U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

Audit of the SEC's Process for Reviewing Self-Regulatory Organizations' Proposed Rule Changes

September 23, 2016
Report No. 537

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

September 23, 2016

TO: Jessica Kane, Director, Office of Municipal Securities
Stephen Luparello, Director. Division of Trading and Markets
Jeffery Heslop, Chief Operating Officer

FROM: Carl W. Hoecker, Inspector General

SUBJECT: *Audit of the SEC's Process for Reviewing Self-Regulatory Organizations' Proposed Rule Changes*, Report No. 537

Attached is the Office of Inspector General (OIG) final report detailing the results of our audit of the U.S. Securities and Exchange Commission's (SEC or agency) process for reviewing proposed rule changes submitted by self-regulatory organizations. The report contains seven recommendations that should help improve the SEC's process for compliance with agency policies and procedures and information technology controls for the Electronic Form Filing System/SRO Tracking System.

On September 13, 2016, we provided management with a draft of our report for review and comment. In its September 22, 2016, response, management concurred with our recommendations. We have included the response as Appendix II in the final report.

Within the next 45 days, please provide the OIG with a written corrective action plan that addresses the recommendations. The corrective action plan should include information such as the responsible official/point of contact, timeframe for completing required actions, and milestones identifying how the Division of Trading and Markets, the Office of Municipal Securities, and the Office of Information Technology will address the recommendations.

We appreciate the courtesies and cooperation extended to us during the audit. If you have questions, please contact me or Rebecca L. Sharek, Deputy Inspector General for Audits, Evaluations, and Special Projects.

Attachment

cc: Mary Jo White, Chair
Andrew Donohue, Chief of Staff, Office of the Chair
Michael Liftik, Deputy Chief of Staff, Office of the Chair
Nathaniel Stankard, Deputy Chief of Staff, Office of the Chair
Michael S. Piwowar, Commissioner
Jaime Klima, Counsel, Office of Commissioner Piwowar
Kara M. Stein, Commissioner

Robert Peak, Advisor to the Commissioner, Office of Commissioner Stein
Anne K. Small, General Counsel
Keith Cassidy, Director, Office of Legislative and Intergovernmental Affairs
Rick Fleming, Investor Advocate
John J. Nester, Director, Office of Public Affairs
Rebecca Olsen, Deputy Director, Office of Municipal Securities
Gary Goldsholle, Deputy Director, Division of Trading and Markets
Pamela C. Dyson, Director/Chief Information Officer, Office of Information Technology
Darlene L. Pryor, Management and Program Analyst, Office of the Chief Operating Officer

Executive Summary Audit of the SEC's Process for Reviewing Self-Regulatory Organizations' Proposed Rule Changes

Report No. 537
September 23, 2016

Why We Did This Audit

Privately funded nongovernmental entities, referred to as self-regulatory organizations (SROs), conduct much of the day-to-day oversight of the U.S. securities markets and broker-dealers under their jurisdiction. SROs, including national securities exchanges, registered securities associations, and registered clearing agencies, establish rules that govern member activities. The U.S. Securities and Exchange Commission (SEC or agency) reviews SROs' proposals for new rules and changes to existing rules (referred to as proposed rule changes) to ensure compliance with applicable SEC rules and regulations and the Securities Exchange Act of 1934 (Exchange Act), as amended by the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act). The SEC must review and process SROs' proposed rule changes according to certain requirements and within specified timeframes. Proper review of SROs' proposed rule changes helps the agency achieve its mission to protect investors, maintain fair, orderly and efficient markets, and facilitate capital formation.

What We Recommended

We made seven recommendations for corrective action. Our recommendations address the need to better document TM's and OMS' basis for rejecting SROs' proposed rule changes, and needed improvements in SRTS/EFFS information security controls and contingency planning documents. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action.

What We Found

The SEC's Division of Trading and Markets (TM) and its Office of Municipal Securities (OMS) are responsible for reviewing SROs' proposed rule changes. TM and OMS receive and track proposed rule changes using the SRO Rule Tracking System/Electronic Form Filing System (SRTS/EFFS). We determined that TM and OMS policies and procedures were consistent with statutory requirements for reviewing and processing proposed rule changes. In addition, SROs we surveyed were generally satisfied with EFFS and reported that TM and OMS staff (1) applied processes for reviewing and processing proposed rule changes consistently, and (2) effectively communicated with SROs and other stakeholders when the agency initiated proceedings to determine whether to disapprove an SRO's proposed rule change. We also reviewed TM's and OMS' processing of 345 of the 3,494 proposed rule changes received by the SEC in fiscal years 2014 and 2015 and found that TM and OMS staff complied with statutory requirements and generally complied with agency policies and procedures. However, TM and OMS staff did not consistently document in SRTS the basis for rejecting proposed rule changes, as required by agency policy. As a result, we determined that the SEC, in some cases, may not have a complete historical record for proposed rule changes received in FYs 2014 and 2015.

We also found that SRTS/EFFS information security controls need improvement. (b)(7)(E)

(b)(7)(E)

Lastly, we found that contingency planning controls for SRTS/EFFS were inadequate. Specifically, (1) OIT did not update the system's Business Impact Analysis to reflect major system changes, (2) contingency planning documents were inconsistent, and (3) OIT

(b)(7)(E)

For additional information, contact the Office of Inspector General at (202) 551-6061 or http://www.sec.gov/oig.

TABLE OF CONTENTS

ABBREVIATIONS

BIA	Business Impact Analysis
Dodd-Frank Act	Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010
EDRP	Enterprise Disaster Recovery Plan
EFFS	Electronic Form Filing System
Exchange Act	Securities Exchange Act of 1934
FINRA	Financial Industry Regulatory Authority
FY	fiscal year
GAO	U.S. Government Accountability Office
ISCP	Information System Contingency Plan
ISO	Information System Owner
MSRB	Municipal Securities Rulemaking Board
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information Technology
OMS	Office of Municipal Securities
POA&M	plan of action and milestones
RTO	recovery time objective
SEC or agency	U.S. Securities and Exchange Commission
SRO	self-regulatory organization
SRTS	SRO Rule Tracking System
TM	Division of Trading and Markets

Background and Objectives

Background

Privately funded nongovernmental membership entities, referred to as self-regulatory organizations (SROs), conduct much of the day-to-day oversight for the U.S. securities markets and broker-dealers under SROs' jurisdiction.[1] SROs include national securities exchanges, registered securities associations, and registered clearing agencies. For example, the New York Stock Exchange, the Financial Industry Regulatory Authority (FINRA), and the Options Clearing Corporation are SROs. The Municipal Securities Rulemaking Board (MSRB) is also an SRO.[2] SROs set standards, conduct examinations, and enforce rules regarding their members, including rules that address, among other things, members' sales practices, operational capabilities, and fees charged.

The Securities Exchange Act of 1934 (Exchange Act) gives the U.S. Securities and Exchange Commission (SEC or agency) broad authority over the securities industry, including the power to register, regulate, and oversee participants in securities markets, including SROs.[3] Generally, SROs must submit to the SEC proposals for new rules and changes to existing rules (hereafter referred to as "proposed rule changes") before implementing the rules. When submitting rules, SROs must follow requirements prescribed by the agency. The SEC then sends notice of the SROs' proposed rule changes to the *Federal Register* to allow for public comment, reviews any comments received, and assesses proposed rule changes for compliance with the Federal securities laws and applicable SEC rules and regulations. The SEC, in approving proposed rule changes, must determine that they are consistent with the Exchange Act.

As of the date of this report, the following three offices in the agency's Division of Trading and Markets (TM) oversee 29 SROs: the Office of the Chief Counsel, the Office of Clearance and Settlement Supervision, and the Office of Market Supervision. In addition to TM, the agency's Office of Municipal Securities (OMS) oversees the MSRB. According to the Exchange Act, as amended by Section 916 of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act), the SEC

---

[1] Generally, broker-dealers must register with the U.S. Securities and Exchange Commission and join an SRO. The term "broker-dealer" refers to brokers, dealers, or firms that act as brokers and dealers (that is, any person engaged in the business of effecting transactions in securities for the account of others, or any person engaged in the business of buying and selling securities for his own account, through a broker or otherwise). 15 U.S.C. § 78c(a)(4)(A) and 15 U.S.C. § 78c(a)(5)(A).

[2] While the MSRB is the principal SRO for the municipal securities market, the MSRB does not enforce or conduct compliance exams and entities registered with the MSRB are not "members." MSRB Rule D-15 defines "member" to mean "a member of the Board".

[3] 15 U.S.C. § 78a, Securities Exchange Act of 1934 (June 6, 1934).

must process SROs' proposed rule changes within specified timeframes. Proper review and processing of proposed rule changes submitted by SROs helps the SEC achieve its mission to protect investors; maintain fair, orderly and efficient markets; and facilitate capital formation.

Proposed Rule Change Types. SROs submit proposed rule changes to the SEC under Section 19 of the Exchange Act and Section 806(e) of Title VIII of the Dodd-Frank Act. The following describes each type of proposed rule change:

- 19(b)(2) – Proposed rule changes submitted under Section 19(b)(2) of the Exchange Act are not effective unless approved by the SEC. These include proposed changes to an SRO's procedures for its transaction reporting system.

- 19(b)(3)(A) – Proposed rule changes submitted under Section 19(b)(3)(A) of the Exchange Act take effect upon submission to the SEC if the changes meet certain criteria. These include proposed changes concerned solely with the administration of an SRO.

- 19(b)(7) – Proposed rule changes submitted under Section 19(b)(7) of the Exchange Act shall be filed concurrently with the Commodity Futures Trading Commission and may take effect upon (1) filing a written certification with the Commodity Futures Trading Commission, (2) a determination by the Commodity Futures Trading Commission that review of the proposed rule change is not necessary, or (3) Commodity Futures Trading Commission approval of the proposed rule change. These include proposed changes concerning higher margin levels, fraud or manipulation, recordkeeping, reporting, or decimal pricing for security futures products.

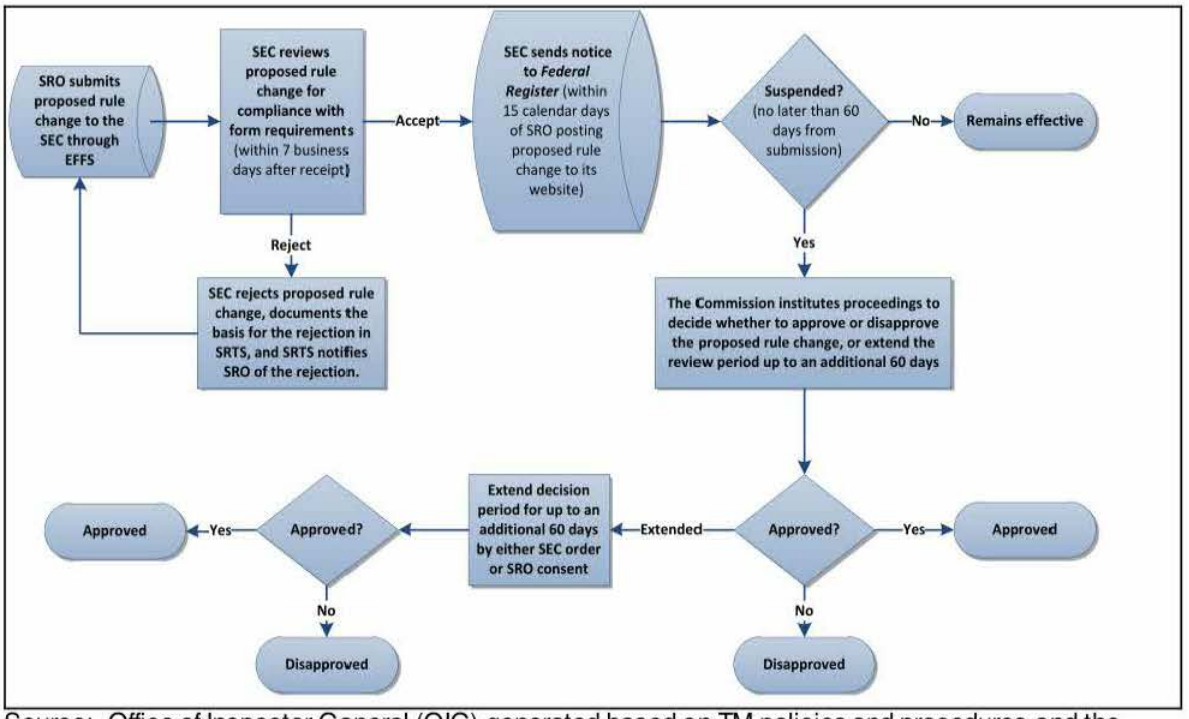
- 806(e)(1) and 806(e)(2) – Proposed rule changes submitted under Sections 806(e)(1) and 806(e)(2) of Title VIII of the Dodd-Frank Act relate to the operations of designated financial market utilities[4] and may take effect if the designated financial market utility does not receive a timely objection from the SEC. These include (1) proposed changes to a designated financial market utility's rules, procedures, or operations that could materially affect the nature or level of risks presented by the designated financial market utility, and (2) changes that are immediately necessary for the designated financial market utility to continue to provide its services in a safe and sound manner.

[4] The term "designated financial market utility" means a financial market utility that the Financial Stability Oversight Council has designated as systemically important under Section 804 of the Dodd-Frank Act. This could include a clearing agency registered with the SEC.

The SEC receives and tracks proposed rule changes using the SRO Rule Tracking System/Electronic Form Filing System (SRTS/EFFS).[5] Specifically, SROs use EFFS – the external web-based component of SRTS/EFFS – to submit to the SEC proposed rule changes. SEC personnel track the proposed changes and respond to the SROs electronically using SRTS – the internal Web-based component of SRTS/EFFS.

The SEC must act on each proposed rule change type according to specific timeframes (or deadlines) and requirements. For example, the following figure illustrates the process for reviewing a proposed rule change submitted as type 19(b)(3)(A) (the type most often received by the SEC in fiscal years (FYs) 2014 and 2015), including publication deadlines and statutory requirements for communicating with the SRO.

Figure: The SEC's Proposed Rule Change Review Process for Rule Type 19(b)(3)(A) Including Publication Deadlines and Statutory Requirements



Source: Office of Inspector General (OIG)-generated based on TM policies and procedures and the Exchange Act, as amended by the Dodd Frank Act.

In FYs 2014 and 2015, the SEC received 3,494 proposed rule changes from 32 SROs.[6] Table 1 shows the number received by the SEC by type and FY.

[5] SRTS and EFFS share system documents (that is, System Security Plan, Authorization to Operate, and Business Impact Analysis) and, therefore, are often referred to as "SRTS/EFFS."

[6] During FYs 2014 and 2015, there were 32 SROs registered with the SEC. As of the date of this report, there were 30 SROs registered with the SEC.

Table 1. Number of Proposed Rule Changes Received by the SEC, by Type and FY

Type	Number Received		Total
	FY 2014	FY 2015	
19(b)(2)	457	383	
19(b)(3)(A)	1,197	1,386	
19(b)(7)	14	14	
806(e)(1)	19	23	
806(e)(2)	0	1	
Total	1,687	1,807	3,494

Source: OIG-generated based on SRTS records.

Annual Performance Goal. The SEC established an annual performance goal for reviewing SROs' proposed rule changes: Performance Goal 1.2.1, *Time to complete SEC review of SRO rules that are subject to SEC approval*. The agency's FYs 2014 and 2015 Annual Performance Reports describe the performance goal as follows: "The SEC reviews SRO rule proposals for consistency with the Exchange Act standards of investor protection, fair and orderly operation of the markets and market structure, as well as other statutory requirements. This metric gauges the timeliness of those reviews."[7] Proposed rule changes subject to this measure are those submitted pursuant to Section 19(b)(2) of the Exchange Act. The agency's goal is to review 70 percent of those proposed rule changes within 45 days after sending notice to the *Federal Register*. The SEC exceeded its goal by 5 percentage points in FY 2014, and fell short of its goal by 7 percentage points in FY 2015. However, in both FYs, the SEC reported meeting all statutory timeframes for 19(b)(2) proposed rule changes 100 percent of the time.

Objectives

Our objectives were to (1) assess the SEC's compliance with applicable laws, regulations, policies, and procedures for reviewing SROs' proposed rule changes, including requirements for communicating with SROs and other external stakeholders when the agency initiated proceedings to determine whether to disapprove an SRO's proposed rule change; and (2) evaluate the information security controls for SRTS/EFFS. In addition, to the extent that prior recommendations were relevant and applicable, we followed up on corrective actions to address recommendations from a previous OIG audit report: *SRO Rule Filing Process,* Audit No. 438 (March 31, 2008).

[7] U.S. Securities and Exchange Commission, *FY 2016 Congressional Justification & FY 2014 Annual Performance Report and FY 2016 Annual Performance Plan* (February 2, 2015); and U.S. Securities and Exchange Commission, *FY 2017 Congressional Justification & FY 2015 Annual Performance Report and FY 2017 Annual Performance Plan* (February 9, 2016).

To address our objectives, we reviewed applicable Federal laws and regulations, SEC policies and procedures, and SRTS/EFFS system documentation. We also interviewed personnel from TM, OMS, and the SEC's Office of Information Technology (OIT). We reviewed the SEC's processing of a statistical and judgmentally selected sample of 345 of the 3,494 proposed rule changes received by the SEC in FYs 2014 and 2015. Finally, we conducted web-based surveys of 20 SROs, requesting information about (1) the SEC's processes for reviewing proposed rule changes and for communicating with SROs, and (2) EFFS functionality and SROs' experiences using the system. Appendix I includes additional information on our scope and methodology, including our sampling and survey methodology, our review of internal controls, prior audit coverage, applicable Federal laws and regulations, and SEC policies and procedures.

Results

Finding 1: TM and OMS Complied With Statutory Requirements and Generally Complied With SEC Policies and Procedures for Reviewing and Processing SROs' Proposed Rule Changes, But Can Better Document the Basis for Rejections

We determined that policies and procedures established by TM and OMS were consistent with applicable statutory requirements of the Exchange Act, as amended by the Dodd-Frank Act. In addition, SROs we surveyed were generally satisfied with EFFS and reported that TM and OMS staff (1) applied processes for reviewing and processing proposed rule changes consistently, and (2) effectively communicated with SROs and other stakeholders when the agency initiated proceedings to determine whether to disapprove an SRO's proposed rule change. Finally, we reviewed TM's and OMS' processing of 345 of the 3,494 proposed rule changes received by the SEC in FYs 2014 and 2015. We found that TM and OMS staff:

- complied with applicable sections of the Exchange Act as amended by the Dodd-Frank Act, and generally complied with agency policies and procedures when reviewing and processing SROs' proposed rule changes; but
- did not consistently document in SRTS the basis for rejecting proposed rule changes, as required by agency policy.

Because SRTS/EFFS did not include the basis for each rejected proposed rule change we reviewed, we determined that the SEC, in some cases, may not have a complete historical record of proposed rule changes rejected in FYs 2014 and 2015.

TM and OMS Complied with the Exchange Act, as amended by the Dodd-Frank Act and Generally Complied with SEC Policies and Procedures

The Exchange Act, as amended by the Dodd-Frank Act, establishes the requirements for the SEC's review and processing of SROs' proposed rule changes. For example, according to the Exchange Act, SROs must submit proposed rule changes in accordance with rules prescribed by the agency. The Dodd-Frank Act amended Section 19(b) of the Exchange Act by, among other things, establishing statutory deadlines by which the SEC must act on proposed rule changes submitted by SROs. To ensure compliance with statutory requirements, TM and OMS established policies

and procedures for reviewing and processing proposed rule changes. These policies and procedures include requirements for submitting notices to the *Federal Register*, documenting the basis for rejecting proposed rule changes,[8] and initiating proceedings to determine whether to disapprove an SRO's proposed rule change. We found that policies and procedures established by TM and OMS to ensure agency compliance with applicable sections of the Exchange Act, as amended by the Dodd-Frank Act, were consistent with statutory requirements.

In addition, we reviewed TM's and OMS' processing of proposed rule changes by selecting a statistical and judgmental sample of 345 of the 3,494 proposed rule changes received by the SEC in FYs 2014 and 2015. We tested sample items for compliance with statutory and agency requirements. Overall, we found that TM and OMS complied with applicable sections of the Exchange Act, as amended by the Dodd-Frank Act, and generally complied with agency policies and procedures when reviewing and processing SROs' proposed rule changes. Requirements we tested included those for:

- rejecting, sending notice for publishing, and acting on proposed rule changes before established deadlines;
- approving or disapproving proposed rule changes;
- instituting proceedings to determine whether to disapprove proposed rule changes and, when necessary, notifying SROs of the grounds for disapprovals; and
- receiving SRO consent for extending the timeframe for reviewing proposed rule changes.

We determined that TM and OMS met or exceeded established timeframes for the 345 items in our sample. For example, the SEC must reject proposed rule changes submitted pursuant to Sections 19(b)(2) and 19(b)(3)(A) of the Exchange Act within 7 business days after receipt. We found that, on average, the agency exceeded this requirement by 2 and 3 business days for the two rule types, respectively. In addition, within 15 calendar days of an SRO posting to its website a proposed rule change submitted under Sections 19(b)(2) and 19(b)(3)(A) of the Exchange Act, the SEC must send notice to the *Federal Register* to allow for public comment. We found that, on average, the agency sent notice to the *Federal Register* for the two rule types within 12 and 8 calendar days, respectively. Based on our testing, we concluded that TM and OMS complied with applicable sections of the Exchange Act, as amended by the Dodd-Frank Act, and generally complied with agency policies and procedures when reviewing and processing SROs' proposed rule changes in FYs 2014 and 2015.

[8] The SEC may reject a proposed rule change within 7 business days after the date of receipt if the proposed rule change is technically defective or incomplete (for example, if it is missing exhibits or does not comply with filing instructions).

TM and OMS Can Better Document the Basis for Rejections

Although TM and OMS established policies and procedures and generally complied with them when reviewing and processing SROs' proposed rule changes in FYs 2014 and 2015, during that time, TM and OMS staff did not consistently document in SRTS the basis for rejecting proposed rule changes. TM and OMS policy requires staff to document in SRTS the basis for rejecting proposed rule changes. Documenting the basis for rejections is important so that the SEC has a complete historical record of each rejected proposed rule change reviewed.

We reviewed 73 of the proposed rule changes rejected by TM and OMS in FYs 2014 and 2015.[9] We found that TM and OMS staff did not document in SRTS the basis for rejecting 17 of the 73 rejected proposed rule changes we reviewed.[10] Nine of these 17 proposed rule changes were included in our statistical sample of proposed rule changes submitted to the SEC pursuant to Sections 19(b)(2) and 19(b)(3)(A) of the Exchange Act.[11] Based on the results of our statistical sampling, we project that agency staff may not have documented in SRTS the basis for rejecting as many as 122 of the 3,399 proposed rule changes submitted to the SEC pursuant to Sections 19(b)(2) and 19(b)(3)(A) of the Exchange Act in FYs 2014 and 2015 (or about 4 percent).[12]

TM and OMS staff were aware of the requirement to document in SRTS the basis for rejecting SROs' proposed rule changes, but did not always comply with established policy. TM and OMS staff told us that they typically discussed with SROs the basis for rejections. OMS staff also provided us e-mails sent to the MSRB that included standard language informing the MSRB that staff rejected a proposed rule change, although the e-mails did not specify the basis for the rejection. We noted that, although staff did not always document in SRTS the basis for rejecting proposed rule changes, staff were able to provide support for most of the rejections when asked. However, TM's Office of Clearance and Settlement could not provide the basis for rejecting five proposed rule changes we reviewed. For one of these five proposed rule changes, staff stated there was nothing in the file to support why they rejected the proposed rule change. Staff told

---

[9] In FYs 2014 and 2015, TM rejected a total of 787 proposed rule changes, and OMS rejected a total of 3 proposed rule changes. Our randomly selected statistical sample from FYs 2014 and 2015 included 50 rejected proposed rule changes submitted by SROs under Sections 19(b)(2) and 19(b)(3)(A) of the Exchange Act. The remaining 23 rejected proposed rule changes that we reviewed were submitted by the MSRB and other SROs under Section 19(b)(7) of the Exchange Act and Section 806(e)(1) of the Dodd-Frank Act.

[10] TM staff rejected 14 of these proposed rule changes and OMS staff rejected the remaining 3.

[11] The remaining 8 proposed rule changes were included as a part of the total population of other rule types we reviewed.

[12] We are 90 percent confident that, in FYs 2014 and 2015, agency staff did not document in SRTS the basis for rejecting between 116 (lower limit) and 128 (upper limit) of the proposed rule changes submitted pursuant to Sections 19(b)(2) and 19(b)(3)(A) of the Exchange Act.

us that they could not determine the basis for rejecting the remaining four proposed rule changes because the person who worked on those proposed rule changes had left the agency.

Because SRTS/EFFS did not include the basis for each rejected proposed rule change we reviewed, we determined that the SEC, in some cases, may not have a complete historical record of proposed rule changes rejected in FYs 2014 and 2015.

Recommendations, Management's Response, and Evaluation of Management's Response

To improve the SEC's process for reviewing SROs' proposed rule changes and ensuring compliance with agency policies and procedures, we recommend that the Division of Trading and Markets and the Office of Municipal Securities:

Recommendation 1: Establish procedures to verify that staff document in the SRO Rule Tracking System the basis for rejecting self-regulatory organizations' proposed rule changes, in accordance with established agency requirements.

Management's Response. The Division of Trading and Markets and the Office of Municipal Securities concurred with the recommendation. The Division of Trading and Markets will take action to coordinate with the Office of Information Technology to enhance the SRO Rule Tracking System/Electronic Form Filing System to automate capture of the reasons for rejection of a filing. The Division of Trading and Markets will work with users outside the Division of Trading and Markets, including the Office of Municipal Securities, to update procedural documentation for each system release as necessary. This release is scheduled for late fall 2016.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 2: Train staff on their responsibilities for documenting in the SRO Rule Tracking System the basis for rejecting self-regulatory organizations' proposed rule changes.

Management's Response. The Division of Trading and Markets and the Office of Municipal Securities concurred with the recommendation. The Division of Trading and Markets will take action to ensure the system release and updated documentation are released to staff that participate in the self-regulatory organization proposed rule filing review process and the Division of Trading and Markets and the Office of Municipal Securities will ensure staff are trained on their responsibilities associated with rejected filings.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 3: Review all proposed rule changes rejected in fiscal years 2014 and 2015 to determine if staff documented in the SRO Rule Tracking System the basis for each rejection, and add the basis for each rejection where missing.

Management's Response. The Division of Trading and Markets and the Office of Municipal Securities concurred with the recommendation. The Division of Trading and Markets and the Office of Municipal Securities will take action, as applicable, to review all rule changes rejected in fiscal years 2014 and 2015 and ensure that the basis for rejection is appropriately documented. Wherever possible, the reason for rejection will be included in SRO Rule Tracking System.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Finding 2: Information Security Controls for the SEC's SRTS/EFFS Need Improvement

According to the National Institute of Standards and Technology (NIST), information security controls are "the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information." The SEC completed a major system upgrade for SRTS/EFFS in 2015; nevertheless, information security controls for the system need improvement. Specifically, we found that

(b)(7)(E)

(b)(7)(E)

[13] The SRTS/EFFS Business Owner – a senior accountant in TM – is familiar with the business uses of the system and is able to authorize access to the information in SRTS/EFFS.

[14] The SRTS/EFFS Information System Owner – a Branch Chief in OIT – is familiar with all technical and system administration/maintenance aspects of SRTS/EFFS.

(b)(7)(E) Furthermore, the Business Owner does not agree with the (b)(7)(E) and stated that OIT officials have not provided a description (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

[15] SEC OIT 24-04A, *Information Security Controls Manual (Rev. 2.1);* November 10, 2015.

[16] U.S. Securities and Exchange Commission, Office of Inspector General, Audit No. 438, *SRO Rule Filing Process*; March 31, 2008.

[17] According to TM's *Access Controls: Policies and Procedures for EFFS and SRTS*, dated September 30, 2015, (b)(7)(E)
(b)(7)(E)

(b)(7)(E)

(b)(7)(E) which could have adversely affected the integrity of the system.

Recommendations, Management's Response, and Evaluation of Management's Response

To improve the SEC's SRTS/EFFS information security controls, we recommend that the Office of Information Technology:

Recommendation 4: Work with the Division of Trading and Markets (b)(7)(E)

(b)(7)(E)

Management's Response. The Office of Information Technology concurred with the recommendation. The Office of Information Technology will take action to meet with the SRO Rule Tracking System/Electronic Form Filing System business owner (b)(7)(E)

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 5: (b)(7)(E)

(b)(7)(E)

Management's Response. The Office of Information concurred with the recommendation. The Office of Information Technology will take action to update (b)(7)(E)

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Finding 3: Contingency Planning Controls for the SEC's SRTS/EFFS Were Inadequate

We determined that contingency planning controls for SRTS/EFFS were inadequate. Specifically, (1) OIT did not update the SRTS/EFFS Business Impact Analysis (BIA) to reflect major system changes, (2) contingency planning documents were inconsistent, and (3) OIT (b)(7)(E)

OIT Did Not Update the SRTS/EFFS BIA to Reflect Major System Changes

We determined that OIT did not update the SRTS/EFFS BIA to reflect major system changes.[18] Specifically, we found that OIT updated the BIA during our audit in March 2016 as part of an SEC-wide initiative to update BIAs for all agency systems. However, before the March 2016 update, OIT did not update or revisit the BIA despite five major system changes that occurred between 2009 and 2015.[19] The ISO inquired about updating the BIA in January 2014 because the release of Version 5.0 (which occurred the previous month) made significant changes to the functionality of the system. However, OIT did not update the BIA in response to the inquiry.

BIAs help identify and prioritize information systems and components critical to supporting the organization's mission and business process, what impact the loss of the system could have on the organization, and the system Recovery Time Objectives

[18] We have previously reported that OIT did not always timely update BIAs: U.S. Securities and Exchange Commission, Office of Inspector General, Report No. 535, *Audit of the SEC's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2015*; June 2, 2016.

[19] According to officials in the OIT Transition Management Branch, SRTS/EFFS has had five major system updates since 2009: (1) SRTS/EFFS Version 2.0 in September 2009, (2) Version 3.0 in June 2010, (3) Version 4.0 in December 2013, (4) Version 5.0 in December 2013, and (5) Version 6.0 in October 2015.

(RTO).[20] NIST SP 800-34 identifies a seven-step process to develop and maintain effective information system contingency plans. According to NIST, the second step in this process, "Conduct Business Impact Analysis," is "a key step in implementing the [Contingency Planning] controls in NIST SP 800-53, and in the contingency planning process overall." Furthermore, NIST states that when a significant change occurs to a system or within the organization, agency staff should update the BIA with the new information to identify new contingency requirements or priorities. Although a major system change does not necessarily require an update to the BIA, we could not find evidence that OIT revisited the SRTS/EFFS BIA for continued accuracy in accordance with SEC policy.

SEC policy states that the BIA is an essential component of the agency's business continuity management program. Specifically, *SEC Implementing Instruction 24-04.09.01 (02.0), Business Impact Analysis* (August 22, 2011), states that "results from the BIA are incorporated into the analysis and strategy formulated during the [business continuity management] program development process, and serve as the primary support in creating contingency plans." The Implementing Instruction also states, "…when the information system undergoes major revisions and at regular intervals in the lifecycle of the completed system, the BIA is revisited for continued accuracy."

OIT personnel did not timely update the SRTS/EFFS BIA, in part, because they did not comply with OIT policies and procedures for updating BIAs to reflect major system changes. OIT officials told us that OIT personnel, with support from a contractor, are currently creating or updating BIAs for new or existing systems that undergo major system upgrades. However, they do not review or revisit BIAs on a cyclical basis. According to OIT officials, in 2012, OIT removed the requirement for supporting the agency's BIA needs from the contract supporting OIT's efforts. In 2015, OIT management assigned the requirement to OIT's Data Center Operations Branch. Because of the delayed reassignment, the agency did not create or update BIAs for SEC systems, including SRTS/EFFS, between calendar years 2013 and 2015.

Without an up-to-date SRTS/EFFS BIA, OIT may be unaware of the systems' current impact on other functional areas of the SEC that could increase the risk that the agency may not recover the system in a timely manner after a failure. In addition, in the event of a failure, SRTS/EFFS data may not be available, as needed which could impact TM's and OMS' ability to meet statutorily mandated timeframes for reviewing and processing SROs' proposed rule changes.

[20] RTO is the period of time within which systems, applications, or functions recover after an outage. RTOs facilitate development and implementation recovery strategies.

SRTS/EFFS Contingency Planning Documents Were Inconsistent

We found inconsistencies in the SRTS/EFFS contingency planning documents. Specifically, the SRTS/EFFS RTO established in the system's BIA and stated in other contingency planning documents, such as the Information System Contingency Plan (ISCP) and the Enterprise Disaster Recovery Plan (EDRP), was inconsistent. For example, the 2016 BIA [redacted] However, the system's ISCP, which refers to the March 2009 BIA, states that SRTS/EFFS is a [redacted] Additionally, the system's EDRP identifies SRTS/EFFS [redacted] Table 2 describes differences in the SRTS/EFFS RTO according to each system contingency planning document.

Table 2. SRTS/EFFS RTO as Described in System Contingency Planning Documents

Contingency Planning Document	Document Date	RTO
BIA	March 2009	[redacted]
	March 2016	
ISCP	September 2015	
EDRP	December 2014	

Source: SEC-OIG generated based on contingency planning documents.

According to OIT's *Information Technology Contingency Planning Handbook*, the ISO is responsible for developing, documenting, testing, updating and maintaining ISCPs and ensuring ISCPs, disaster recovery procedures, disaster recovery test plans, BIAs, and standard operating procedures reflect changes in the system and/or organization. The OIT Data Center Operations Branch is responsible for updating and maintaining the SEC EDRP. Although the SRTS/EFFS ISO and officials from the OIT Data Center Operations Branch agreed that the system's RTO should be consistent across system documents, they could not explain the inconsistencies we observed.

[21] According to the Federal Continuity Directive 1, *Federal Executive Branch National Continuity Program and Requirements*, mission essential Functions are those functions that enable an organization to provide vital services, exercise civil authority, maintain the safety of the public, and sustain the industrial/economic base. The Directive defines primary mission essential functions as those essential functions that organizations must perform to support or implement the performance of national essential functions before, during, and in the aftermath of an emergency. Organizations need to continuously perform primary mission essential functions during continuity activation or resume such functions within 12 hours of an event and must maintain all primary mission essential functions until they can resume normal operations. National essential functions represent the overarching responsibilities of the Federal Government to lead and sustain the Nation and are the primary focus of the Federal Government's leadership during and in the aftermath of an emergency.

Without consistent SRTS/EFFS contingency planning documents, OIT may not recover the system in the appropriate timeframe during an outage. This could adversely affect TM's and OMS' day-to-day operations and the SEC's ability to comply with statutory requirements for reviewing and processing SROs' proposed rule changes.

(b)(7)(E)

As stated earlier, the SRTS/EFFS 2016 BIA (b)(7)(E)

(b)(7)(E)

However, according to OIT personnel, SRTS/EFFS (b)(7)(E)

(b)(7)(E)

According to the Federal Continuity Directive 1, *Federal Executive Branch National Continuity Program and Requirements*, the identification and prioritization of essential functions are prerequisites for continuity planning. These functions establish the planning parameters that drive an organization's efforts in all other planning and preparedness areas. Furthermore, the Directive states that the goal of continuity in the executive branch is the continuation of National Essential Functions. To achieve that goal, agencies must identify mission essential functions and primary mission essential functions, and ensure that they can be continued throughout, or resumed rapidly after a disruption of normal activities. Federal Continuity Directive 1 identifies three categories of essential functions: National Essential Functions, Primary Missions Essential Functions, and Mission Essential Functions.[23]

As stated in the SEC EDRP, in the event of an emergency, system recovery follows the recovery priorities and RTO established in each application's BIA. In addition, system

---

[22] During the BIA process, OIT uses information provided by the Business Owner and ISO to perform a weighted analysis, assign an RTO, and assign system rankings for recovery in the agency EDRP. As a

(b)(7)(E)

[23] National essential functions are functions and overarching responsibilities of the federal government to lead and sustain the Nation that the President and national leadership will focus on during a catastrophic emergency. Primary mission essential functions need to be continuous or resumed within 12 hours after an event and maintained for up to 30 days or until normal operations resume. Mission Essential Functions are those functions that enable an organization to provide vital services, exercise civil authority, maintain the safety of the public, and sustain the industrial/economic base during disruption of normal operations.

(b)(7)(E)

(b)(7)(E)

Recommendations, Management's Response, and Evaluation of Management's Response

To improve the SEC's information security controls, we recommend that the Office of Information Technology:

Recommendation 6: In conjunction with the Division of Trading and Markets, review the Business Impact Analysis for the SRO Rule Tracking System/Electronic Form Filing System to determine whether the system supports (b)(7)(E) and, as appropriate, update the system's contingency planning documents (Business Impact Analysis, Information System Contingency Plan, and Enterprise Disaster Recovery Plan) to ensure they are consistent.

Management's Response. The Office of Information concurred with the recommendation. The Office of Information Technology will coordinate with the Division of Trading and Markets and perform a comprehensive review of the SRO Rule Tracking System/Electronic Form Filing System (SRTS/EFFS) Business Impact Analysis (BIA) and form a consensus with respect to the application's mission criticality. The Office of Information Technology will also perform a review of the SRTS/EFFS BIA, Information System Contingency Plan, and Enterprise Disaster Recovery Plan and ensure all three documents are consistent.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Recommendation 7: Establish procedures to conduct cyclical reviews of the Business Impact Analyses for each of the agency's systems, and ensure staff documents such reviews.

Management's Response. The Office of Information concurred with the recommendation. The Office of Information Technology will develop a process to ensure that cyclical reviews of agency system Business Impact Analyses are conducted and documented.

OIG's Evaluation of Management's Response. Management's proposed actions are responsive; therefore, the recommendation is resolved and will be closed upon verification of the action taken.

Appendix I. Scope and Methodology

We conducted this performance audit from September 2015 through September 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Scope. The audit covered proposed rule changes received by to the SEC in FYs 2014 and 2015 (between October 1, 2013, and September 30, 2015). Our objectives were to (1) assess the SEC's compliance with applicable laws, regulations, policies, and procedures for reviewing SROs' proposed rule changes, including requirements for communicating with SROs and other external stakeholders when the agency initiated proceedings to determine whether to disapprove an SRO's proposed rule change; and (2) evaluate the information security controls for the SRTS/EFFS. In addition, to the extent that prior recommendations were relevant and applicable, we followed up on corrective actions to address recommendations from a previous OIG audit report: *SRO Rule Filing Process,* Audit No. 438 (March 31, 2008). We conducted fieldwork at the SEC's Headquarters in Washington, DC and, as described below, corresponded with SRO personnel.

Methodology. To address our audit objectives, we reviewed TM and OMS policies and procedures for reviewing and processing proposed rule changes and applicable Federal laws and regulations including the following:

- 15 U.S.C. § 78s – *Registration, responsibilities, and oversight of self-regulatory organizations*.
- Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1833 (2010) (codified as amended in various sections of the U.S. Code).
- 17 Code of Federal Regulations, part 200 – *Organization; Conduct and Ethics; and Information and Requests*.
- 17 Code of Federal Regulations, part 201 – *Rules of Practice*.
- 17 Code of Federal Regulations, part 202 – *Informal and Other Procedures*.
- 17 Code of Federal Regulations, part 240 – *General Rules and Regulations, Securities Exchange Act of 1934*.
- Executive Order No. 13579, *Regulation and Independent Regulatory Agencies* (July 14, 2011).
- U.S. Dept. of Homeland Security, Federal Continuity Directive 1, *Federal Executive Branch National Continuity Program and Requirements* (October 2012).

We also reviewed relevant guidance from NIST, OIT policies and procedures, and SRTS/EFFS system documentation, and we interviewed personnel from TM, OMS, and OIT.

To assess the SEC's compliance with laws, regulations, policies, and procedures for reviewing SROs' proposed rule changes, we took two approaches. First, we reviewed the SEC's processing of all:

- 24 proposed rule changes received by the SEC in FYs 2014 and 2015 from the MSRB under Sections 19(b)(2) and 19(b)(3)(A) of the Exchange Act,
- 28 proposed rule changes received by the SEC in FYs 2014 and 2015 under Section 19(b)(7) of the Exchange Act, and
- 43 proposed rule changes received by the SEC in FYs 2014 and 2015 under Sections 806(e)(1) and 806(e)(2) of the Dodd-Frank Act.

Second, using a sampling methodology provided by a contractor, Data and Analytic Solutions, Inc., we selected and reviewed a sample of 250 of the 3,399 proposed rule changes received by the SEC in FYs 2014 and 2015 pursuant to Sections 19(b)(2) and 19(b)(3)(A) of the Exchange Act. Our review of the SEC's processing of proposed rule changes was limited to determining whether information (1) in SRTS, (2) in the *Federal Register*, and (3) on SRO websites was consistent and complied with requirements of the Exchange Act, the Dodd-Frank Act, and agency policies and procedures. In addition, we determined if the SEC complied with provisions of the Exchange Act, as amended by the Dodd-Frank Act, and agency policies and procedures when reviewing proposed rule changes. Our sample size was determined using the following parameters:

- a presumed error rate of ±6% percent,
- a desired maximum precision range of 10 percent, and
- a desired confidence level of 90 percent.

We used a random number generator to select items for testing from the population of proposed rule changes received by the SEC in FYs 2014 and 2015. For FY 2014, we selected 16 19(b)(2) type proposed rule changes and 97 19(b)(3)(A) type proposed rule changes (for a total of 113 proposed rule changes). For FY 2015, we selected 8 19(b)(2) type proposed rule changes and 129 19(b)(3)(A) type proposed rule changes (for a total of 137 proposed rule changes). In total, we reviewed the SEC's processing of 345 of the 3,494 proposed rule changes (or about 10 percent) received by the SEC in FYs 2014 and 2015.

In April 2016, we sent web-based surveys to 20 SROs that submitted to the SEC proposed rule changes in FYs 2014 and 2015. Based on the type of proposed rule change submitted most often by each SRO, we sent 11 SROs 1 of 3 "legal surveys" requesting information about the SEC's processes for reviewing proposed rule changes

and for communicating with SROs. Two of the 11 survey respondents reported inconsistencies in the agency's approval of "copycat" rules.[24] However, we were unable to confirm such concerns. We also sent nine SROs an "EFFS user survey" requesting information about EFFS functionality and SROs' experiences using the system. Table 3 shows the survey description, number of surveys sent by type, number completed, and the response rate for each survey type as of the date of this report.

Table 3. Number of Surveys Sent by Type, Number Completed, and Response Rate

Survey Description	Number Sent	Number Completed	Response Rate
19(b)(2) and 19(b)(3)(A) - Legal Survey	8	5	63%
19(b)(7) - Legal Survey	2	2	100%
19(b)(2), 19(b)(3)(A), and 19(b)(7) - Legal Survey	1	1	100%
Subtotal	**11**	**8**	
EFFS User Survey	9	7	78%
Total	**20**	**15**	

Source: SEC-OIG generated.

Internal Controls. We gained an understanding of the SEC's process for reviewing SROs' proposed rule changes and identified key internal controls related to our objectives, including key system controls for SRTS/EFFS. TM and OMS staff provided a walkthrough of their processes for reviewing a proposed rule change. We also obtained a copy of TM's and OMS' FYs 2014 and 2015 management assurance statements. We determined that TM identified an internal control weaknesses that did not pertain to the SRO proposed rule change process, and OMS mitigated the risks identified in its management assurance statement.

As discussed in this report, we found that the SEC complied with applicable sections of the Exchange Act, as amended by the Dodd-Frank Act, and generally complied with agency policies and procedures for reviewing and processing proposed rule changes during the period reviewed. However, TM and OMS staff did not consistently document in SRTS the basis for rejecting proposed rule changes, as required by TM and OMS policy. Furthermore, the SRTS/EFFS Business Owner and OIT did not (b)(7)(E) (b)(7)(E) (b)(7)(E) Lastly, contingency planning controls for SRTS/EFFS were inadequate. Our recommendations, if implemented, should correct the weaknesses we identified.

[24] Copycat rules are proposed rule changes based on similar rules of another SRO or of the Commission.

Computer-processed Data. The U.S. Government Accountability Office's (GAO) *Assessing the Reliability of Computer-Processed Data* (GAO-09-680G, 2009) states that "data reliability refers to the accuracy and completeness of computer-processed data, given the uses they are intended for. Computer-processed data may be data (1) entered into a computer system or (2) resulting from computer processing." Furthermore, GAO-09-680G defines "reliability," "accuracy," and "completeness" as follows:

- "Reliability" means that data are reasonably complete and accurate, meet your intended purposes, and are not subject to inappropriate alteration.
- "Accuracy" refers to the extent that recorded data reflect the actual underlying information.
- "Completeness" refers to the extent that relevant records are present and the fields in each record are appropriately populated.

The computer-processed information that had a material impact on our objectives, findings, conclusions, and recommendations was the information in SRTS. We compared information in SRTS with information in the *Federal Register* and the SROs' websites for the 345 proposed rule changes we reviewed and for 27 other judgmentally selected proposed rule changes that were not included in our sample. Based on these steps, we determined the information in SRTS was sufficiently reliable for the purpose of the audit.

Prior Audit Coverage. During the last 8 years, the SEC OIG and GAO issued three reports of particular relevance to this audit.

SEC OIG:

- *SRO Rule Filing Process*, Audit No. 438, March 31, 2008.

  The OIG's 2008 report made 19 recommendations to improve TM's process for reviewing proposed rule changes. We determined that TM took actions to address the recommendations and the OIG closed all 19 recommendations. We also determined that TM has enhanced its process for reviewing and managing SROs' proposed rule changes since the 2008 audit. For example, SRTS e-mails staff assigned to review and process proposed rule changes to remind staff of critical timeframes and notify staff when a change has occurred. Also, beginning in June 2010, "noteworthy" (as determined by a TM Associate Director) proposed rule changes are included on an SRO Dashboard of Noteworthy Filings. Examples of noteworthy filings include 19(b)(2) filings that TM is considering disapproving, filings for which TM is considering instituting (or has instituted) disapproval proceedings, or filings that have attracted material comment letters. However, we also found that OIT and TM did not review SRTS/EFFS user accounts in accordance with SEC policy, which is a repeat finding.

- *Audit of the SEC's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2015*, Report No. 535, June 2, 2016.

  This audit identified two other matters of interest related to our audit objectives. Specifically, the OIG determined that the SEC did not always update (1) Business Impact Analyses and (2) contingency planning documents to reflect major system changes.

Unrestricted SEC OIG reports can be accessed at: http://www.sec.gov/about/offices/oig/inspector_general_audits_reports.shtml.

GAO:

- *Opportunities Exist to Improve SEC's Oversight of the Financial Industry Regulatory Authority*, GAO-12-625, May 2012.

  GAO found that TM had taken steps to strengthen its review of FINRA's proposed rule changes by: (1) developing a more formal structure to consult with the SEC's Office of Compliance Inspections and Examinations, (2) strengthening and clarifying the SRO rule filing process, (3) tracking complex proposed rule changes under review because of certain procedures under Section 19(b) of the Exchange Act modified by Section 916 of the Dodd-Frank Act, and (4) assisting in organizing the SEC's SRO outreach conference in January 2012 to promote transparency of and provide information on the SRO rule filing process.

Unrestricted GAO reports can be accessed at: http://www.gao.gov/.

Appendix II. Management Comments

MEMORANDUM

TO: Rebecca Sharek, Deputy Inspector General for Audits, Evaluations, and Special Projects

FROM: Steve Luparello, Director, Division of Trading and Markets
Pamela Dyson, Chief Information Officer
Jessica Kane, Director, Office of Municipal Securities

DATE: September 20, 2016

SUBJECT: Audit of the SEC's Process for Reviewing Self-Regulatory Organizations' Proposed Rule Changes

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) memorandum on the audit of the SEC's process for reviewing self-regulatory organizations' (SRO) proposed rule changes. We are pleased that the OIG's audit found that: (i) the Division of Trading and Markets (TM) and the Office of Municipal Securities (OMS) policies and procedures were consistent with statutory requirements for reviewing and processing proposed rule changes; (ii) the SROs surveyed were generally satisfied with the Electronic Form Filing System (EFFS) and reported that TM and OMS staff (1) applied processes for reviewing and processing proposed rule changes consistently, and (2) effectively communicated with SROs and other stakeholders when the agency initiated proceedings to determine whether to disapprove an SRO's proposed rule change; (iii) that the review of TM's and OMS' processing of 345 of the 3,494 proposed rule changes received by the SEC in fiscal years 2014 and 2015 and found that TM and OMS staff complied with statutory requirements and generally complied with agency policies and procedures; and (iv) further that TM and OMS met or exceeded established the statutory timeframes for acting on the filings. Report No. 537 contains seven recommendations with which we concur. Below, we have indicated the actions we have taken or intend to take for each recommendation.

Recommendation 1: Establish procedures to verify that staff document in the SRO Rule Tracking System the basis for rejecting self-regulatory organizations' proposed rule changes, in accordance with established agency requirements.

Response: Concur. TM will take action to coordinate with the Office of Information Technology (OIT) to enhance the SRTS/EFFS system to automate capture of the reasons for rejection of a filing. TM will work with users outside TM, including OMS, to update procedural documentation for each system release as necessary. This release is scheduled for late fall 2016.

Recommendation 2: Train staff on their responsibilities for documenting in the SRO Rule Tracking System the basis for rejecting self-regulatory organizations' proposed rule changes.

Response: Concur. TM will take action to ensure the system release and updated documentation are released to staff that participate in the SRO proposed rule filing review process and TM and OMS will ensure staff are trained on their responsibilities associated with rejected filings. In past releases, training consisted of a combination of live demonstration, updated documentation, and communication outlining changes and associated requirements.

Recommendations 3: Review all proposed rule changes rejected in fiscal years 2014 and 2015 to determine if staff documented in the SRO Rule Tracking System the basis for each rejection, and add the basis for each rejection where missing.

Response: Concur. TM and OMS will take action, as applicable, to review all rule changes rejected in fiscal years 2014 and 2015 and ensure that the basis for rejection is appropriately documented. Wherever possible, the reason for rejection will be included in SRTS.

Recommendation 4: Work with the TM (b)(7)(E)
(b)(7)(E)

Response: Concur. The OIT will take action to meet with the SRTS/EFFS business owner (b)(7)(E)

Recommendation 5: (b)(7)(E)
(b)(7)(E)

Response: Concur. The OIT will take action to (b)(7)(E)
(b)(7)(E)
(b)(7)(E)

Recommendation 6: In conjunction with the Division of Trading and Markets, review the Business Impact Analysis for the SRO Rule Tracking System/Electronic Form Filing System to determine whether the system (b)(7)(E) and, as appropriate, update the system's contingency planning documents (Business Impact Analysis, Information System Contingency Plan, and Enterprise Disaster Recovery Plan) to ensure they are consistent.

Response: Concur. The OIT will take action to coordinate with TM and perform a comprehensive review of the SRTS/EFFS Business Impact Analysis (BIA) and form a consensus with respect to the application's mission criticality. OIT will also take action to perform a review of the SRTS/EFFS BIA, Information System Contingency

Plan, and Enterprise Disaster Recovery Plan and ensure all three documents are consistent.

Recommendation 7: Establish procedures to conduct cyclical reviews of the Business Impact Analyses for each of the agency's systems, and ensure staff documents such reviews.

Response: Concur. The OIT will take action to develop a process to ensure that cyclical reviews of agency system BIAs are conducted and documented.

Thank you for the consideration that you and your staff have shown throughout the engagement. We look forward to continuing our productive dialogue in the coming months on the SEC's efforts to address the areas noted in your report. If you have any questions, or you would like to discuss this response in more detail, please contact Jennah Mathieson at (202) 551-4541.

Major Contributors to the Report

Kelli Brown-Barnes, Audit Manager

Andrea Holmes, Lead Auditor

John Dettinger, Auditor

Nicolas Harrison, Auditor

To Report Fraud, Waste, or Abuse, Please Contact:

Web: www.reportlineweb.com/sec_oig

Telephone: (877) 442-0854

Fax: (202) 772-9265

Address: U.S. Securities and Exchange Commission
Office of Inspector General
100 F Street, N.E.
Washington, DC 20549

Comments and Suggestions

If you wish to comment on the quality or usefulness of this report or suggest ideas for future audits, evaluations, or reviews, please send an e-mail to OIG Audit Planning at AUDplanning@sec.gov. Comments and requests can also be mailed to the attention of the Deputy Inspector General for Audits, Evaluations, and Special Projects at the address listed above.