive assessment of every registered entity's ability to adhere to its own cybersecurity policies and procedures as well as the system safeguards requirements of the Commodity Exchange Act and CFTC regulations. To the extent consistent with other budgetary needs and position allocations, the CFTC under my leadership will prioritize directing the Divisions to implement this recommendation.

2. Conduct more thorough and in-depth testing [examinations] of registrants in order to validate that their cybersecurity policies and procedures are being adhered to.

Although our assessment found that current CFTC policies and procedures appropriately provide oversight over its registrants, there could be more operational examinations across all CFTC divisions. Often, the CFTC divisions did not examine certain registrants based on information from registrants (such as no major changes to the cybersecurity infrastructure and/or incidents from prior year) that were not indicative of deficient cybersecurity policies and procedures. Even though it is the registrant's responsibility to self-report any cybersecurity-related incident to the CFTC, there is still a possibility that not all information will be communicated to the CFTC. By requesting more robust and independent testing [examination] of registrants, CFTC will be able to validate that registrants are adhering to their policies and procedures. Additionally, conducting more localized on-site, in-depth testing [examinations] will provide the CFTC with more information on how registrants conduct their cybersecurity safeguard[s] testing. With this knowledge, the CFTC will be able to accumulate more industry specific cybersecurity risk information. Cataloging registrants' cybersecurity risks will enable CFTC to disseminate useable information to reduce cybersecurity risk among CFTC registrants.

The CFTC does perform ad-hoc testing [examinations] for certain registrants, but those registrants who undergo testing [examination] usually fall into a "high-risk" category. The risk assessment used for determining risk level is based off metrics that the commission utilizes. Often times, many registrants who are not deemed "high-risk" by the commission will not undergo a full SSE. This leaves the possibility that some registrants may be in violation of regulations. The division staff does provide a sound methodology for which registrants to test [examine] every year, but without validating a greater sample of registrants regardless of risk level, the CFTC cannot reduce the risk of non-compliant registrants. Lastly, some registrants may not undergo full SSEs for many years, leaving the opportunity for a potential cybersecurity threat to go undetected for long periods of time.

Incident Report Processing

On behalf of the Commission, I agree with the recommendation that improved and consistent tracking of cybersecurity incident reports from registered entities would enhance the Divisions' oversight of system safeguards. The reports received from registered entities vary considerably in their significance, as does the necessary response required by the receiving Division. The reports also vary in the manner by which they are submitted to CFTC. Many incident reports are sent to DMO by email via a dedicated mailbox, while others come by telephone or via the CFTC Portal. DCR receives all incident reports via the CFTC Portal.

All reports are currently reviewed by Systems Risk Analysts, who employ a risk-based approach in determining what further action, if any, is required. The Divisions plan to respond to the audit report's recommendation by implementing an improved method to track all incident reports and notify management of significant incidents.

Building of Registered Entity System Safeguards Profiles

On behalf of the Commission, I likewise agree with the audit report's observation that more frequent examinations to determine compliance with the CEA and implementing regulations will allow the Divisions to accumulate more industry specific cybersecurity risk information. The Divisions also agree that cataloging registered entity cybersecurity risks will assist the Divisions' continuing efforts to strengthen cyber resilience at registered entities.

The Divisions therefore plan to continue work already commenced on building and maintaining current system safeguards profiles of each DCM, SEF, SDR, and DCO. For this purpose, the Divisions plan to enhance their risk assessment procedures and request additional information from all registered entities, including the results of their mandatory cybersecurity tests. This additional information will aid in ensuring that all registered entities are performing cybersecurity testing as required under our regulations, and will enhance the results of risk assessments that aid determining which registered entities should be examined.

3. Implement better data tracking and data analytics tools in order to use available registrant's incident data to analyze and predict trends of potential cybersecurity threats, and to keep track of registrant communication with CFTC personnel.

CFTC designates a dedicated CFTC portal through which registrants can freely communicate any cybersecurity-related incident. Communication of that information across CFTC personnel could be improved, however. When a CFTC employee with oversight over a certain registrant receives [a] communication, other CFTC employees might not have that information in real time. If imminent and current cybersecurity threats are happening in real time, all appropriate CFTC employees need to be made aware so that senior leadership could decide on how to communicate those threats to other registrants in that market. Dissemination of information received from registrants could be more formalized to establish protocols and efficient processes to ensure relevant stakeholders (internal and external) receive information in a timely manner.

As information and data are communicated from registrants, the CFTC logs that information mainly for recordation purposes. By implementing a data analytics tool or enhanced dashboards, CFTC personnel could leverage the existing data to help analyze trends, predict certain risks, and to overall be better equipped to utilize the data in an effort to alert registrants of emerging cybersecurity threats.

This recommendation echoes some elements related to the system safeguards profile observations in recommendation Two. As noted above, the Divisions will work with our technology staff to implement an improved method to track all incident reports and provide notification of significant incidents to management.

On behalf of the Commission, I agree that when a cybersecurity incident is reported, it can be useful for other appropriate Division staff to also receive timely notification of the incident. The Divisions will streamline their communication protocols to ensure that senior management is appropriately notified of significant cybersecurity incidents.

Notably, the CFTC incident reports cannot be sent to other registered entities because they include confidential information received as part of the CFTC's oversight activities. As such, their disclosure is prohibited by the Commodity Exchange Act.⁵ However, I agree—on behalf of the Commission—with the report's observation that data analytic tools may be helpful to identify emerging vulnerabilities and the registered entities that may be impacted by such vulnerabilities. It may be possible for the Divisions to share appropriately anonymized cybersecurity information with other registered entities where such anonymization is possible, and the Divisions will explore this possibility.

4. Emphasize to CFTC registrants usage of information sharing facilities so as to promote rapid awareness of emerging cyber threats.

The CFTC currently encourages its registrants to report any potential threat in their market to the Financial Services Information Sharing and Analysis Center (FS-ISAC). This allows registrants to report any major incident anonymously so that all other financial industry entities are aware of potential issues that may affect them. However, it would be more beneficial for CFTC registrants to have a dedicated anonymous sharing platform within the financial derivatives markets, so that registrants can be made immediately aware if an incident occurs in one of their markets. Since the CFTC has their own regulatory measures that registrants must abide by, an information-sharing program dedicated to CFTC-related registrants can alert those registrants and better anticipate potential disruptions and changes. Moreover, it can ensure that CFTC meets its strategic goal #1 and #2, noted below.

On behalf of the Commission, I agree that emphasizing the use of information sharing facilities by registered entities to stay informed about current cyber threats is important. To implement this recommendation, the Divisions plan to send a joint communication to all registered entities urging them to sign up for alerts available from (1) the Department of the Treasury's Financial Sector Cyber Information Group and (2) the Department of Homeland Security Cybersecurity and Infrastructure Security Agency. This joint communication will also urge all registered entities to become members of the Financial Services Information Sharing and Analysis Center (FS-ISAC) if they have not already done so, so that they can receive the alerts available from that important source.

The Divisions also plan to remind registered entities that FS-ISAC has an information-sharing sub-group dedicated to derivatives markets and clearing organizations, which they are welcome to use. The Divisions will also note that exchanges and clearing organizations have also established their own information-sharing organization known as the Clearing House and Exchange Forum whose members actively communicate with each other about current threats.

⁵ See Commodity Exchange Act § 8(e), 7 USC § 12(e).

CFTC's oversight of the system safeguards of registered entities is important to the security of the U.S. financial system and the protection of the American people. Our Commission is committed to fulfilling its responsibilities for such oversight, and I very much appreciate the recommendations provided by OIG via the IntelliPath report to ensure the continued success of that mission.