Office of the Inspector General
U.S. Commodity Futures Trading Commission

Commodity Futures Trading Commission's Policies and Procedures For Reviewing Registrants' Cybersecurity Policies

October 11, 2016

--Blank Page--

U.S. COMMODITY FUTURES TRADING COMMISSION
OFFICE OF INSPECTOR GENERAL
Three Lafayette Centre
1155 21st Street, NW, Washington, DC 20581
Telephone: (202) 418-5110

TO: Timothy G. Massad, Chairman
Sharon Y. Bowen, Commissioner
J. Christopher Giancarlo, Commissioner

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

DATE: October 11, 2016

SUBJECT: Commodity Futures Trading Commission's Policies and Procedures for Reviewing Registrants' Cybersecurity Policies

Introduction

The Office of the Inspector General (OIG) contracted with Brown & Company to review existing CFTC policies and procedures toward reducing cybersecurity risks of CFTC registrants. Specifically, they reviewed:

- Division of Swap Dealer and Intermediary Oversight (DSIO) monitoring of registrants' IT infrastructure;
- Procedures examined by Division of Market Oversight (DMO) when it conducts System Safeguard Examinations;
- Division of Clearing and Risk (DCR) monitoring of IT systems at clearinghouses; and
- Office of Data and Technology (ODT) IT systems for protecting sensitive information received from registrants.

Highlights

Brown & Company highlighted that CFTC and its oversight divisions have developed policies and procedures to address cybersecurity risks at CFTC registrants and identified five areas with recommendations where the CFTC could improve its policies and procedures toward reducing cybersecurity risks of registrants. Specifically, the CFTC has the opportunity to improve data transfer protocols, frequency of registrant internal and external penetration and vulnerability testing, oversight assessments, and intelligence and information sharing.

Management Comments and OIG Evaluation

In reference to data transfer protocols, CFTC notified all entities who continue to use non-secure FTP that it will no longer allow these connections. Management's action is responsive and we closed recommendation 1.

In reference to the frequency of registrant internal and external penetration and vulnerability testing, the CFTC issued two parallel final rules regarding cybersecurity testing by registrants. These final rules require external and internal penetration and vulnerability testing at a frequency determined by appropriate risk analysis. Management's action is responsive and we closed recommendations 2 and 3.

Management did not concur with recommendation 4 for DSIO to use a risk-based approach to independently test the results of the assessments of cybersecurity preparedness at Futures Commission Merchants (FCM) and Swap Dealers (SD). Management conveyed a factual difference in Brown and Company's reference to the Securities and Exchange Commission and asserted that the report mischaracterizes CFTC's cybersecurity assessments as a request for information. Management conveyed that due to current budgetary constraints, the creation of an independent testing program is not feasible. Lastly, management highlighted that the National Futures Association (NFA) also reviews the cybersecurity programs of registrants. As such, CFTC will consider how best to leverage its resources and further rely on NFA's programs to address the critical issue of cybersecurity among registrants.

In reference to intelligence and information sharing (recommendation 5), management stated that extensive inf0rmation sharing arrangements are already in place. Notwithstanding existing information sharing mechanisms, the CFTC appreciates the recommendation and will keep it in mind as it continues to review such information sharing arrangements in the future.

The OIG appreciates CFTC's commitment to mitigating cyber security threats as well as CFTC's current budget constraints as reflected in our management challenges report. In reference to the accuracy of facts contained in the initial draft report, Brown and Company corrected the report as they determined appropriate. In reference to the vigor of the current assessments (recommendation 4), we recognize DSIO accepts supplied data for FCMs and SDs reviewed. Looking to federal assurance standards as a benchmark, CFTC could assess whether the evidence is relevant, valid, and reliable. For example, in establishing the appropriateness of evidence, CFTC could independently test its reliability by documenting supporting evidence or corroborating evidence. This approach validates registrants' responses and sharpens attention on cyber related risk at registrants. Given budget constraints, we believe the CFTC, at a minimum, can explore whether its own benchmark information security program and staff can assist oversight teams to further validate registrant cybersecurity preparedness. As such, we will keep recommendation 4 open for semiannual reporting to Congress and reassess its status at the conclusion of our ongoing audit of DSIO's oversight of the NFA.

In reference to recommendation 5, Brown and Company considered management's assertion responsive. We will monitor CFTC's actions regarding recommendation 5 for a follow-up audit.

Attached is Brown & Company's updated audit report. The report includes management's response in its entirety and Brown and Company's evaluation. The report will not be published on the OIG webpage. However, a synopsis will be presented in the CFTC OIG March 31, 2017 *Semiannual Report to Congress* and the open recommendations will be tracked by the OIG for audit follow-up. If you have any questions, please contact me at (202) 418-5084 or Tony Baptiste, project manager, at (202) 418-5115.

Cc: Eileen Flaherty, Director DSIO
Vincent McGonagle, Director, DMO
Jeffrey Bandman, Acting Director, DCR
John L. Rogers, Chief Information Officer, ODT
Anthony Thompson, Executive Director
A. Roy Lavik, Inspector General
Judith Ringle, Deputy Inspector General and Chief Counsel

Independent Audit Report

Performance Audit
Examination of the Commodity Futures Trading Commission's Policies and Procedures For Reviewing Registrants' Cybersecurity Policies

FINAL REPORT

Prepared by:

Brown & Company
Certified Public Accountants and Management Consultants, PLLC
1101 Mercantile Lane, Suite 122
Largo, Maryland 20774
(240) 770-4903

Date: September 29, 2016

Table of Contents

List of Figures

List of Tables

1. EXECUTIVE SUMMARY

On behalf of the U.S. Commodity Futures Trading Commission (CFTC), Office of Inspector General (OIG), Brown & Company CPAs and Management Consultants, PLLC, an independent public accounting firm, conducted a performance audit of CFTC's policies and procedures for reviewing registrants' cybersecurity policies. The objective of this performance audit was to review existing CFTC policies and procedures toward reducing cybersecurity risks of CFTC registrants,[1] as conducted by designated CFTC oversight divisions,[2] and for operational matters within the Office of Data and Technology (ODT).

The scope of the audit was to conduct an independent audit of CFTC's performance in reviewing information technology system safeguards in place at entities subject to CFTC regulatory oversight. We conducted this audit from September 25, 2015 through July 25, 2016. We relied on CFTC's annual Federal Information Security Modernization Act of 2014 (FISMA) report to gauge CFTC's adherence to federal best practices for federal agencies.

We conducted the audit in accordance with generally accepted government auditing standards (GAGAS), as stated in the Government Accountability Office's *Government Auditing Standards,* 2011 revision.

We conclude that CFTC and its oversight divisions have developed policies and procedures to address cybersecurity risks at CFTC registrants. CFTC has issued several rules and has conducted initiatives to address cybersecurity risk in the derivatives market space between 2010 and 2015, the scope of our audit. (See **Table 4**, CFTC Existing Policies and Procedures). On December 23, 2015, the CFTC issued proposed rules for enhancing and clarifying existing provisions relating to system safeguards, risk analysis, oversight, and cybersecurity testing for registrants.[3] However, our performance audit identified five areas where the CFTC could improve its policies and procedures toward reducing cybersecurity risks of registrants and offers five recommendations on how the Commission can do so.

Audit Findings:

1. CFTC should improve cybersecurity oversight by ensuring that all registrants use a secure file transfer protocol (SFTP) account for submitting sensitive financial information.
2. CFTC should provide guidance to registrants to increase the frequency of internal and external penetration testing for DCMs, SEFs, DCOs and SDRs.

[1] FY 2015 Registrants: futures commission merchants (FCMs), swap dealers (SDs), major swap participants (MSPs), retail foreign exchange dealers (RFEDs), introducing brokers (IBs), commodity pool operators (CPOs), commodity trading advisors (CTAs), designated contract markets (DCMs), swap execution facilities (SEFs), derivatives clearing organizations (DCOs), and swap data repositories (SDRs).
[2] Division of Swap Dealer and Intermediary Oversight (DSIO), Division of Market Oversight (DMO), and Division of Clearing and Risk (DCR), and Office of Data and Technology (ODT).
[3] 17 CFR Part 37, 38 and 49 System Safeguards Testing Requirements; Proposed Rules, 80 FR 801406 (December 23, 2015) http://www.cftc.gov/idc/groups/public/@lrfederalregister/documents/file/2015-32143a.pdf and 17 CFR Part 39 System Safeguards Testing Requirements for Derivatives Clearing Organizations , 80 FR 80114 (December 23, 2015) http://www.cftc.gov/idc/groups/public/@lrfederalregister/documents/file/2015-32144a.pdf.

3. CFTC should provide guidance to registrants to increase the frequency of vulnerability testing for DCMs, SEFs, DCOs and SDRs.
4. DSIO assessment should include testing to assess implementation of certain firm controls.
5. CFTC oversight guidance should encourage registrants to participate anonymously in intelligence and information sharing with CFTC.

Audit Recommendations:

1. We recommend appropriate CFTC divisions verify that registrants with reporting requirements use a SFTP account for filing sensitive financial information with CFTC.
2. We recommend the appropriate CFTC division encourage registrants to increase the frequency of internal and external penetration testing after any significant change in the registrant's network and testing after receiving information that could harm the network.
3. We recommend the appropriate CFTC division encourage registrants to increase the frequency of vulnerability testing to include scanning after any significant change in the network and scanning after receiving knowledge of new information that could harm the network.
4. We recommend DSIO use a risk-based approach to independently test the results of the assessments of cybersecurity preparedness at FCMs and SDs.
5. We recommend that CFTC develop an anonymous information-sharing program with registrants to stay current with cyber threats.

The detailed audit findings and recommendations are provided in **Section 4, *Audit Results*** of this report. The detailed audit objective, scope, and methodology are provided in **Appendix A** of this report. CFTC's Management Response is provided in **Section 6**.

This report is intended for use by the CFTC OIG and CFTC officials, and should not be distributed or used for any other purpose.

2. BACKGROUND

This report presents the following:

1. Overview of Commodity Futures Trading Commission (CFTC) (Commission) strategic goals designed to reduce cybersecurity threats affecting registrants and agency operations;
2. The CFTC divisions responsible for oversight of registrants' cybersecurity posture;
3. The current cybersecurity threat affecting registrants;
4. CFTC regulations designed to address cybersecurity at the registrants; and
5. Results of our audit and recommendations for improving cybersecurity controls at registrants.

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.

CFTC's strategic goals—designed to support the agency's mission—are outlined in **Table 1** below.

Table 1. CFTC Strategic Goals

Commodity Futures Trading Commission Strategic Plan 2011–2015 Strategic Goals[4]	
Goal 1: Market Integrity and Transparency	Protect the public and market participants by ensuring market integrity; promoting transparency, competition, and fairness; and lowering risk in the system.
Goal 2: Financial Integrity	Protect the public and market participants by ensuring the financial integrity of derivatives transactions, mitigation of systemic risk, and the fitness and soundness of intermediaries and other registrants.
Goal 3: Robust Enforcement	Protect the public and market participants through a robust enforcement program.
Goal 4: Cross-Border Cooperation	Enhance integrity of U.S. markets by engaging in cross-border cooperation, promoting strong international regulatory standards, and encouraging ongoing convergence of laws and regulation worldwide.
Goal 5: Organizational Excellence	Promote Commission excellence through executive direction and leadership, organizational and individual performance management, and effective management of resources.

[4] Commodity Futures Trading Commission Strategic Plan 2011–2015. http://www.cftc.gov/reports/strategicplan/2015/.

The CFTC Office of Inspector General (OIG) is required by statute to summarize the "most serious" management and performance challenges facing CFTC yearly. The OIG cited the following most serious management challenges for FY 2015:

OIG's Management Challenges for FY 2015
1. Minimize information security vulnerabilities in its network.
2. Stimulate registrants toward enhancing their cybersecurity controls over vital client information so as to reduce the impact of any future information technology breach.
3. Effectively triage oversight tasks in order to execute its strategic plan with limited budgetary resources.

The Commission historically has been charged by CEA with regulatory authority over the commodity futures markets. These markets have existed since the 1860s, beginning with agricultural commodities, such as wheat, corn and cotton.

Over time, the markets regulated by the Commission have grown to include contracts on energy and metals commodities, such as crude oil, heating oil, gasoline, copper, gold and silver, and contracts on financial products, such as interest rates, stock indexes and foreign currency. In the aftermath of the 2008 financial crisis—caused in part by the unregulated swaps market—President Obama and Congress charged the CFTC with reforming this market. The agency now also has regulatory oversight of the over $400 trillion swaps market, which is about 12 times the size of the futures market.[5]

CFTC Oversight Divisions

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

Division of Swap Dealer and Intermediary Oversight (DSIO)
Division of Market Oversight (DMO)
Division of Clearing and Risk (DCR)
Office of Data and Technology (ODT)

CFTC divisions oversee futures commission merchants (FCMs), swap dealers (SDs), major swap participant (MSP), retail foreign exchange dealers (RFEDs), introducing brokers (IBs), commodity pool operators (CPOs), commodity trading advisors (CTAs), designated contract markets (DCMs), swap execution facilities (SEFs)[6], derivatives clearing organizations (DCOs), swap data repositories (SDRs), and hereafter identified as registrants. ODT provides technology and data management support to CFTC components. **Figure 1.** depicts the oversight divisions and their registrants. (See also **Appendix B - CFTC Overview**).

[5] CFTC was charged with reforming the futures market http://www.cftc.gov/About/MissionResponsibilities/index.htm.
[6] For this report we view system safeguard requirements, as defined under core principles 20 for DCMs and 14 for SEFs, to possess no substantive difference and therefore comments related to DCMs can be applied to SEFs.

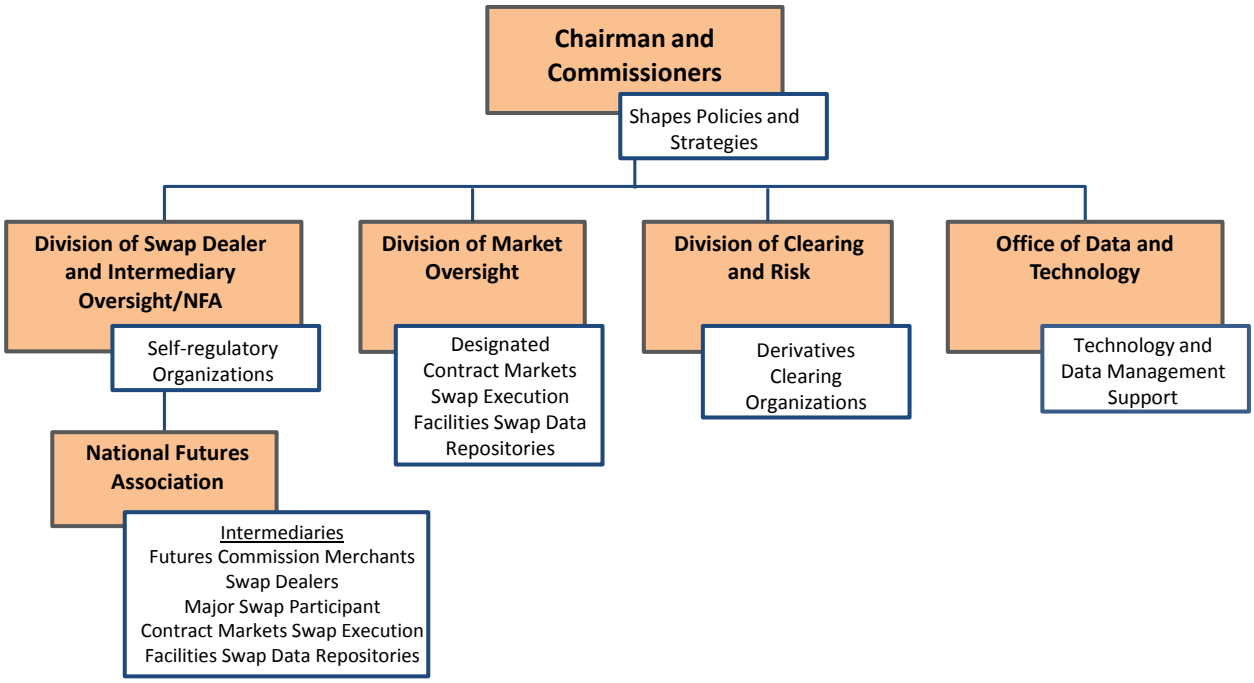

Figure 1. Cybersecurity Oversight Divisions and Their Respective Registrants

Cybersecurity Risks Affecting the Registrants

What is Cybersecurity?

Cybersecurity, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.[7] Firms defined "cybersecurity" in different ways. For purposes of this report, we apply Financial Industry Regulatory Authority's (FINRA) definition for cybersecurity as the protection of investor and firm information from compromise through the use—in whole or in part—of electronic digital media, (e.g., computers, mobile devices or Internet protocol-based telephony systems). "Compromise" refers to a loss of data confidentiality, integrity or availability.[8]

The Cybersecurity Threat Environment

Until recently, criminals whose aim was monetary theft or fraud conducted most cyber attacks on financial sector institutions. While such attacks continue, there has been a rise in attacks by politically motivated hacktivists or terrorists and by nation state actors, aimed at disruption of operations, theft of data or intellectual property, extortion, cyber espionage, corruption or destruction of data, and degradation or destruction of automated systems.

Cybersecurity experts participating in a 2015 Staff Roundtable on Cybersecurity and System Safeguards Testing informed the CFTC that recent studies have shown that the volume of cyber attacks is growing, therefore making it the number one concern for nearly half of all financial institutions in the United States.[9]

[7] http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm.
[8] https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf FINRA Report On Cybersecurity Practices—February 2015.
[9] 17 CFR Part 39 System Safeguards Testing Requirements for Derivatives Clearing Organizations (Escalating and Evolving Cybersecurity Threats), 80 Fed. Reg. 80113, 80137 (Dec. 23, 2015).

"*Total number of security incidents detected in 2014 increased by 48% over 2013, for a total of 42.8 million incoming attacks, the equivalent of more than 117,000 attacks per day, every day.*"

—PricewaterhouseCoopers Global State of Information Security Survey

"During 2014, the financial services sector experienced an average of 350 malware attacks per week."

—Verizon's 2015 Data Breach Investigations Report

"Cyber attacks against the financial system are becoming more frequent, more sophisticated and more widespread.''

—Bank for International Settlements

The interconnectivity between market participants, intermediaries, trading and clearing organizations increases the cyber threat landscape for the futures trading financial market. As described by the National Futures Association (NFA),[10] intermediaries may have websites that are available to customers and counterparties for opening accounts, trading, and accessing account information, and rely upon electronic means to enter customer, counterparty and proprietary orders. Intermediaries either directly or indirectly connect electronically with other intermediaries, exchanges, clearinghouses, third-party service providers, self-regulatory organizations (SROs) and CFTC. In addition, intermediaries use electronic means to collect and maintain customer and counterparty information. Risk is compounded for firms that are part of a larger holding company structure that shares information systems security personnel, resources, systems and infrastructure.[11]

In June 2011, the FINRA conducted a survey of 224 firms to understand their cybersecurity practices and to learn what issues they were facing in protecting investors and maintaining market integrity. In 2014, FINRA took a step further and conducted a cybersecurity sweep across firms that included large investment banks, clearing firms, online brokerages, high-frequency traders and independent dealers. Both surveys revealed that firms are challenged by cyber risks of malevolent actors penetrating their systems. Some actors seek to gain network access to steal assets, deface data, and manipulate accounts. Some firms are also subject to operational risk associated with environmental problems (e.g., power failures) or natural disasters (e.g., earthquakes, hurricanes) and insider risk of employees or other authorized users abusing their access by harvesting sensitive information or otherwise manipulating the system or data.[12]

CFTC held a Cybersecurity and System Safeguards Roundtable meeting on March 8, 2015 to discuss cybersecurity threats facing the financial futures trading industry. The meeting focused on the need for testing cybersecurity defenses in the current environment, as well as system safeguards testing and associated risk assessment practices. These practices included vulnerability and penetration testing, key controls testing, and business continuity-disaster recovery testing.

[10] The NFA is a registered futures association under section 17 of the Commodity Exchange Act (CEA) established to safeguard market integrity, protect investors and assist members with meeting regulatory requirements.
[11] NFA explains the interconnectivity of intermediaries and the information they collect. http://www.nfa.futures.org/news/PDF/CFTC/InterpNotc_CR2-9_2-36_2-49_InfoSystemsSecurityPrograms_Aug_2015.pdf.
[12] FINRA, 2011 survey and 2014 examination results, https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.

At the meeting, CFTC Chairman, Mr. Massad, stated:

> "Cybersecurity is the most important single issue facing markets today in terms of market integrity and financial stability, and the examples of cyber attacks unfortunately are all too frequent and familiar, whether JP Morgan or Home Depot, Target, or Sony. Some of our nation's exchanges have been hit or suffered other technological problems that have caused outages or raised concerns."[13]

3. 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 CFTC has approved the NFA Information Systems Security Programs, which became effective on March 1, 2016.[14] The program requires NFA members to establish cybersecurity policies and controls to protect information systems and customer data. **Figure 2** below shows the hierarchy of regulators that issue policies and guidance for CFTC registrants.

Presidential Policy Directive-21 (PPD-21)[15] states that all Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and security of their respective internal critical infrastructure that supports primary mission and essential functions. Therefore, this audit builds on PPD-21's goals for enhancing cybersecurity in the financial services sector as one of our nation's 16 critical infrastructures and examines CFTC's efforts at identifying and mitigating cybersecurity risk at CFTC registrants. Treasury's mission includes its role as the steward of U.S. economic and financial systems and as an influential participant in the world economy.

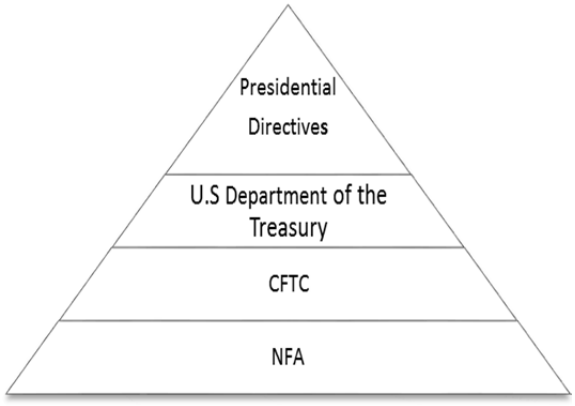

Figure 2.Oversight Hierarchy of Regulators

The CFTC is subject to CEA, the Commodity Futures Modernization Act of 2000, Dodd-Frank Wall Street Reform and Consumer Protection Act and others. The CFTC's regulations are recorded under Title 17, Chapter I of the Code of Federal Regulations (CFR) Commodity Futures Trading Commission.

[13] CFTC Roundtable opening comments from CFTC Chairman, http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/transcript031815.pdf.
[14] http://www.nfa.futures.org/news/newsNotice.asp?ArticleID=4701 Notice I-16-10, February 29, 2016, Self-Examination Questionnaire—Cybersecurity. The Cybersecurity Interpretive Notice will become effective on March 1, 2016, and applies to all membership categories.
[15] Presidential Policy Directive -- Critical Infrastructure Security and Resilience. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Table 2 lists current policies and rules issued by CFTC and NFA that cover system safeguard oversight.

Table 2. CFTC's Registrants, Oversight Divisions and Regulations

Critical Cybersecurity Requirements for Intermediaries		
Registrants	**Division**	**CFTC and National Futures Association**
FCMs, SDs, MSPs, RFEDs, IBs, CPOs and CTAs	DSIO/NFA	• 17 CFR § 160.30 Procedures to safeguard customer records and information • 17 CFR Parts 1, 3, 23, and 170 Registration of Swap Dealers and Major Swap Participants; Final rules, January 19, 2012[16] • 17 CFR § 23.600 Risk Management Program for swap dealers and major swap participants • 17 CFR Parts 230, 240 and 241 Further Definition of "Swap," "Security-Based Swap," and "Security-Based Swap Agreement;" Mixed Swaps; Security-Based Swap Agreement Recordkeeping; Final Rule, August 13, 2012[17] • CFTC Announces Real-Time Public Reporting of Swap Transactions and Swap Dealer Registration Began December 31, 2012[18] • 17 CFR Part 3 Registration of Intermediaries, August 28, 2012[19] • 17 CFR § 1.11 Risk Management Program for Futures Commission Merchants • NFA Information Systems Security Programs Proposed Adoption of the Interpretive Notice to NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs (Issued August 28, 2015, Effective March 1, 2016) [20]; and • NFA Manual /Rule Book [21]
Critical Cybersecurity Requirements for Designated Contract Markets		
Registrants	**Division**	**CFTC**
DCMs	DMO	• 17 CFR Parts 1, 16, and 38 Core Principles and Other Requirements for Designated Contract Markets; Final Rule, June 19, 2012[22] • 17 CFR Part 37, 38 and 49 System Safeguards Testing Requirements; Proposed Rules, December 23, 2015[23]

[16] Registration of Swap Dealers and Major Swap Participants; Final Rule, 77 FR 2613 (Jan. 19, 2012). http://www.cftc.gov/LawRegulation/FederalRegister/FinalRules/2012-792.

[17] Commodity Futures Trading Commission, 17 CFR Part 1, Securities and Exchange Commission, 17 CFR Parts 230, 240 and 241, Further Definition of "Swap," "Security-Based Swap," and "Security-Based Swap Agreement"; Mixed Swaps; Security-Based Swap Agreement Recordkeeping. 77 FR 48207 (Aug. 13, 2012). http://www.cftc.gov/idc/groups/public/@lrfederalregister/documents/file/2012-18003a.pdf.

[18] CFTC open meeting to propose final rules for swap dealer registration under the Dodd-Frank Act: registration standards, duties and core Principles http://www.cftc.gov/PressRoom/PressReleases/pr6085-11.

[19] Registration of Intermediaries, Final Rule, 77 FR 51898 (Aug. 28, 2012) http://www.cftc.gov/LawRegulation/FederalRegister/FinalRules/2012-20962.

[20] NFA Information Systems Security Programs Proposed, https://www.nfa.futures.org/nfamanual/NFAManual.aspx?RuleID=9070&Section=9.

[21] NFA Manual and rules http://www.nfa.futures.org/nfamanual/indexNFAManual.aspx.

[22] 17 CFR Parts 1, 16, and 38 Core Principles and Other Requirements for Designated Contract Markets; Final Rule, 77 FR 36611 (June 19, 2012), http://www.cftc.gov/LawRegulation/FederalRegister/FinalRules/2012-12746.

[23] See footnote[3].

Critical Cybersecurity Requirements for Swap Execution Facilities		
Registrants	**Division**	**CFTC**
SEFs	DMO	• 17 CFR Part 37 Core Principles and Other Requirements for Swap Execution Facilities, June 4, 2013[24] • 17 CFR Part 37, 38 and 49 System Safeguards Testing Requirements; Proposed Rules, December 23, 2015[25]
Critical Cybersecurity Requirements for Derivatives Clearing Organizations		
Registrants	Division	CFTC
DCOs	DCR	• 17 CFR Parts 1, 21, 39, and 140 Derivatives Clearing Organization General Provisions and Core Principles; November 8, 2011[26] • 17 CFR Part 39, System Safeguards Testing Requirements for Derivatives Clearing Organizations; Proposed Rule, December 23, 2015[27]
Critical Cybersecurity Requirements for Swap Data Repositories		
Registrants	**Division**	**CFTC**
SDRs	DMO	• 17 CFR Part 37, 38 and 49 System Safeguards Testing Requirements; Proposed Rules, December 23, 2015[28]

4. AUDIT RESULTS

We conclude that CFTC ODT and oversight divisions have made progress in developing policies and procedures toward reducing cybersecurity risks at CFTC registrants. For current policies and initiatives taken by CFTC refer to **Table 4**. Our performance audit identified the following opportunities for improvement to CFTC system safeguards risk analysis, oversight and cybersecurity testing for registrants. We used financial industry best practices (**Appendix C)** to identify gaps in CFTC's cybersecurity policies and procedures and to develop the following findings and recommendations. **Appendix D** illustrates finding 2 and 3.

Finding No. 1: CFTC should improve cybersecurity oversight by ensuring that all registrants use a secure FTP account for submitting sensitive financial information.

Condition:

Some CFTC registrants with reporting requirements use non-secure file transfer protocol (FTP) accounts. The appropriate oversight division should validate that all registrants have secure FTP (SFTP) accounts to submit sensitive information to CFTC.

CFTC operates a comprehensive system for collecting information on market participants as part of its market surveillance program. Under CEA, CFTC is required to collect market data and position information from exchanges, clearing members, FCMs, foreign brokers, and traders.

[24] 17 CFR Part 37 Core Principles and Other Requirements for Swap Execution Facilities, 78 FR 33475 (June 4, 2013). http://www.cftc.gov/LawRegulation/FederalRegister/FinalRules/2013-12242.
[25] "See footnote[3]".
[26] 17 CFR Parts 1, 21, 39, and 140 Derivatives Clearing Organization General Provisions and Core Principles, 78 FR 33475 (June 4, 2013) http://www.cftc.gov/LawRegulation/FederalRegister/FinalRules/2011-27536.
[27] "See footnote[3]".
[28] "See footnote[3]".

Some registrants are allowed to submit this data to CFTC using unsecured FTP methods. Unsecured FTP methods transmit data, including user names, passwords and sensitive financial data in plain text rather than concealing through encryption.

Criteria:

Federal Information Processing Standards (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules* requires the use of encryption to hide a user name and password transmitted over the Internet.

Cause:

ODT FTP servers accept data transmission from unsecured and secured FTP protocols.[29] ODT is working with registrants to transition from unsecured FTP to SFTP.[30]

Effect:

Because FTP is an unsecured protocol, there is increased opportunity for hackers to intercept registrants' login details or eavesdrop inside the file while it is being transferred over the public Internet. This puts registrants' login credentials at risk and allows hackers to submit unauthorized data in the name of a registrant's without the registrant's knowledge.

[29] CFTC audit interview of ODT staff. ODT staff reported that 10% of registrants use unsecured FTP to submit financial data to CFTC.

[30] CFTC Technical Guidance Document provides technical specifications for transmitting Forms 102A, 102B, 102S, 40 and 71 via FTP XML and Connect to CFTC with Secure FTP submissions, May 25, 2016. http://www.cftc.gov/idc/groups/public/@forms/documents/generic/ocrtechguideapr132016.pdf.

Recommendation 1:

We recommend appropriate CFTC divisions verify that registrants with reporting requirements use a SFTP account for filing sensitive financial information with CFTC.

Management's Response:

See **Section 6** for management's response.

Finding No. 2:	**CFTC should provide guidance to registrants to increase the frequency of internal and external penetration testing for DCMs, SEFs, DCOs and SDRs.**

Condition:

CFTC should provide guidance to registrants to increase the frequency of internal and external penetration testing. The FINRA report stated "in both the 2014 sweep and the 2011 survey, firms identified hackers penetrating firm systems"[31] as the number one threat.

DMO and DCR system safeguard testing requirements recommend that DCMs, SEFs, DCOs and SDRs perform internal and external penetration testing at a frequency determined by an appropriate risk analysis and at least annually for covered DCMs, SEFs, DCOs and SDRs. However, the requirements for penetration testing does not include testing after any significant change in the registrant's network and testing after receiving information that could harm the network.

Criteria:

Best practices applicable to DCMs, SEF, DCOs, and SDRs.

1. **17 CFR Part 37, 38 and 49, *System Safeguards Testing Requirements; Proposed Rules*, December 23, 2015,** states:

   > The proposed rules would require a DCM, SEF, or SDR to conduct external penetration testing that is sufficient to satisfy the scope requirements in proposed § 38.1051(k), 37.1401(k), and 49.24(l), at a frequency determined by an appropriate risk analysis. At a minimum, covered DCMs and SDRs would be required to conduct external penetration testing no less frequently than annually.

2. **17 CFR Part 39, *System Safeguards Testing Requirements for Derivatives Clearing Organizations; Proposed Rule*, December 23, 2015,** states:

   > Proposed § 39.18(e)(3)(i) would require a DCO to conduct external penetration testing at a frequency determined by an appropriate risk analysis, but at a minimum no less frequently than annually.

[31] https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf, Report on Cybersecurity Practices—February 2015.

3. **SEC 17 CFR Parts 240, 242, and 249 Regulation Systems Compliance and Integrity; Final Rule, December 5, 2014,** states:

   Rule 1003(b)(1)(i)

   Regular Penetration test reviews of the network, firewalls, and production systems shall be conducted at a frequency of not less than once every three years.

4. **Payment Card Industry (PCI) Data Security Standard, v3.2, April 2016,** states:

   Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

Cause:

DMO and DCR have proposed annual penetration-testing criteria for DCMs, SEFs, DCOs and SDRs. CFTC's requirement exceeds the SEC requirements at a frequency of not less than once every three years. However, the annual penetration-testing requirement may not reduce current cyber threats affecting registrant.

Effect:

Without conducting external penetration testing after significant changes in the network or notification of significant threat, vulnerabilities such as installing default passwords, leaving unused ports open and losing segmentation of protective environments could go undetected for days.

Recommendation 2:

We recommend the appropriate CFTC division encourage registrants to increase the frequency of internal and external penetration testing to testing after any significant change in the registrant's network and testing after receiving information that could harm the network.

Management's Response:

See **Section 6** for management's response.

Finding No. 3	**CFTC should provide guidance to registrants to increase the frequency of vulnerability testing for DCMs, SEFs, DCOs and SDRs.**

Condition:

CFTC should provide guidance to registrants to increase the frequency of vulnerability testing. The FINRA report stated "in both the 2014 sweep and the 2011 survey, firms identified hackers penetrating firm systems"[32] as the number one threat.

DMO and DCR system safeguard testing requirements recommend that DCMs, SEFs, DCOs and SDRs perform vulnerability testing at a frequency determined by an appropriate risk analysis and at least quarterly for covered DCMs, SEFs, DCOs and SDRs. The requirements for vulnerability testing do not include scanning after any significant change in the registrant's network and scanning after receiving information that could harm the network.

Criteria:

1. **17 CFR Part 37, 38 and 49, *System Safeguards Testing Requirements; Proposed Rules*, December 23, 2015,** states:

   > The proposed rules would require a DCM, SEF, or SDR to conduct vulnerability testing that is sufficient to satisfy the testing scope requirements in proposed §§38.1051(k), 37.1401(k), and 49.24(l), at a frequency determined by an appropriate risk analysis. At a minimum, covered DCMs and SDRs would be required to conduct vulnerability testing no less frequently than quarterly.

2. **17 CFR Part 39, *System Safeguards Testing Requirements for Derivatives Clearing Organizations; Proposed Rule*, December 23, 2015,** states:

   > Regulation 39.18(e)(2)(i) requires a DCO to conduct vulnerability testing at a frequency determined by an appropriate risk analysis, but at a minimum no less frequently than quarterly.

3. **NIST *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 12, 2014,** states:

   > Security Continuous Monitoring: The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. Vulnerability scans are performed.

4. **PCI Council, *Payment Card Industry Data Security Standard*, v3.2, April 2016,** states:

   > The PCI Council that issues system safeguards for businesses that process, store and transmit credit card data requires vulnerability scanning at least quarterly and after any significant change in the network. This would allow the organization to capture unknown threats that may have entered the network during a change such as operating systems upgrade, software patch or a hardware upgrade.

[32] https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf, Report on Cybersecurity Practices—February 2015.

5. **The Center on Cyber Security, *The Critical Security Controls for Effective Cyber Defense,* version 6.0, October 15, 2015.**[33]

   Critical Security Control (CSC) 4.1 – Continuous Vulnerability Assessment and Remediation states:

   > Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis.

Cause:

DMO and DCR have issued new vulnerability testing criteria for DCMs, SEFs, DCOs and SDRs. Performing vulnerability testing after significant changes and after receiving new information on unknown threats could impose additional costs to registrants.

Effect:

Without conducting vulnerability testing after significant changes in the network, vulnerabilities -- such as installing default passwords and losing segmentation of protective environment-- could go undetected for days. Delaying vulnerability testing until the next quarterly scan leaves the network open to attack.

Recommendation 3:

We recommend the appropriate CFTC division encourage registrants to increase the frequency of vulnerability testing to include scanning after any significant change in the network and scanning after receiving knowledge of new information that could harm the network environment.

Management's Response:

See **Section 6** for management's response.

Finding No. 4	**DSIO assessment should include testing to assess implementation of certain firm controls.**

Condition:

DSIO conducted assessments of cybersecurity preparedness for 48 FCMs and 49 SDs and 7 jointly registered FCM/SDs as part of the DSIO's "Cybersecurity Examination Initiative." The assessments included a preliminary request for information related to cybersecurity practices that may be contained in the policies and procedures constituting a firm's Risk Management Program. The request for information was based, in large part, on a similar cybersecurity examination initiative started by the SEC in 2014 and continued in 2015. However, the DSIO assessment did not include testing to assess implementation of certain firm's controls.

[33] The CIS Controls are especially relevant because they are updated by cyber experts based on actual attack data pulled from a variety of public and private threat sources, https://www.cisecurity.org/critical-controls.cfm.

Criteria:

1. **17 CFR Parts 1, 3, 22, 30, *Enhancing Protections Afforded Customers and Customer Funds Held by Futures Commission Merchants and Derivatives Clearing Organizations*, Final Rule, 78 FR 68506, 68517 (Nov. 14, 2013)**, **§1.11: Risk Management Program for Futures Commission Merchants,** states:

   > The Commission proposed new §1.11 to require each FCM that carries customer accounts to establish a ''Risk Management Program,'' as defined in §1.11(c), designed to monitor and manage the risks associated with the FCM's activities as an FCM. Under the Commission's proposal, the Risk Management Program must: (1) consist of written policies and procedures that have been approved by the ''governing body'' (defined below) of the FCM and furnished to the Commission; and (2) establish a risk management unit that is independent from an FCM's ''business unit'' (defined below) to administer the Risk Management Program.

2. **17 CFR Part 23 Subpart J §23.600 Risk Management Program for Swap Dealers and Major Swap Participants,** states:

   > (b) Risk management program – (1) Purpose. Each swap dealer and major swap participant shall establish, document, maintain, and enforce a system of risk management policies and procedures designed to monitor and manage the risks associated with the swaps activities of the swap dealer or major swap participant. For purposes of this regulation, such policies and procedures shall be referred to collectively as a "Risk Management Program."

3. **SEC, National Examination Program (NEP), Office of Compliance Inspections and Examinations (OCIE). *Examination Information for Entities Subject to Examination or Inspection by the Commission*** states:

   > Examination staff will seek to determine whether the entity being examined is conducting its activities in accordance with the federal securities laws and rules adopted under these laws.
   >
   > The Office of Compliance Inspections and Examinations (OCIE) conducts examinations of the broker-dealers and investment advisors pursuant to Rule 30(a) of Regulation S-P (17 CFR § 248.30(a)) (the "Safeguards Rule").

Cause:

Based on interviews with DSIO management, DSIO has not included testing as part of the assessment process due to limited resources.

Effect:

The DSIO assessment without testing will not effectively assess cybersecurity preparedness in the market space, including FCM's and SD's ability to protect market participants and customers.

Recommendation 4:

We recommend DSIO use a risk-based approach to independently test the results of the assessments of cybersecurity preparedness at FCMs and SDs.

Management's Response:

See **Section 6** for management's response.

Finding No. 5	**CFTC oversight guidance should encourage registrants to participate anonymously in intelligence and information sharing with CFTC.**

Condition:

CFTC's oversight guidance should encourage DCMs, SEFs and SDRs intelligence and information sharing with CFTC. Information sharing is essential for protecting the infrastructure of CFTC and to furthering cybersecurity for the registrants. Best practices for securing information and information systems require implementation of procedures for intelligence and information sharing to help alert other stakeholders of potential attacks and provide critical actionable information to speed and bolster defenses.

Criteria:

1. **Executive Order 13691, *Promoting Cybersecurity Information Sharing,* , February 13, 2015,** states

   > Entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible. Information Sharing and Analysis Organizations (ISAOs) membership may be drawn from the public or private sectors, or consist of a combination of public and private sector organizations. ISAOs may be formed as for-profit or nonprofit entities.

2. **NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February 12, 2014**, states:

   > Response Communications:
   >
   > Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
   >
   > Recover Communications:
   >
   > Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims and vendors.

Cause:

CFTC has developed an information-sharing program to share market data with other agencies to benefit customers and strengthen oversight of the commodity futures and options markets, but CFTC has not developed an anonymous information-sharing program with CFTC registrants to address cyber threats.

Effect:

Lack of intelligence and information sharing between CFTC and its registrants, increases the risk of registrants not receiving notices needed to protect the network environments from harmful malware and cyberattacks.

Recommendation 5:

We recommend that CFTC develop an anonymous information-sharing program with registrants to stay current on cyber threats.

Management's Response:

See **Section 6** for management's response.

5. EVALUATION OF MANAGEMENT'S RESPONSE

Management generally concurs with all but one of the findings and recommendations. Management actions are responsive to the recommendations by the issuance of rules and procedures that follow Recommendations 1, 2, 3, and 5. In regard to Recommendation 1, Management has notified all entities that CFTC will no longer allow non-secure FTP connections to the CFTC.

In reference to Recommendations 2 and 3, management asserts that the frequency of registrant internal and external penetration and vulnerability testing have been resolved through CFTC issuance of two parallel final rules regarding system safeguards cybersecurity testing by registrants. These final rules require external and internal penetration and vulnerability testing at a frequency determined by appropriate risk analysis and are responsive to the recommendation.

Management disagrees with Recommendation 4 for DSIO to use a risk-based approach to independently test results of the cybersecurity assessments of FCMs and SDs by existing CFTC staff. However, validating registrant data submitted in the assessments can enhance the agency's ability to effectively deploy its limited staff resources and may reduce cybersecurity risks at registrants.

We clarified Finding No. 4 "Condition" presented in the draft report and restated the quantity of assessments performed by DSIO.

In regards to Recommendation 5, Management asserts that information-sharing arrangements are in place among CFTC registrants, and some—but not all—CFTC registrants can anonymously access threat information through affiliates and other industry sources. Management is responsive in its decision to continue monitoring the recommendation.

Management's comments can be found in its entirety in Section 6 **Management's Response**.

6 MANAGEMENT'S RESPONSE

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

Timothy G. Massad
Chairman

(202) 418-5050
tmassad@CFTC.gov

MEMORANDUM

TO: Roy Lavik, Inspector General

DATE: September 28, 2016

SUBJECT: Management Response to the Draft OIG Audit of CFTC's Policies and Procedures for Reviewing Registrants' Cybersecurity Policies

The Commission sincerely appreciates the opportunity to review the Draft OIG Audit of CFTC's Policies and Procedures for Reviewing Registrants' Cybersecurity Policies and submits the following management responses:

OIG Recommendation 1*: We recommend appropriate CFTC divisions verify that registrants with reporting requirements use a SFTP account for filing sensitive financial information with CFTC.*

CFTC Response: We have notified all entities who continue to use non-secure FTP that we will no longer allow these connections to the CFTC after 5pm on Friday, September 30, 2016.

In 2012, the CFTC began requiring that all new market participants obtain a secure FTP account, and utilize that account when transmitting data to us. However, some legacy data providers reporting certain pre-Dodd-Frank data to the Commission were not asked to upgrade their data transmissions to Secure FTP. The only data providers which submitted data in this manner were FCM's providing Futures and Options position information related to CEA Part 17. Data providers such as registrants submitting financial statements, segregation computations, and segregated investment detail reports via WinJammer™ are not affected by this condition as WinJammer™ already utilizes secure FTP.

In March 2016, the CFTC began contacting data reporters (FCMs and their vendors) whom we identified were using non-secure FTP software to send data to us. In many cases, the data providers are using software provided by a third party vendor (e.g. SunGard) to send data to the CFTC. The software connection may be coming through the vendor's location as opposed to the actual reporter, so research has been required to identify the actual party that is making the

connection. The CFTC has worked through the summer to reduce the number of connections we receive using non-secure FTP. As of September 21, 2016, 16 entities were connecting to the CFTC using non-secure FTP, and the remaining entities have been contacted and are aware that after September 30, 2016 we will no longer allow them to submit data in this manner.

OIG Recommendation 2: *We recommend the appropriate CFTC division encourage registrants to increase the frequency of internal and external penetration testing to testing after any significant change in the registrant's network and testing after receiving information that could harm the network.*

CFTC Response: The Commission has already addressed this recommendation. On September 8, 2016, the Commission issued two parallel final rules regarding system safeguards cybersecurity testing by (1) DCMs, SEFs, and SDRs, and (2) DCOs. These final rules require all these critical infrastructures to conduct both external and internal penetration testing at a frequency determined by appropriate risk analysis. In addition, the final rules require covered DCMs (as defined), all SDRs, and all DCOs to conduct external and internal penetration testing no less frequently than annually. These requirements are in line with generally accepted system safeguards standards and best practices.

While testing after significant changes to the registrant's network or receipt of information that could harm the network is not expressly addressed in the new system safeguards rule, the rule nevertheless requires testing after these events. Specifically, the frequency for penetration testing is determined by "an appropriate risk analysis," and any appropriate and compliant analysis will identify significant changes and receipt of potentially harmful information as risks that necessitate prompt testing. In fact, the preamble language accompanying the proposal of both parallel rules listed several example factors an appropriate risk analysis should consider, and these included "the frequency and extent of changes in the organization's automated systems and operating environment." [1]

OIG Recommendation 3: *We recommend the appropriate CFTC division encourage registrants to increase the frequency of vulnerability testing to include scanning after any significant change in the network and scanning after receiving knowledge of new information that could harm the network environment.*

CFTC Response: The Commission has already addressed this recommendation. On September 8, 2016, the Commission issued two parallel final rules regarding system safeguards cybersecurity testing by (1) DCMs, SEFs, and SDRs, and (2) DCOs. These final rules require all these critical infrastructures to conduct vulnerability testing at a frequency determined by appropriate risk analysis. In addition, the final rules require covered DCMs (as defined), all SDRs, and all DCOs to conduct vulnerability testing no less frequently than quarterly. These requirements are in line with generally accepted system safeguards standards and best practices.

[1] System Safeguards Testing Requirements, 80 Fed. Reg. 80140, 80150 (Dec. 23, 2015); System Safeguards Testing Requirements for Derivatives Clearing Organizations, 80 Fed. Reg. 80114, 80118 (Dec. 3, 2015).

While testing after significant changes to the registrant's network or receipt of information that could harm the network is not expressly addressed in the new system safeguards rule, the rule nevertheless requires testing after these events. Specifically, the frequency for vulnerability testing is determined by "an appropriate risk analysis," and any appropriate and compliant analysis will identify significant changes and receipt of potentially harmful information as risks that necessitate prompt testing. In fact, the preamble language accompanying the proposal of both parallel rules listed several example factors an appropriate risk analysis should consider, and these included "the frequency and extent of changes in the organization's automated systems and operating environment."[2]

OIG Recommendation 4: *We recommend DSIO use a risk-based approach to independently test the results of the assessments of cybersecurity preparedness at FCMs and SDs.*

CFTC Response: Although the Commission appreciates the benefits that an independent testing program may provide, the Commission disagrees with the conclusion stated in the audit report that the absence of such a program will render DSIO unable to "effectively assess cybersecurity preparedness in the market space." The Commission notes that the recommendation appears to be based, at least in part, on an incorrect factual predicate: that the SEC's Office of Compliance Inspections and Examinations ("SEC-OCIE") has conducted the independent testing that is being recommended. Through conversations with SEC-OCIE staff, Commission staff has confirmed that the SEC-OCIE has not performed such testing. The Commission also notes that, due to current budgetary constraints, the creation of an independent testing program is not feasible.

The Commission further notes that the audit report's description of DSIO's cybersecurity assessments does not accurately reflect the examinations that were conducted. First, the audit report states that "DSIO conducted assessments of cybersecurity preparedness for 71 FCMs and 104 SDs," when, in fact, the assessment was performed on 48 FCMs, 49 SDs and 7 jointly registered FCM/SDs. Using a risk-based approach, DSIO focused its assessment on FCMs that maintain customer segregated funds and on US-based SDs. Second, the audit report mischaracterized the cybersecurity assessments as a "request for information" that "included a preliminary request for information related to cybersecurity practices that may be contained in the policies and procedures constituting a firm's Risk Management Program." In fact, DSIO's Examination Team performed a comprehensive review of FCMs and SDs concerning their cybersecurity activities with respect to their policies and procedures that address five separate categories of cybersecurity:

1. Identification of Cybersecurity Governance and Policies and Procedures;
2. Protection of Firm Networks and Information;
3. Risks Associated with Remote Customer or Counterparty Access and Funds Transfer Requests;
4. Risks Associated With Vendors and Other Third Parties; and

[2] System Safeguards Testing Requirements, 80 Fed. Reg. 80140, 80150 (Dec. 23, 2015); System Safeguards Testing Requirements for Derivatives Clearing Organizations, 80 Fed. Reg. 80114, 80118 (Dec. 3, 2015).

5. Detection of Unauthorized Activity.

Within these five categories, FCMs and SDs were asked to provide information relating to 53 specific cybersecurity practices. Firms participating in a consolidated risk management program with related entities were asked to specifically identify the policies and procedures that apply to the respective registrant.

All responses were reviewed to assess whether they adequately addressed the practices identified in the request. If the firm's initial response failed to address a practice, or if the response was unclear or inadequate, DSIO sent a follow-up request for additional information until an adequate response was received.

DSIO also identified specific areas of improvement that were applicable to a number of firms, namely Third Party Vendor Guidance and Training, and Risks Associated with Remote Customer or Counterparty Access and Funds Transfer Access.

This approach is virtually identical to the approach employed by the SEC, as noted in the National Exam Program Risk Alerts issued by the SEC on February 3, 2015, and September 15, 2015.

Finally, in addition to the cybersecurity practices described above, the Commission notes that DSIO reviewed and advanced for Commission approval the NFA Interpretation on Cybersecurity, which became effective March 1, 2016 and requires a cybersecurity program at each registrant. In addition, NFA held three cybersecurity workshops for registrants, which included cybersecurity experts. NFA also reviews the cybersecurity programs of registrants. The Commission continues to consider how best to leverage its resources – both through the CFTC's own programs and through further reliance on NFA's programs – to address the critical issue of cybersecurity among FCMs, SDs and other Commission registrants.

OIG Recommendation 5: *We recommend that CFTC develop an anonymous information-sharing program with registrants to stay current on cyber threats.*

CFTC Response: The Commission notes that extensive information-sharing arrangements are already in place. Registered entities already have a mechanism to share information with the Commission, and financial services entities including those registered with the CFTC are already anonymously sharing and receiving information security intelligence among themselves.

Commission system safeguards regulations for DCMs, SEFs, and SDRs require these registered entities to notify Commission staff promptly of all electronic trading halts and significant system malfunctions, and of all cyber security incidents or targeted threats that actually or potentially jeopardize automated system operation, reliability, security or capacity.[3]

[3] Similarly, the Commission's regulations require DCOs to notify Commission staff of any hardware or software malfunction, security incident, or targeted threat that materially impairs, or creates a significant likelihood of material impairment, of automated system operation, reliability, security, or capacity. 17 C.F.R. § 39.18(g)(1).

The Commission shares registrant cybersecurity incident and threat information with the intelligence community and federal law enforcement agencies through the Financial and Banking Information Infrastructure Committee ("FBIIC"), the inter-agency cybersecurity and critical infrastructure protection committee of financial sector regulators. Through FBIIC, the Commission also regularly receives Financial Sector Cyber Intelligence Group Circulars containing urgent cybersecurity intelligence and threat information and shares these circulars with DCMs, SEFs, SDRs, and DCOs located in the U.S. The Commission also arranges technical assistance and intelligence and information-sharing between these registered entities and the intelligence community and federal law enforcement agencies through the FBIIC Request for Technical Assistance ("RTA") process. In addition, DCMs, SEFs, SDRs, and DCOs engage in information-sharing through the Clearing House and Exchange Forum of the Financial Services Sector Coordinating Council, FBIIC's private sector counterpart and partner regarding critical infrastructure protection.

Finally, the Commission encourages[4] registered entities to participate in anonymized cybersecurity threat signature information-sharing through the Financial Sector Information Sharing and Analysis Center ("FS-ISAC"). FS-ISAC is a group of private sector organizations with over 10,000 members. FS-ISAC sends alerts to all of its members regarding threats, holds conference calls with members to discuss vulnerabilities like HeartBleed, and maintains a database of threats and vulnerabilities that its members can access to assist in their threat analysis.

Notwithstanding the CFTC's existing information-sharing mechanisms, the Commission appreciates the recommendation and will keep it in mind as it continues to review such information-sharing arrangements in the future.

If you have any questions, please contact Anthony C. Thompson, Executive Director, at (202) 418-5697 or AThompson@CFTC.gov.

Sincerely,

Timothy Massad

Although the audit report does not mention DCOs in this finding, this discussion applies equally to DCMs, SEFs, SDRs, and DCOs.

[4] For example, when DCR staff learn of a cyber event at a DCO, they ask the DCO if they have notified law enforcement and shared the incident with FS-ISAC. It is DCR's understanding that all U.S.-based DCOs are members of FS-ISAC. DMO makes similar inquiries when it is notified of a cybersecurity incident or targeted threat, and it encourages DCMs, SEFs, and SDRs to consider joining FS-ISAC in discussions during the interview phase of System Safeguards Examinations.

Appendix A – Audit Objective, Scope and Methodology

Objective

The objective of this performance audit was to review existing CFTC policies and procedures toward reducing cybersecurity risks to CFTC registrants. The objective spans several divisions. Specifically, we reviewed:

- DSIO monitoring of registrants' IT infrastructure;
- Procedures examined by DMO when it conducts System Safeguard Examinations at DCMs;
- DCR monitoring of IT systems at clearinghouses; and
- ODT IT systems for protecting sensitive information received from registrants.

Scope

The scope of the audit was to conduct an independent audit of CFTC's performance in reviewing information technology system safeguards in place at entities subject to CFTC regulatory oversight. The scope of this audit covered the period January 1, 2010 to April 1, 2015. However, we specifically intended to evaluate the organization's effort at reducing cybersecurity risk at registrants and to a lesser extent at the CFTC, since the agency's information systems are examined annually during the OIG's FISMA audit. During this performance audit, we relied on information provided by CFTC and other references as indicated throughout the report.

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.

Audit Strategy

The performance audit, at a minimum, included the following activities:

- Compiling CFTC's regulatory processes for evaluating information technology system safeguards in place during the audit period.
- Identifying any information technology review tasks outsourced to non-CFTC entities, such as the NFA.
- Evaluating the impact of the Dodd-Frank Act on CFTC responsibilities related to registrants' IT systems security.
- Examining relevant best practices suggested by independent entities, such as NIST, Futures Industry Association (FIA), Center for Internet Security (CIS), Financial Industry Regulatory Authority (FINRA), Presidential Directives, and other appropriate entities.
- Reviewing best practices for reducing cybersecurity risk in place at different categories of registrants.
- Evaluating CFTC staff reviews for completeness and contribution to improving registrants' cybersecurity posture.
- Identifying gaps, such as timeliness and scope, in CFTC's information technology system security reviews at CFTC-regulated entities.

We also considered:

- CFTC's staff evaluation of system security plans;
- Registrants' use of independent system certifications and periodic testing processes;
- Incident response policies and program;
- Privacy policies and controls, including system Privacy Impact Assessments; and
- Recently signed Executive Orders on cybersecurity[34] applicable to the financial services industry.

Audit Methodology

Our 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 compiling cybersecurity risks in order to provide guidance and respond to cybersecurity breaches, if any, at CFTC registrants;
4. Documenting CFTC's effectiveness in reducing cybersecurity risk among CFTC registrants and reporting best practices for reducing cybersecurity risk to its registrants;
5. Reporting audit results to CFTC OIG;
6. Issuing Notifications of Findings and Recommendations (NFRs);
7. Issuing a draft report;
8. Obtaining management comments on the draft report; and
9. Issuing a final report.

[34] For example Executive Order—Promoting Private Sector Cybersecurity Information Sharing dated February 13, 2015; available at https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-sharing.

Appendix B – CFTC Overview

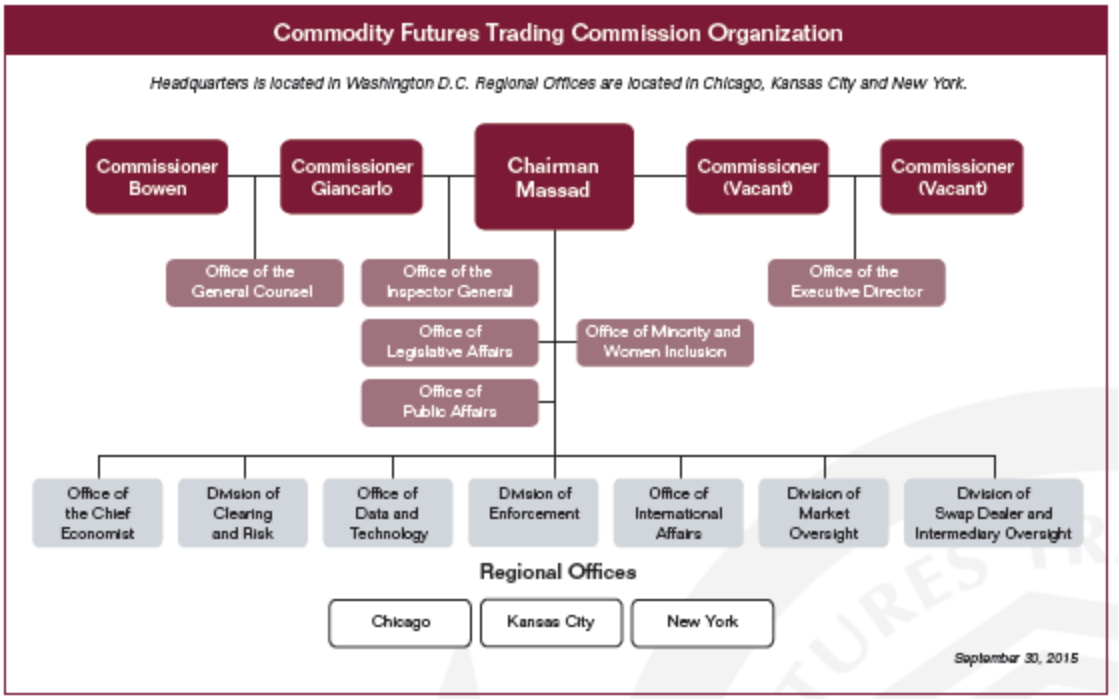

Figure 3. CFTC Organization as of September 30, 2015

The Commission consists of the following oversight divisions:

***Division of Clearing and Risk (DCR)* –** Oversees DCOs and other market participants in the clearing process, including futures commission merchants, swap dealers, major swap participants and large traders. It monitors the clearing of futures, options on futures, and swaps by DCOs; assesses DCO compliance with Commission regulations; and conducts risk assessment and surveillance. DCR also makes recommendations on DCO applications and eligibility, rule submissions, and which types of swaps should be cleared.

***Division of Market Oversight (DMO)* –** Fosters derivatives markets that accurately reflect the forces of supply and demand and are free of disruptive activity. It oversees trade execution facilities and data repositories, conducts surveillance, reviews new exchange applications and examines existing exchanges to ensure compliance with applicable core principles. DMO also evaluates new products to ensure they are not susceptible to manipulation as well as rules filings by exchanges to ensure compliance with core principles.

***Division of Swap Dealer and Intermediary Oversight (DSIO)* –** Oversees the registration and compliance of intermediaries and futures industry SROs, including U.S. derivatives exchanges and the NFA. Under Dodd-Frank, DSIO is also responsible for developing and monitoring compliance with regulations addressing registration, business conduct standards, capital adequacy, and margin requirements for swap dealers and major swap participants.

***Other Offices* –** There are nine other operating offices at the CFTC. They are: (1) Chief Economist (OCE); (2) Data and Technology (ODT); (3) Executive Director (OED); (4) General Counsel (OGC); (5) Whistleblower Office (WBO); (6) International Affairs (OIA); (7) Legislative Affairs (OLA); (8) Public Affairs (OPA); and (9) Inspector General (OIG), which is an independent unit. In this report, these units are categorized as other offices, and their cybersecurity concerns are addressed during the annual agency-wide FISMA review.

Number of Financial Entities Registered with CFTC

Table 3 below summarizes the number of financial entities registered with CFTC over the auditing period (2010 – 2015). CFTC has designated NFA as the registered futures association for FCMs, SDs, MSPs, RFEDs, IBs, CPOs and CTAs.

Table 3. Number of Registrants Under CFTC Jurisdiction From 2010 Through 2016

Type of Registrant	2010	2011	2012	2013	2014	2015/2016
Intermediaries registered as NFA Members [35]						
FCMs	142	137	128	105	78	71
SDs	0	0	0	82	104	104
MSPs	0	0	0	2	2	1
RFEDs	8	14	14	9	7	5
IBs	1,596	1,535	1,354	1,328	1,359	1,306
CPOs	1,228	1,183	1,172	1,811	1,774	1,719
CTAs	2,560	2,530	2,470	2,636	2,525	2,377
Designated as DCM with CFTC[36]						
DCMs	11	12	13	14	15	15
Organizations registered with CFTC						
SEFs	0	0	0	0	0	22
DCOs	10	11	11	13	13	15
Data Repositories registered with CFTC						
SDRs	0	0	3	3	4	4

Table 4 lists the current policies and initiatives taken by CFTC to address cybersecurity for its registrants.

[35] Numbers for registered intermediaries are from CFTC annual financial reports.

[36] http://sirt.cftc.gov/SIRT/SIRT.aspx?Topic=SwapExecutionFacilities Search Designated Contract Markets (DCM) using the following criteria: Status=Designated; Search Swap Execution Facilities (SEF) using the following criteria: Status= Registered, Search Derivatives Clearing Organizations (DCO) using the following criteria: Status=Registered; Search Swap Data Repository Organizations (SDR) using the following criteria: Status =Pending-Provisional Registration.

Table 4. CFTC Existing Policies and Procedures

CFTC Existing Policies and Procedures			
Date	**Division**	**Action**	**Description**
July 22, 2011	DSIO	17 CFR §160.30 Procedures to safeguard customer records and information[37]	Every futures commission merchant, retail foreign exchange dealer, commodity trading advisor, commodity pool operator, introducing broker, major swap participant, and swap dealer subject to the jurisdiction of the Commission must adopt policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information.
July 22, 2011	ALL	17 CFR § 37 162.21 Proper disposal of consumer information[38]	Any covered affiliate must adopt reasonable, written policies and procedures that address administrative, technical, and physical safeguards for the protection of consumer information. These written policies and procedures must be reasonably designed.
December 31, 2012	DSIO	CFTC Announces Real-Time Public Reporting of Swap Transactions and Swap Dealer Registration Began December 31, 2012[39]	Real-time public reporting of swap transactions and swap dealer registration, pursuant to reforms enacted by Congress, began on December 31, 2012.
April 3, 2013	DSIO	17 CFR § 23.600 Risk Management Program for swap dealers and major swap participants[40]	Each swap dealer and major swap participant shall establish, document, maintain, and enforce a system of risk management policies and procedures designed to monitor and manage the risks associated with the swaps activities of the swap dealer or major swap participant.

[37] Electronic Code of Federal Regulations, http://www.ecfr.gov/cgi-bin/text-idx?SID=77e7da58000a26da0c91ee7f6ae1fd83&mc=true&node=pt17.2.160&rgn=div5#se17.2.160_130.
[38] Electronic Code of Federal Regulations, http://www.ecfr.gov/cgi-bin/text-idx?SID=77e7da58000a26da0c91ee7f6ae1fd83&mc=true&node=pt17.2.162&rgn=div5#se17.2.162_121.
[39] CFTC open meeting to propose final rules for swap dealer registration under the Dodd-Frank Act: registration standards, duties and core Principles, http://www.cftc.gov/PressRoom/PressReleases/pr6085-11.
[40] Electronic Code of Federal Regulations, http://www.ecfr.gov/cgi-bin/text-idx?SID=77e7da58000a26da0c91ee7f6ae1fd83&mc=true&node=pt17.1.23&rgn=div5#se17.1.23_1600.

CFTC Existing Policies and Procedures			
Date	**Division**	**Action**	**Description**
April 19, 2013	ALL	17 CFR § 162.30 Duties regarding the detection, prevention, and mitigation of identity theft.[41]	Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.
June 4, 2013	DMO	17 CFR Part 37 Core Principles and Other Requirements for Swap Execution Facilities[42]	The final rules, guidance, and acceptable practices, which apply to the registration and operation of a new type of regulated entity named a swap execution facility, implement the Dodd-Frank Act's new statutory framework.
November 14, 2013	DSIO	17 CFR § 1.11 Risk Management Program for Futures Commission Merchants	Regulations to enhanced customer protections, risk management programs, internal monitoring and controls, capital and liquidity standards, customer disclosures, and auditing and examination programs for futures commission merchants.
March 18, 2015	DMO & DCR	Roundtable on Cybersecurity and System Safeguards Testing[43]	To review system safeguards testing requirements, including potential enhancements to further strengthen the resilience of futures exchanges, clearing organizations, and swap data repositories. The CFTC is also considering how best to leverage enhanced system safeguards testing requirements, including independent testing, to satisfy regulatory requirements for these entities.
August 28, 2015	DSIO/NFA	NFA Information Systems Security Programs Proposed Adoption of the Interpretive Notice to NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs (Effective March 1, 2016)[44]	Members should have supervisory practices in place reasonably designed to diligently supervise the risks of unauthorized access to or attack of their information technology systems, and to respond appropriately should unauthorized access or attack occur.

[41] Identify Theft Program, http://www.ecfr.gov/cgi-bin/text-idx?SID=4de5d617a7c3bd8d789c0dd14a77172f&mc=true&node=pt17.2.162&rgn=div5#se17.2.162_130.
[42] http://www.cftc.gov/idc/groups/public/@lrfederalregister/documents/file/2013-12242a.pdf.
[43] SEC Cybersecurity Roundtable, https://www.sec.gov/spotlight/cybersecurity-roundtable.shtml.
[44] https://www.nfa.futures.org/nfamanual/NFAManual.aspx?RuleID=9070&Section=9.

CFTC Existing Policies and Procedures			
Date	**Division**	**Action**	**Description**
December 23, 2015	DCR	17 CFR Part 39, System Safeguards Testing Requirements for Derivatives Clearing Organizations; Proposed Rule, December 23, 2015[45]	To enhance and clarify existing provisions relating to system safeguards risk analysis and oversight and cybersecurity testing, and adding new provisions concerning certain aspects of cybersecurity testing for derivatives clearing organizations.
December 23, 2015	DMO	17 CFR Part 37, 38 and 49 System Safeguards Testing Requirements; Proposed Rules, December 23, 2015[46]	To enhance and clarify existing provisions relating to system safeguards risk analysis and oversight and cybersecurity testing, and adding new provisions concerning certain aspects of cybersecurity testing for designated contract markets, swap execution facilities, derivatives clearing organizations, swap data repositories.

[45] "See footnote[9]".
[46] "See footnote[9]".

Appendix C – Financial Industry Best Practices

Financial Industry Best Practices for Cybersecurity Oversight

The regulations, policies, reports, and guidance that aided us in identifying best practices to reduce cybersecurity risks are listed in **Table 5** below.

Table 5. Financial Industry Best Practice Related to Cybersecurity Oversight

Organization	Best Practices
Presidential Executive Order	Presidential Executive Order 1336, Improving Critical Infrastructure Cybersecurity, February 2013[47]
NIST	NIST's Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February 2014[48]
SEC	Securities and Exchange Commission (SEC) Office of Compliance Inspections and Examinations (OCIE), National Exam Program Risk Alert, OCIE Cybersecurity Initiative, Volume IV, Issue 2, April 15, 2014[49] 17 CFR Parts 240, 242, and 249 Regulation Systems Compliance and Integrity (Regulation SCI), issued December 2014[50] 17 CFR Part 248.30 Procedures to Safeguard Customer Records and Information; Disposal of Consumer Report Information[51] 17 CFR Parts 232, 240, and 249 Security-Based Swap Data Repository Registration, Duties, and Core Principles; Final rule; Effective Date May 18, 2015[52]
FINRA	Financial Industry Regulatory Authority Report on Cybersecurity Practices (February 2015)[53]
CPMI	Guidance of Cyber Resilience for Financial Market Infrastructures[54]
Federal Financial Institutions Examination Council (FFIEC)	Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook (IT Handbook)[55]
PCI Security Standards Council	Payment Card Industry Security Standards [56]
Council on CyberSecurity	The Critical Security Controls for Effective Cyber Defense[57]

[47] Presidential Executive Order 1336 https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.
[48] NIST Framework for Improving Critical Infrastructure Cybersecurity http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.
[49] OCIE Cybersecurity Initiative https://www.eci.com/pdf/SEC-Cybersecurity-Sample-Questions.pdf.
[50] 17 CFR Parts 240, 242, and 249 Regulation Systems Compliance and Integrity https://www.sec.gov/rules/final/2014/34-73639.pdf.
[51] 17 CFR Part 248.30 Procedures to Safeguard Customer Records and Information https://www.sec.gov/spotlight/regulation-s-p.htm.
[52] 17 CFR Parts 232, 240, and 249 Security-Based Swap Data Repository Registration, Duties, and Core Principles https://www.sec.gov/rules/final/2015/34-74246.pdf.
[53] FINRA Report on Cybersecurity Practices http://www.finra.org/file/report-cybersecurity-practices.
[54] CMPI Guidance of Cyber Resilience for Financial Market Infrastructures 2016 https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf.
[55] FFIEC IT Examination Handbook booklets http://ithandbook.ffiec.gov/it-booklets.aspx.
[56] PCI Standards https://www.pcisecuritystandards.org/document_library.
[57] Council on CyberSecurity, https://www.cisecurity.org/critical-controls.cfm.

CFTC and SEC Oversight Over Respective Registrants

On a Federal level, financial markets get general regulatory oversight from two government bodies: CFTC and the Securities and Exchange Commission (SEC). Both have similar goals and are under the jurisdiction of the U.S. Department of the Treasury.

The SEC has regulatory and supervisory responsibility over securities companies, including securities brokers, securities dealers, clearing agencies, transfer agents, certain investment advisers, and investment companies. **Table 6** presents a list of comparable entities among CFTC, SEC and other federal regulators.

Table 6. CFTC Registrants and Equivalent Entities In The Financial Market

Crosswalk of CFTC Registrants to SEC and other Federal Regulators		
CFTC	**SEC**	**Other Federal Regulators**
FCMs[58]	Broker-Dealers[59] [60]	Designated Primary Dealers[61]
SDs	Broker-Dealers	Designated Primary Dealers
MSPs	Broker-Dealers	Designated Primary Dealers
RFEDs	Broker-Dealers	
IBs	Securities Brokers	
CPOs	Mutual Funds and Hedge Funds	
CTAs	Fund Managers and Investment Managers	
DCMs[62]	Exchanges	
SEFs[63]	Security-Based Swap Execution Facilities (SB SEFs)	
DCOs[64]	Clearing Corporations	
SDRs[65]	Security-Based Swap Data Repository (SB SDR)	

Table 7 lists the policies and initiatives taken by SEC to address cybersecurity for its registrants.

Table 7. SEC Existing Policies and Procedures

SEC Existing Policies and Procedures		
Date	**Action**	**Description**
May 20, 2013	Regulation S-ID ◦Subpart C - Regulation S-ID: Identity Theft Red Flags,[66] 17 CFR Part 162 Identity Theft Red Flags Rules	SEC and CFTC Jointly issuing final rules and guidelines to require certain regulated entities to establish programs to address risks of identity theft.
January 9, 2014	Examination Priorities for 2014[67]	Published examination priorities SEC perceives to have heightened risk.

[58] CFTC Intermediaries (FCMs, SDs, MSPs, RFEDs, IBs, CPOs and CTAs), http://www.cftc.gov/IndustryOversight/Intermediaries/index.htm.
[59] A broker is any person engaged in the business of effecting transactions in securities for the account of others, https://www.sec.gov/divisions/marketreg/bdguide.htm.
[60] A dealer any person engaged in the business of buying and selling securities for his own account, through a broker or otherwise.
[61] Designated Primary Dealers are banks and securities broker dealers that trade in U.S. Government securities with the Federal Reserve Bank of New York, https://www.treasury.gov/resource-center/data-chart-center/quarterly-refunding/Pages/primary-dealers.aspx.
[62] CFTC Designated contract markets, http://www.cftc.gov/IndustryOversight/TradingOrganizations/DCMs/index.htm.
[63] CFTC Swaps Execution Facilities, http://www.cftc.gov/IndustryOversight/TradingOrganizations/SEF2/index.htm.
[64] CFTC Derivatives clearing organizations, http://www.cftc.gov/IndustryOversight/ClearingOrganizations/index.htm.
[65] CFTC Swap data repositories, http://www.cftc.gov/IndustryOversight/DataRepositories/index.htm.
[66] Joint regulation for Identity Theft Red Flags, https://www.sec.gov/rules/final/2013/34-69359.pdf.
[67] SEC Examination Priorities for 2014, https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2014.pdf.

SEC Existing Policies and Procedures		
Date	**Action**	**Description**
March 26, 2014	Cybersecurity Roundtable[68]	To discuss cybersecurity and the issues and challenges it raises for market participants and public companies, and how they are addressing those concerns.
April 15, 2014	Risk Alert - OCIE's examinations of registered broker-dealers and investment advisers [69]	To conduct examinations of more than 50 registered broker-dealers and registered investment advisers, focusing on areas related to cybersecurity.
November 19, 2014	17 CFR Part 242 Regulation SCI—Systems Compliance and Integrity; Final Rule, November 19, 2014[70]	Require Systems Compliance and Integrity (SCI) entities to establish written policies and procedures reasonably designed to ensure that their systems have levels of capacity, integrity, resiliency, availability, and security adequate to maintain their operational capability and promote the maintenance of fair and orderly markets, and that they operate in a manner that complies with the Exchange Act.
February 3, 2015	Cybersecurity Examination Sweep Summary[71]	Examination results of 57 registered broker-dealers and 49 registered investment advisers.
February 11, 2015	SEC Regulation SDR[72]	SEC adopted 21 new rules that would increase transparency and provide enhanced reporting requirements in the security-based swap market. The rules require SDRs to register with the Commission and establishes a framework for the reporting and public dissemination of security-based swap transactions.
May 18, 2015	17 CFR Parts 232, 240, and 249 Security-Based Swap Data Repository Registration, Duties, and Core Principles; Final rule; Effective Date May 18, 2015[73]	New rules governing the security-based swap data repository registration process, duties, and core principles.
March 19, 2015	SEC Regulation S_P: 17 CFR Part 240.13n-6 Automated systems[74]	Every security-based swap data repository, with respect to those systems that support or are integrally related to the performance of its activities, shall establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its systems provide adequate levels of capacity, integrity, resiliency, availability, and security.
September 15, 2015	Risk Alert - OCIE's 2015 Cybersecurity Examination Initiative[75]	To assess implementation of firm procedures and controls.

[68] "See footnote[43]".
[69] SEC 2014 OCIE Cybersecurity Initiative http://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf.
[70] "See footnote[50]".
[71] SEC Cybersecurity Examination Sweep Summary, https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.
[72] Regulation SDR ◦Exchange Act Rule 13n-6, http://www.ecfr.gov/cgi-bin/text-idx?SID=e77a0b38297f6bb207cbc8cf0fe1e199&mc=true&node=se17.4.240_113n_66&rgn=div8.
[73] "See footnote[52]."
[74] Regulation SDR ◦Exchange Act Rule 13n-6, http://www.ecfr.gov/cgi-bin/text-idx?SID=e77a0b38297f6bb207cbc8cf0fe1e199&mc=true&node=se17.4.240_113n_66&rgn=div8.
[75] SEC Risk Alert - OCIE's 2015 Cybersecurity Examination Initiative, http://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.

SEC Existing Policies and Procedures		
Date	**Action**	**Description**
November 15, 2010	Market Access Rule ◦Exchange Act Rule 15c3-5; Risk Management Controls for Brokers or Dealers with Market Access[76]	Require brokers or dealers with access to trading securities directly on an exchange or alternative trading system (ATS), including those providing sponsored or direct market access to customers or other persons, and broker-dealer operators of an ATS that provide access to trading securities directly on their ATS to a person other than a broker or dealer, to establish, document, and maintain a system of risk management controls and supervisory procedures.
September 15, 2015	2015 Examination Priorities[77]	Provide areas of focus for OCIE's second round of cybersecurity examinations.

[76] https://www.sec.gov/rules/final/2010/34-63241.pdf.
[77] Footnote OCIE's 2015 Cybersecurity Examination Initiative, https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.

Appendix D – Illustration of Findings 2 and 3

Note: The blue shaded boxes indicate CFTC meets Best Practice Standards. Green boxes indicate a difference between CFTC and Best Practice Standards testing requirements. Orange box in the first column identifies similar testing requirements, but requirements below best practice standards. Orange box in the second column identifies similar testing requirements, but requirements below CFTC standards.

External Penetration Testing Frequency Requirements for DCOs

- **CFTC – DCOs**
  - At a minimum, covered DCOs would be required to conduct the external penetration testing at a frequency determined by an appropriate risk analysis, no less frequently than annually.
- **Best Practice**
  - NIST – Calls for at least annual penetration testing of an organization's network and systems.
  - SEC's Regulation SCI – Conduct SCI reviews that include penetration testing at least every three years or more frequently based on risk.
  - FFIEC – Calls for independent penetration testing of high risk systems at least annually, and for quarterly testing and verification of the efficacy of firewall and access control defenses.
  - PCI – Perform both external and internal penetration testing "at least annually," as well as after any significant network changes.

Internal Penetration Testing Frequency Requirements for DCOs

- **CFTC – DCOs**
  - At a minimum, covered DCOs would be required to conduct the internal penetration testing at a frequency determined by an appropriate risk analysis, no less frequently than annually.
- **Best Practice**
  - NIST – Calls for at least annual penetration testing of an organization's network and systems
  - SEC's Regulation SCI – Conduct SCI reviews that include penetration testing at least every three years or more frequently based on risk.
  - FFIEC – Calls for independent penetration testing of high risk systems at least annually, and for quarterly testing and verification of the efficacy of firewall and access control defenses.
  - PCI – Perform both external and internal penetration testing "at least annually," as well as after any significant network changes.

Vulnerability Testing Frequency Requirements for DCOs

- **CFTC – DCOs**
  - At a minimum, covered DCOs would be required to conduct the vulnerability testing at a frequency determined by an appropriate risk analysis, but no less frequently than quarterly.
- **Best Practice**
  - NIST – Scan for automatic system vulnerabilities on a regular and ongoing basis and when new vulnerabilities potentially affecting systems are identified.
  - SEC Regulation SCI requires regular reviews and testing of such systems, including backup systems, to identify vulnerabilities pertaining to internal and external threats, physical hazards, and natural or manmade disasters.
  - The Council on CyberSecurity - Calls for entities to "continuously acquire, assess, and take action on new information in order to identify vulnerabilities."
  - FFIEC – states that the frequency of testing should be determined by the institution's risk assessment.
  - PCI – Requires internal and external network vulnerability scans "at least quarterly" as well as after any significant network changes.

External Penetration Testing for All DCMs, SEFs, and SDRs

- **CFTC – DCMs, SEFs, and SDRs**
  - Conduct external penetration testing at a frequency determined by an appropriate risk analysis.
- **Best Practice**
  - NIST – Calls for at least annual penetration testing of an organization's network and systems.
  - SEC's Regulation SCI – Conduct SCI reviews that include penetration testing at least every three years or more frequently based on risk.
  - FFIEC – Calls for independent penetration testing of high risk systems at least annually, and for quarterly testing and verification of the efficacy of firewall and access control defenses.
  - PCI – Perform both external and internal penetration testing "at least annually," as well as after any significant network changes.

Internal Penetration Testing for All DCMs, SEFs, and SDRs

- **CFTC – DCMs, SEFs, and SDRs**
  - Conduct internal penetration testing at a frequency determined by an appropriate risk analysis.
- **Best Practice**
  - NIST – Calls for at least annual penetration testing of an organization's network and systems.
  - SEC's Regulation SCI – Conduct SCI reviews that include penetration testing at least every three years or more frequently based on risk.
  - FFIEC – Calls for independent penetration testing of high risk systems at least annually, and for quarterly testing and verification of the efficacy of firewall and access control defenses.
  - PCI – Perform both external and internal penetration testing "at least annually," as well as after any significant network changes.

Minimum Vulnerability Testing Frequency Requirements for Covered DCMs and SDRs

- **CFTC – Covered DCMs and SDRs**
  - Vulnerability testing no less frequently than quarterly.
- **Best Practices**
  - NIST – Scan for automatic system vulnerabilities on a regular and ongoing basis and when new vulnerabilities potentially affecting systems are identified.
  - SEC Regulation SCI requires regular reviews and testing of such systems, including backup systems, to identify vulnerabilities pertaining to internal and external threats, physical hazards, and natural or manmade disasters.
  - The Council on CyberSecurity - Calls for entities to "continuously acquire, assess, and take action on new information in order to identify vulnerabilities."
  - FFIEC – states that the frequency of testing should be determined by the institution's risk assessment.
  - PCI – Requires internal and external network vulnerability scans "at least quarterly" as well as after any significant network changes.

Minimum Internal Penetration Testing Frequency Requirements for Covered DCMs and SDRs

- **CFTC – Covered DCMs and SDRs**
  - At a minimum, covered DCMs and SDRs would be required to conduct the internal penetration testing no less frequently than annually.
- **Best Practice**
  - NIST – Calls for at least annual penetration testing of an organization's network and systems.
  - SEC's Regulation SCI – Conduct SCI reviews that include penetration testing at least every three years or more frequently based on risk.
  - FFIEC – Calls for independent penetration testing of high risk systems at least annually, and for quarterly testing and verification of the efficacy of firewall and access control defenses.
  - PCI – Perform both external and internal penetration testing "at least annually," as well as after any significant network changes.

Vulnerability Testing Requirement for All DCMs, SEFs, and SDRs

- **CFTC – DCMs, SEFs, and SDRs**
  - At a frequency determined by an appropriate risk analysis.
- **Best Practice**
  - NIST – Scan for automatic system vulnerabilities on a regular and ongoing basis and when new vulnerabilities potentially affecting systems are identified.
  - SEC Regulation SCI requires regular reviews and testing of such systems, including backup systems, to identify vulnerabilities pertaining to internal and external threats, physical hazards, and natural or manmade disasters.
  - The Council on CyberSecurity - Calls for entities to "continuously acquire, assess, and take action on new information in order to identify vulnerabilities."
  - FFIEC – states that the frequency of testing should be determined by the institution's risk assessment.
  - PCI – Requires internal and external network vulnerability scans "at least quarterly" as well as after any significant network changes.

Minimum External Penetration Testing Frequency Requirements for Covered DCMs and SDRs

- **CFTC – Covered DCMs and SDRS**
  - At a minimum, covered DCMs and SDRs would be required to conduct the external penetration testing no less frequently than annually.
- **Best Practice**
  - NIST – Calls for at least annual penetration testing of an organization's network and systems.
  - SEC's Regulation SCI – Conduct SCI reviews that include penetration testing at least every three years or more frequently based on risk.
  - FFIEC – Calls for independent penetration testing of high risk systems at least annually, and for quarterly testing and verification of the efficacy of firewall and access control defenses.
  - PCI – Perform both external and internal penetration testing "at least annually," as well as after any significant network changes.

Appendix E – Glossary

Term	Definition
Broker	A person paid a fee or commission for executing buy or sell orders for a customer. In commodity futures trading, the term may refer to: (1) Floor broker, a person who actually executes orders on the trading floor of an exchange; (2) Account executive or associated person, the person who deals with customers in the offices of futures commission merchants; or (3) the futures commission merchant.
Clearing Member	A member of an exchange clearinghouse. All trades of a non-clearing member must be registered and eventually settled through a clearing member.
Clearing Organization	An agency or separate corporation of a futures exchange that is responsible for settling trading accounts, collecting and maintaining margin monies, regulating delivery and reporting trade data.
Commodity	An article of commerce or a product that can be used for commerce. In a narrow sense, products traded on authorized commodity exchanges. The types of commodities include agricultural products, metals, petroleum, foreign currencies and financial instruments and indexes to name a few.
Commodity Exchange Act (CEA)	The 1936 Commodity Exchange Act as amended, 7 USC 1, et seq., provides for the federal regulation of commodity futures and options trading.
Commodity Futures Trading Commission (CFTC)	The Federal regulatory agency established by the Commodity Futures Trading Act of 1974 to administer the Commodity Exchange Act.
Commodity Pool Operator (CPO)	A person engaged in a business similar to an investment trust or a syndicate and who solicits or accepts funds, securities, or property for the purpose of trading commodity futures contracts or commodity options. The commodity pool operator either itself makes trading decisions on behalf of the pool or engages a commodity trading advisor to do so.
Commodity Trading Advisor (CTA)	An individual or organization that, for compensation or profit, directly or indirectly advises others as to the value of or the advisability of buying or selling futures or options contracts. Providing advice indirectly includes exercising trading authority over a customer's account. Registration with the Commodity Futures Trading Commission is generally required.
Core Principle	A provision of the Commodity Exchange Act with which a contract market, derivatives transaction execution facility, or derivatives clearing organization must comply on an ongoing basis. There are 18 core principles for contract markets, 9 core principles for derivatives transaction execution facilities, and 14 core principles for derivatives clearing organizations.

Term	Definition
Derivatives Clearing Organization (DCO)	A clearing organization registered with the CFTC that, in respect to a contract (1) enables each party to the contract to substitute, through novation or otherwise, the credit of the derivatives clearing organization for the credit of the parties; (2) arranges or provides, on a multilateral basis, for the settlement or netting of obligations resulting from such contracts; or (3) otherwise provides clearing services or arrangements that mutualize or transfer among participants in the derivatives clearing organization the credit risk arising from such contracts.
Designated Contract Market (DCM)	A board of trade or exchange designated by the CFTC to trade futures, swaps, and/or options under the CEA. A contract market can allow both institutional and retail participants and can list for trading contracts on any commodity, provided that each contract is not readily susceptible to manipulation.
Designated Self-Regulatory Organization (DSRO)	Self-regulatory organizations (i.e., the commodity exchanges and registered futures associations) must enforce minimum financial and reporting requirements for their members, among other responsibilities outlined in the CFTC's regulations. When a futures commission merchant (FCM) is a member of more than one SRO, the SROs may decide among themselves which of them will assume primary responsibility for these regulatory duties and, upon approval of the plan by the Commission, be appointed the "designated self-regulatory organization" for that FCM.
Futures Commission Merchant (FCM)	Individuals, associations, partnerships, corporations, and trusts that solicit or accept orders for the purchase or sale of any commodity for future delivery on or subject to the rules of any exchange and that accept payment from or extend credit to those whose orders are accepted.
Hedge Fund	A private investment fund or pool that trades and invests in various assets such as securities, commodities, currency, and derivatives on behalf of its clients, typically wealthy individuals. Some commodity pool operators operate hedge funds.
Interdealer Broker	A broker that facilitates bilateral trades between large market participants.
Introducing Broker (IB)	A firm or individual that solicits and accepts futures orders from customers but does not accept money, securities or property from the customer. An IB must be registered with the Commodity Futures Trading Commission and must carry all of its accounts through a futures commission merchant on a fully disclosed basis.

Term	Definition
Major Swap Participant (MSP)	A person that maintains a 'substantial position' in any of the major swap categories, excluding positions held for hedging or mitigating commercial risk and positions maintained by certain employee benefit plans for hedging or mitigating risks in the operation of the plan; (2) A person whose outstanding swaps create 'substantial counterparty exposure that could have serious adverse effects on the financial stability of the United States banking system or financial markets'; (3) Any 'financial entity' that is 'highly leveraged relative to the amount of capital such entity holds and that is not subject to capital requirements established by an appropriate Federal banking agency' and that maintains a 'substantial position' in any of the major swap categories.
National Futures Association (NFA)	Authorized by Congress in 1974 and designated by the CFTC in 1982 as a "registered futures association," NFA is the industrywide self-regulatory organization of the futures industry.
Registrant	A person or firm who had properly applied for and received approval to operate in one or more of the following capacities: futures commission merchant, introducing broker, commodity trading advisor, commodity pool operator, leverage transaction merchant, agricultural trade option merchant, floor broker, floor trader, or associate person.
Securities and Exchange Commission (SEC)	The Federal regulatory agency established in 1934 to administer Federal securities laws.
Security-Based Swap Dealer (SB SD)	A swap dealer that deals in security based swaps under SEC regulation.
Security-Based Swap Execution Facility (SB SEF)	A swap execution facility regulated by the SEC where security-based swaps are executed.
Self-Regulatory Organization (SRO)	Self-regulatory organizations enforce minimum financial and sales practice requirements for their members.
Swap	In general, the exchange of one asset or liability for a similar asset or liability for the purpose of lengthening or shortening maturities, or raising or lowering coupon rates, to maximize revenue or minimize financing costs.
Swap Data Repository (SDR)	Swap data repositories (SDRs) are registered entities created by the Dodd-Frank Act that collect and maintain information or records with respect to transactions or positions in, or the terms and conditions of, swaps entered into by third parties for the purpose of providing a centralized recordkeeping facility for swaps.
Swap Dealer (SD)	An entity such as a bank or investment bank that markets swaps to end users. Swap dealers often hedge their swap positions in futures markets.
Swap Execution Facility (SEF)	A trading system or platform created by the Dodd-Frank Act in which multiple participants have the ability to execute or trade swaps by accepting bids and offers made by multiple participants in the facility or system, through any means of interstate commerce.
Systems Compliance and Integrity (SCI)	SCI entities include self-regulatory organizations (SROs), including stock and options exchanges, registered clearing agencies, FINRA and the MSRB, alternative trading systems (ATSs), that trade NMS and non-NMS stocks exceeding specified volume thresholds, disseminators of consolidated market data (plan processors), and certain exempt clearing agencies.

Appendix F –Acronyms

Acronym	Definition
CEA	Commodity Exchange Act
CFR	Code of Federal Regulations
CFTC	U.S. Commodity Futures Trading Commission
COR	Contract Officer Representative
CPMI	Committee on Payments and Market Infrastructures
CPO	Commodity Pool Operator
CSC	Critical Security Control
CTA	Commodity Trading Advisor
DCM	Designated Contract Market
DCO	Derivatives Clearing Organization
DCR	Division of Clearing and Risk
DMO	Division of Market Oversight
Dodd-Frank Act	Dodd-Frank Wall Street Reform and Consumer Protection Act
DOE	Division of Enforcement
DSIO	Division of Swap Dealer and Intermediary Oversight
DSRO	Designated Self-Regulatory Organization
DTCC	Depository Trust & Clearing Corporation
FCM	Futures Commission Merchant
FFIEC	Federal Financial Institutions Examination Council
FIA	Futures Industry Association
FINRA	Financial Industry Regulatory Authority
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FTP	File Transfer Protocol
GAGAS	Generally Accepted Government Auditing Standards
IB	Introducing Broker
IOSCO	International Organization of Securities Commissions
IT	Information Technology
MP	Market Participant
MSP	Major Swap Participant
MSRB	Municipal Securities Rulemaking Board
NEP	National Examination Program
NFA	National Futures Association
NFR	Notification of Findings and Recommendations
NIST	National Institute of Standards and Technology
NMS	National Market System
OCE	Office of Chief Economist
OCIE	Office of Compliance Inspections and Examinations
ODT	Office of Data and Technology
OED	Office of Executive Director
OGC	Office of General Counsel
OIA	Office of International Affairs
OIG	Office of Inspector General
OLA	Office of Legislative Affairs
OPA	Office of Public Affairs

Acronym	Definition
PCI	Payment Card Industry Security Standards
PPD-21	Presidential Policy Directive-21
RFED	Retail Foreign Exchange Dealers
SB SDR	Security-Based Swap Data Repository
SCI	Systems Compliance and Integrity
SD	Swap Dealer
SDR	Swap Data Repository
SEC	U.S. Securities and Exchange Commission
SEF	Swap Execution Facilities
SFTP	Secured File Transfer Protocol
SRO	Self-Regulatory Organization
WBO	Whistleblower Office
WFE	World Federation of Exchanges