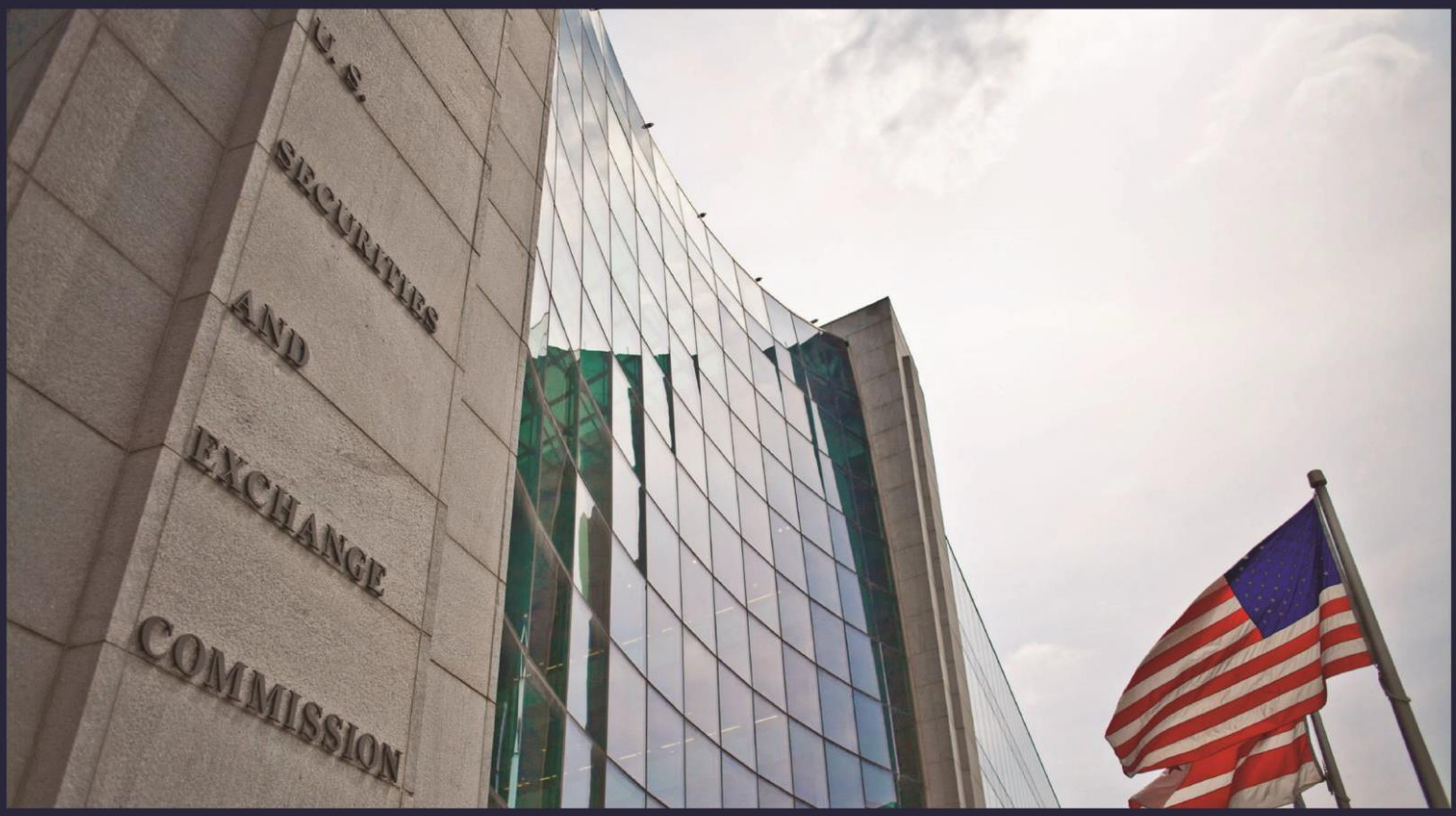
U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

# TCP Established Method To Effectively Oversee Entity Compliance With Regulation SCI But Could Improve Aspects of Program Management




September 24, 2018
Report No. 551

**REDACTED FOR PUBLIC RELEASE**

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

OFFICE OF
INSPECTOR GENERAL

# MEMORANDUM

September 24, 2018

**TO:** Peter Driscoll, Director, Office of Compliance Inspections and Examinations

**FROM:** Carl W. Hoecker, Inspector General

**SUBJECT:** *TCP Established Method To Effectively Oversee Entity Compliance With Regulation SCI But Could Improve Aspects of Program Management*, Report No. 551

Attached is the Office of Inspector General (OIG) final report detailing the results of our evaluation of the Office of Compliance Inspections and Examinations' (OCIE) Technology Controls Program (TCP). The report contains three recommendations that should help improve TCP program management.

On September 7, 2018, we provided management with a draft of our report for review and comment. In its September 20, 2018, response, management concurred with our recommendations. We have included management's 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 OCIE will address the recommendations.

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

Attachment

cc: Jay Clayton, Chairman
Lucas Moskowitz, Chief of Staff, Office of Chairman Clayton
Sean Memon, Deputy Chief of Staff, Office of Chairman Clayton
Peter Uhlmann, Managing Executive, Office of Chairman Clayton
Kara M. Stein, Commissioner
Robert Peak, Advisor to the Commissioner, Office of Commissioner Stein
Robert J. Jackson Jr., Commissioner
Caroline Crenshaw, Counsel, Office of Commissioner Jackson
Prashant Yerramalli, Counsel, Office of Commissioner Jackson

Hester M. Peirce, Commissioner
Jonathan Carr, Counsel, Office of Commissioner Peirce
Elad Roisman, Commissioner
Christina Thomas, Counsel, Office of Commissioner Roisman
Robert B. Stebbins, General Counsel
Rick Fleming, Investor Advocate
John J. Nester, Director, Office of Public Affairs
Bryan Wood, Director, Office of Legislative and Intergovernmental Affairs
Daniel Kahl, Chief Counsel, Office of Compliance Inspections and Examinations
Robert Fisher, Managing Executive, Office of Compliance Inspections and Examinations
Keith Cassidy, Associate Director, Office of Compliance Inspections and Examinations, Technology Controls Program
Jennifer McCarthy, Assistant Director, Office of Compliance Inspections and Examinations, Office of Legal and Policy Guidance
Kenneth Johnson, Chief Operating Officer
Vance Cathell, Director, Office of Acquisitions
Gregory Steigerwald, Competition Advocate, Office of Acquisitions
Julie Erhardt, Acting Chief Risk Officer, Office of the Chief Operating Officer

# Executive Summary

## TCP Established Method To Effectively Oversee Entity Compliance With Regulation SCI But Could Improve Aspects of Program Management

Report No. 551
September 24, 2018

## Why We Did This Evaluation

In recent years, several factors, including a significant number of systems issues at exchanges and other trading venues, increased concerns over "single points of failure" in the U.S. securities markets. These concerns contributed to the U.S. Securities and Exchange Commission's (SEC or agency) decision to address technological vulnerabilities and improve agency oversight of the core technology of key U.S. securities markets entities. In November 2014, the SEC adopted Regulation Systems Compliance and Integrity (SCI), under which the agency monitors the security and capabilities of U.S. securities markets' technological infrastructure. The SEC's Office of Compliance Inspections and Examinations' (OCIE) Technology Controls Program (TCP) is responsible for ensuring entities comply with Regulation SCI and for evaluating whether entities have established, maintained, and enforced written policies and procedures reasonably designed to ensure the capacity, integrity, resiliency, availability, and security of their Regulation SCI systems. We initiated this evaluation to assess OCIE's TCP and determine whether the program provided effective oversight of entities' compliance with Regulation SCI.

## What We Recommended

At the outset of our evaluation, TCP management identified ongoing improvement initiatives and began implementing changes. To further improve TCP program management, we recommend that OCIE: (1) ensure TCP management updates the TCP Examination Manual in a timely manner following TCPs' transition to TRENDS; (2) identify and document the risks and controls related to TCP operations, and update OCIE's RCM accordingly; and (3) ensure TCP management properly plans and documents TCP's transition to TRENDS, and retains all relevant materials in a central location. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action. This report contains non-public information that we redacted (deleted) to create this public version.

## What We Found

TCP has an established method to effectively oversee entity compliance with Regulation SCI. The program assesses compliance through its CyberWatch program and through TCP examinations. However, we identified opportunities to improve aspects of TCP program management. Specifically, we found that TCP's examination manuals in effect at the outset of our evaluation were outdated; management had not identified or documented TCP risks and control activities in OCIE's internal risk and control matrix (RCM), and TCPs' development of the Technology Risk-Assurance, Compliance, and Examination Report (TRACER) system—the program's system of record—was not well-planned or documented.

*Examination Manuals*. The TCP Examination Manual and draft TRACER Examination User Manual in effect at the outset of our evaluation were outdated and did not align with TCP examination practices. Management was in the process of revising the TCP Examination Manual and, on June 25, 2018, released an updated version.

*Risks and Control Activities.* TCP management had not identified or documented the program's risks and corresponding control activities in OCIE's RCM. Although TCP examinations appear to have similar risks and controls as other OCIE examinations, documentation we reviewed did not clearly identify comparable documented control activities specific to TCP examination processes for all identified risks.

*TRACER Development.* Between September 2015 and January 2018, TCP continued development of the SEC's TRACER system at a cost of nearly $780,000. As the system's business owner during that time, TCP oversaw frequent (sometimes weekly) system updates, but did not properly plan or document its development efforts. TRACER's purpose and functions evolved over time as TCP was considering continued development of the system or migration to an existing OCIE system known as the Tracking and Reporting Examinations National Documentation System (TRENDS). Certain planned system capabilities were not realized and it is unclear, based on a lack of documentation, how TCP assessed or managed system requirements. On May 4, 2018, TCP management decided to discontinue developing TRACER and transition its examination program to TRENDS, which is expected to yield operational and cost savings benefits. Migration from TRACER to TRENDS is expected to be complete by late 2018.

We also identified two other matters of interest for management's consideration. First, a majority of TCP staff who responded to a survey we administered indicated that they either did not receive adequate training or only sometimes received adequate training. TCP management has completed a three-year training plan. We encourage management to continue to review TCP staff training to ensure staff have the knowledge and skills necessary to perform TCP examinations. Secondly, we identified a gap in the Office of Acquisitions' process for reviewing contracting officer's representatives' files. We suggest that the Office of Acquisitions consider establishing follow-up procedures to address this gap.

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

# TABLE OF CONTENTS



# ABBREVIATIONS

| | |
|---|---|
| ARP | Automation Review Policy |
| COR | contracting officer's representative |
| Dodd-Frank Act | Dodd-Frank Wall Street Reform and Consumer Protection Act |
| FY | fiscal year |
| GAO | U.S. Government Accountability Office |
| NEP | National Examination Program |
| OA | Office of Acquisitions |
| OCIE | Office of Compliance Inspections and Examinations |
| OIG | Office of Inspector General |
| RCM | Risk and Control Matrix |
| SCI | Systems Compliance and Integrity |
| SEC or agency | U.S. Securities and Exchange Commission |
| SECR | SEC Administrative Regulation |
| TCP | Technology Controls Program |
| TM | Division of Trading and Markets |
| TRACER | Technology Risk-Assurance, Compliance, and Examination Report |
| TRENDS | Tracking and Reporting Examination National Documentation System |

# Background and Objective

## Background

In recent years, technological advances have transformed the U.S. securities markets, which, among other things, substantially enhanced the speed, capacity, efficiency, and sophistication of the trading functions available to market participants.[1] At the same time, technological advances have increased the risk of operational problems with automated systems, including failures, disruptions, delays, and intrusions. Given the speed and interconnected nature of the U.S. securities markets, a seemingly minor systems problem at a single entity can quickly create losses and liability for market participants, and spread rapidly across the national market system, potentially creating widespread damage and harm to market participants, including investors.

Several factors, including a significant number of systems issues at exchanges and other trading venues, increased concerns over "single points of failure" in the U.S. securities markets. These concerns contributed to the U.S. Securities and Exchange Commission's (SEC or agency) decision to address technological vulnerabilities and improve agency oversight of the core technology of key U.S. securities markets entities.

For more than two decades, SEC oversight of the technology of the U.S. securities markets had been conducted primarily pursuant to a voluntary set of principles. These principles were articulated in the SEC's Automation Review Policy (ARP) Statements[2] and were applied through an inspection program of, at the time, about 25 entities, including securities exchanges, clearing organizations, and electronic communication networks. The SEC's Division of Market Regulation (now known as the Division of Trading and Markets (TM)) administered the ARP inspection program. Because of the voluntary nature of the program, the SEC, at times, had difficulty obtaining cooperation with its recommendations for improvement. In 1998, the Office of Inspector General (OIG) recommended that the SEC reconsider whether the ARP should remain a voluntary program, or become mandatory through rule-making, and determine how the agency assessed compliance with the program.[3] In 2004, the U.S. Government

[1] See Securities Exchange Act Release No. 61358 (January 14, 2010), 75 FR 3594 (January 21, 2010) (Concept Release on Equity Market Structure).

[2] The SEC established the ARP through two policy statements, titled *Automated Systems of Self-Regulatory Organizations*, issued in 1989 and 1991, respectively.

[3] U.S. Securities and Exchange Commission, Office of Inspector General, *Oversight of SRO Automation* (Audit No. 268; May 18, 1998).

Accountability Office (GAO) also criticized the voluntary nature of the ARP program and recommended that the SEC propose a rule making the program mandatory.[4]

**Regulation SCI.** In November 2014, the SEC adopted Regulation Systems Compliance and Integrity (SCI),[5] under which the agency monitors the security and capabilities of U.S. securities markets' technological infrastructure. Entities subject to Regulation SCI (hereafter referred to as SCI entities) include:

- self-regulatory organizations (including stock and options exchanges, registered clearing agencies, the Financial Industry Regulatory Authority, and the Municipal Securities Rulemaking Board);
- alternative trading systems that trade national market system and non-national market system stocks exceeding specified volume thresholds;
- disseminators of consolidated market data (known as plan processors); and
- certain exempt clearing agencies.

Regulation SCI applies primarily to the systems of SCI entities that directly support any one of the following six key securities market functions: (1) trading, (2) clearance and settlement, (3) order routing, (4) market data, (5) market regulation, and (6) market surveillance. The regulation established seven rules for SCI entities pertaining to, among other things, the entities' system policies and procedures, business continuity and disaster recovery plans, recordkeeping requirements, and system changes. The rules are designed to reduce the occurrence of systems issues, improve resiliency when systems problems occur, and enhance the SEC's oversight and enforcement of securities market technology infrastructure. A key element of compliance is timely reporting to the SEC when an SCI entity experiences an SCI event (that is, a systems disruption, a systems intrusion, or a systems compliance issue). The SEC required SCI entities to begin complying with Regulation SCI as of November 3, 2015.

**OCIE's TCP.** In February 2014, ARP transitioned from a voluntary program under TM's direction to a full examination program—the Technology Controls Program (TCP)—under the Office of Compliance Inspections and Examinations (OCIE). TCP is primarily responsible for overseeing entities' compliance with Regulation SCI. As of July 2018, TCP included 26 SEC employees (many of whom are information technology specialists) and 13 contractor employees located at the SEC's headquarters in Washington, DC, and at the agency's Chicago and New York regional offices. TCP assesses compliance with Regulation SCI by evaluating whether SCI entities have

[4] U.S. Government Accountability Office, *Financial Market Preparedness: Improvements Made, but More Action Needed to Prepare for Wide-Scale Disasters* (GAO-04-984; September 27, 2004).

[5] 17 C.F.R. §242.1000-1007.

established, maintained, and enforced written policies and procedures reasonably designed to ensure the capacity, integrity, resiliency, availability, and security of their systems.

As part of its oversight of Regulation SCI compliance, TCP developed the CyberWatch program, which is responsible for receiving and reviewing forms and reports required of SCI entities. The program uses contractor personnel to conduct real-time monitoring and analysis of SCI entity system disruptions, intrusions, and compliance issues, and to serve as the point-of-contact for entities experiencing an SCI event.[6] A TCP Senior Specialized Examiner serves as the contracting officer's representative (COR) who oversees contractor employees in the CyberWatch program and reviews their work. A TCP Assistant Director manages the work of the TCP Senior Specialized Examiner and TCP's CyberWatch program.

In addition, although Regulation SCI does not require examinations of SCI entities, as part of the SEC's National Exam Program (NEP),[7] TCP examines SCI entities based on several factors. TCP performed 61 examinations in fiscal year (FY) 2016 and 70 examinations in FY 2017.

**Program Improvement Efforts**. At the outset of our evaluation, TCP management identified planned and ongoing program improvement initiatives. TCP's Associate Director stated that he was reviewing the possibility of either (a) enhancing Technology Risk-Assurance, Compliance, and Examination Report's (TRACER) features, or (b) using OCIE's Tracking and Reporting Examinations National Documentation System (TRENDS) instead of TRACER. Management noted that, from 2013 (before ARP functions were transferred to OCIE) through May 2018, TM and then TCP staff worked to develop the TRACER system. As discussed in the Results section, in May 2018, new OCIE and TCP leadership (appointed in January and July 2017, respectively), decided to discontinue TRACER and move TCP examination functions to TRENDS.

Other ongoing initiatives included a rewrite of the TCP Examination Manual; improvements to TCP's risk-scoping process for selecting entity for reviews; development of modeling processes, documentation standards, and tools for more sophisticated analysis; and enhancements to TCP's training requirements. In addition, TCP's Associate Director planned to establish a process to make TCP staff available for consultation and analysis to the SEC, at large, and particularly to other OCIE examination programs.

[6] In May 2017, the SEC entered into the current CyberWatch contract: a blanket purchase agreement (contract number SECHQ117A0014) with Iron Vine Security, LLC. Typical CyberWatch support requirements include monitoring SCI entities; responding to SCI entities' phone calls and/or e-mails; processing Regulation SCI filings; triaging Tips, Complaints, and Referrals; producing reports; supporting exams; and conducting regular briefings with TCP staff.

[7] OCIE administers the NEP and conducts examinations and oversight of registered entities including investment advisers, mutual funds and exchange-traded funds, broker-dealers, transfer agents, securities exchanges, and self-regulatory organizations such as the Financial Industry Regulatory Authority.

# Objective

The overall objective of this evaluation was to assess the SEC's OCIE TCP and determine whether the program provided effective oversight of entities' compliance with Regulation SCI. Specifically, we:

- reviewed the controls (including systems, policies, and procedures) in place for monitoring Regulation SCI compliance;
- evaluated the TCP examination process to determine (a) how risks are identified and entities are selected for examination, and (b) whether TCP examinations are performed and documented consistently and in accordance with established controls; and
- reviewed TCP's management and oversight of its CyberWatch program contractor.

To address our evaluation objectives, we (1) interviewed TCP, contracting, and Office of Information Technology personnel; (2) reviewed TCP policies and procedures; (3) assessed OCIE's FY 2016 and 2017 risk and control matrices (RCM) and management assurance statements; (4) reviewed TRACER development and system requirements, including investment proposals and supporting contracts; (5) reviewed CyberWatch contract files and COR files; (6) reviewed the services provided by the CyberWatch contractor; (7) surveyed 23 members of TCP staff; and (8) performed walkthroughs of the TRACER system and the CyberWatch program.

Our evaluation covered TCP activities and program management[8] from the inception of the program in OCIE in February 2014 through August 2018. It was not our objective nor did we compare ARP and TCP program management, or re-perform previous OIG work related to the ARP program.

Appendix I includes additional information about our objective, scope, and methodology, including our survey of TCP staff; our review of internal controls; and prior coverage.

[8] Office of Management and Budget Memorandum M-18-19, *Improving the Management of Federal Programs and Projects through Implementing the Program Management Improvement Accountability Act (PMIAA)*, is generally applicable to the 24 Federal agencies covered by the Chief Financial Officers Act of 1990 (31 U.S.C. § 901(b)), which does not include the SEC. However, for the purposes of this report, we used the definition of "program management" established in Memorandum M-18-19, which states that program management is "The coordinated application of general and specialized knowledge, skills, expertise, and practices to a program for effective implementation."

# Results

## Finding. Method for Overseeing Regulation SCI Compliance Effective; Opportunities to Improve Aspects of Program Management Remain

TCP has an established method to effectively oversee entity compliance with Regulation SCI. The CyberWatch contractor has comprehensive procedures that outline Regulation SCI compliance monitoring and noncompliance reporting, and in FY 2016 and FY 2017 TCP conducted various types of examinations of SCI entities based on several factors. However, we noted opportunities to improve some aspects of TCP program management. Specifically, we found that examination manuals in place at the outset of our evaluation were outdated, management had not identified or documented TCP risks and control activities in OCIE's RCM, and TRACER development was not well-planned or documented. As noted previously and discussed further below, TCP's Associate Director identified planned or ongoing initiatives at the outset of our evaluation that address some of these concerns and (as of the date of this report) had begun to implement changes.

**TCP Oversees Entity Compliance With Regulation SCI Through Its CyberWatch Program and Examination Efforts.** TCP oversees Regulation SCI compliance through the CyberWatch program and through TCP examinations. As further described below, CyberWatch is responsible for the intake and review of all required SCI forms and reports and serves as the point-of-contact for entities when they self-identify an SCI event. Additionally, TCP conducts various examinations of SCI entities to review their systems and verify Regulation SCI compliance.

*CyberWatch Program*. The CyberWatch program reviews required Regulation SCI filings and reports, including:

- Section 1002(b) SCI event notifications,
- Section 1003(a)(1) quarterly system change reports, and
- Section 1003(b)(3) SCI compliance annual review reports.

CyberWatch is composed of contracted staff led by a TCP Senior Specialized Examiner, who is supervised by an Assistant Director. The contractors follow pre-set, detailed guidance the SEC developed to assist the contractors with monitoring entities' compliance with Regulation SCI and reporting incidents of noncompliance. For example, the guidance details how contractors conduct intake for event submissions, create daily and ad-hoc reports, and submit information into the SEC's Tips, Complaints, and Referrals system pursuant to agency policies. According to the CyberWatch (b) (7)(E) , between November 2015

(when SCI entities were required to comply with Regulation SCI) and July 2018, CyberWatch received (b) (7)(E), (b) (8) .

Additionally, CyberWatch is primarily responsible for the management, execution, and oversight of the framework to triage, process, and analyze Regulation SCI events. According to Regulation SCI §242.1002, if an SCI entity has a reasonable basis to conclude that an SCI event occurred, the SCI entity is required to notify the SEC immediately. CyberWatch monitors SCI events through an active dashboard that provides event information by SCI entity.

We reviewed guidance on how CyberWatch functions during an SCI event and observed the CyberWatch team during a simulated SCI event. We noted that, once notified of an SCI event, CyberWatch contractors assume pre-established roles, activate a pre-established conference bridge, notify entity and appropriate SEC personnel, gather information, distribute event updates, and provide end-of-day and end-of-event reporting. According to the CyberWatch (b) (7)(E) , between November 2015 and July 2018, CyberWatch monitored (b) (7)(E), (b) (8) .

In addition to intake of required forms and monitoring of SCI events, CyberWatch provides Regulation SCI information to TCP examiners in the form of daily, monthly, quarterly, and annual reports. We administered a voluntary, anonymous survey to 23 members of TCP staff, excluding the Associate Director and his counsel. Although some survey respondents expressed the need for better communication or coordination with the CyberWatch staff, almost 74 percent of survey respondents[9] felt that the CyberWatch program and work products improved or assisted TCP's examination process.

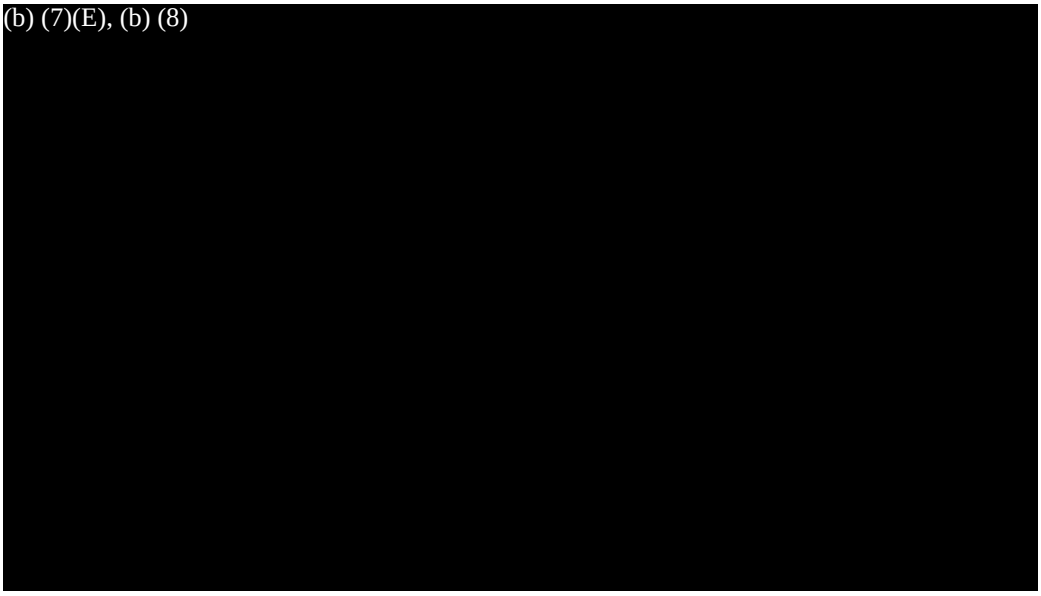
*TCP Examinations*. TCP examines SCI entities based on several factors, including identified examination priorities and risks (referred to as sweeps), prior TCP examinations, and changes over the prior 12 months. TCP also performs examinations when circumstances warrant immediate attention, such as responding to a major SCI event or addressing a referral received from the SEC's Tips, Complaints, and Referrals system. Finally, TCP examines some entities in accordance with Section 31 of the Securities Exchange Act of 1934 and Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act).

According to staff we interviewed, examinations can vary depending on their type. However, an examination generally includes identifying potential entity risks or issues, meeting with entity personnel, requesting relevant documents, assessing the information provided, and completing a letter to the entity on the results of the examination. If an examiner identifies any deficiencies during an examination, TCP will include those in a deficiency letter.

[9] This reflects 14 of the 19 survey respondents who answered this question.

TCP developed some tools to assist examination staff. For example, TCP developed an entity risk assessment tool to help TCP staff assess entities' risks in specific areas such as business continuity planning and disaster recovery, database security, data loss prevention, mobile device security, and information technology governance. In addition, TCP developed work programs that identify by subject area the appropriate standards (Regulation SCI and others) and suggested questions examiners should ask. As previously stated and as the following table shows, TCP performed 61 examinations in FY 2016 and 70 examinations in FY 2017 of the various types described above.

**Table. FY 2016 – 2017 TCP Examinations by Type**




Source: OIG-generated based on examination data provided by OCIE.

Based on the detailed CyberWatch procedures for the intake of required forms and monitoring of SCI events, TCP's examination tools, and the scope and type of TCP examinations performed, we concluded that the program has an established method to effectively oversee SCI entities and their compliance with Regulation SCI. We also noted that 94 percent of the respondents to our survey of TCP staff[10] believed that TCP provides effective oversight of entity compliance with Regulation SCI. However, we identified opportunities to improve some aspects of TCP program management as further described below.

**Examination Manuals Were Outdated.** At the outset of our evaluation, the TCP Examination Manual and draft TRACER Examination User Manual were outdated and neither fully aligned with TCP examination practices. For example, the TCP Examination Manual in effect when we began our evaluation did not refer to TRACER (TCP's system of record) or instruct examiners to use TRACER when performing TCP examinations. Furthermore, the TRACER Examination User Manual referred to

[10] This reflects 17 of the 18 survey respondents who answered this question.

CyberWatch functions not performed in TRACER. We discussed the TCP Examination Manual and draft TRACER Examination User Manual with TCP management who concurred that the manuals were out-of-date. During our evaluation, TCP management provided us a new TCP Examination Manual that became effective June 25, 2018. TCP did not finalize or update the draft TRACER Examination Manual because, on May 4, 2018, TCP management decided to discontinue developing TRACER and began transitioning the TCP examination program to TRENDS—the examination system used by all other OCIE examination programs. According to OCIE management, the transition to TRENDS will further align TCP with OCIE's examination program and will also allow TCP staff to store documents in the same place as other OCIE programs. According to TCP management, once the transition to TRENDS is complete, TCP will transition to the NEP Manual and plans to phase out the separate TCP Examination Manual.

GAO's *Standards for Internal Control in the Federal Government*[11] state that management should, among other things: (1) identify, analyze, and respond to risks related to achieving defined objectives; (2) design control activities to achieve objectives and respond to risks; and (3) document in policies the internal control responsibilities of the organization. Further, SEC Administrative Regulation 30-01, *Internal Control Program* (September 20, 2017) (SECR 30-01), states that SEC management is responsible for designing, implementing, and maintaining internal control to achieve the agency's strategic, operating, reporting, and compliance objectives. Programs can respond to objective risks and maintain internal control by developing policies and procedures—such as manuals—for staff to follow when conducting their work.

Since TCP's inception, key aspects of the program have changed, which may have contributed to the program's outdated manuals. For example, in February 2014 ARP moved from TM to OCIE. Later that year, the SEC adopted Regulation SCI, and TCP became responsible for Regulation SCI oversight. Also, between 2014 and 2018, TCP was under the direction of four different senior officers, including the current Associate Director. Finally, changes in TRACER's purpose and functions, as further described below, may have affected the TCP Examination Manual and draft TRACER Examination User Manual. For example, TRACER was originally intended to intake filings and monitor SCI entity system outages and changes; but the system evolved into the system of record for TCP examinations.

Without current guidance, staff may not consistently conduct and/or document their work. We planned to test TCP staff compliance with four of the TCP Examination

[11] U.S. Government Accountability Office, *Standards for Internal Controls in the Federal Government* (GAO-14-704G, September 2014).

Manual's examination procedures;[12] however, TCP management stated that the procedures were either no longer applicable to TCP's processes or were not followed consistently. For example, management stated that examiners often stored documents in either TRACER or an SEC enterprise network application, and at least one of the four procedures we intended to test was considered optional guidance. Although 61 percent of the staff who responded to our survey[13] believed TCP conducted, managed, and/or documented examinations in a consistent manner, many respondents provided suggestions on how TCP can improve program consistency. For example, respondents felt that having two document storage systems was redundant and confusing, and that examination work practices differed between examination teams. As a result of outdated manuals and inconsistent practices, we did not test TCP staff compliance with the program's examination procedures.

**Management Did Not Clearly Identify or Document TCP Risks and Control Activities in OCIE's RCM.** TCP management did not clearly identify or document TCP's risks or corresponding internal controls in OCIE's FY 2016 and FY 2017 RCMs. Although TCP examinations appear to have similar risks as other OCIE examinations, OCIE's RCMs did not identify comparable documented control activities specific to TCP examination processes for all identified risks.

Internal controls, among other things, promote efficiency, reduce risk, and promote compliance with laws and regulations. As previously stated, GAO's *Standards for Internal Control in the Federal Government* and SECR 30-01 emphasize, among other things, management's responsibility for addressing risks and designing, implementing, and maintaining control activities. In addition, according to the SEC's Office of Financial Management Reference Guide, internal controls are in place to provide reasonable assurance that an organization achieves its objectives through (1) effective and efficient operations, (2) reliable reporting, and (3) compliance with laws and regulations. SEC management annually assesses and documents the organization's risks and related internal control activities in division or office RCMs.

During its FY2016 assessment of internal supervisory controls, as required by Section 961 of the Dodd-Frank Act, OCIE's Office of Strategy and Operational Risk, which annually reviews OCIE's RCM, worked with TCP staff to better clarify and improve OCIE's assessments of its internal supervisory controls.[14] Staff from the Office of Strategy and Operational Risk reviewed TCP's Examination Manual and spoke with TCP staff to create a crosswalk between existing OCIE RCM control activities (control

[12] The procedures related to entity risk assessments, completion of examination work programs and deficiency sheets, issuance of examination reports and deficiency letters, and tracking of recommendations.

[13] This reflects 11 of the 18 survey respondents who answered this question.

[14] According to GAO, its 2016 triennial report on the effectiveness of the SEC's supervisory controls did not include an assessment of TCP examinations, in part, because OCIE's RCMs used in that assessment did not include TCP-specific control activities identified as Dodd-Frank Act internal supervisory controls.

activities specific to TRENDS and the NEP Manual) and similar TCP control activities in an effort to identify and test TCP controls. The crosswalk resulted in a new TCP-specific control activity encompassing three significant controls included in OCIE's FY 2017 RCM. Although the Office of Strategy and Operational Risk was able to develop a new control activity for TCP examinations, TCP management should be more proactive in its review, identification, and documentation of program risks and mitigating control activities.

**TCP's Development of TRACER Was Not Well-Planned or Documented.** Development of the TRACER system began in TM and continued, under TCP's direction, between September 2015 and January 2018. During this time, TCP—as the system's new business owner—oversaw frequent, sometimes weekly, system updates. TCP's continued development of TRACER, however, was not well-planned or documented. As described below, TRACER's purpose and functions evolved and it is unclear, based on a lack of documentation, how TCP assessed or managed the system's development, including system requirements.

TCP's initial TRACER investment proposal identified Regulation SCI compliance, including the intake and review of required SCI forms and reports from SCI entities, as the system's purpose. However, OCIE awarded CyberWatch contracts to manage the intake and review of Regulation SCI filings without TRACER being fully developed, and CyberWatch contractors have not used the TRACER system to monitor SCI entities' compliance. OCIE management explained that staffing positions designated for Regulation SCI compliance were not transferred from TM to OCIE when ARP transitioned from TM. Therefore, according to OCIE management, TCP was required to ramp up quickly with contractors who manage the intake and review of Regulation SCI filings using their own system. As TRACER was not used to manage the intake and review of Regulation SCI filings, it evolved into a TCP examination system.

Plans to migrate or link other systems and data to TRACER and build in certain functions and capabilities also evolved over time with varying degrees of success. For example, TCP planned, but did not complete, migration of certain CyberWatch data to TRACER. Also, with significant effort, TCP was able to migrate to TRACER historical data from a retired SEC database, referred to as Consolidated New Database and Operational Reports, but later removed the data after determining that the data did not integrate well with the TRACER system and was not necessary. The system was also to include questionnaires for TCP staff to use during examinations and a risk assessment function to plan upcoming examinations; however, these and other planned system capabilities were not realized.[15] Moreover, after TCP began developing TRACER, TCP management determined that the system had limited data storage capabilities. This required TCP personnel to retain most examination

[15] Although certain planned capabilities were not built in the TRACER system, TCP established processes outside of TRACER.

documents in an SEC enterprise network application while incrementally uploading documents into TRACER as system updates occurred.

In addition, TCP could not demonstrate system plans or the rationale for critical decisions involving the development of TRACER, in part, because of a lack of documentation maintained by TCP and OCIE Office of Technology Services personnel. Aside from the investment proposal, personnel could not provide us with:

- documentation of the alternatives analysis performed supporting the decision to continue developing TRACER, rather than use OCIE's existing TRENDS system as a repository for TCP examination documents;[16] or

- established business plans or requirements documents that illustrated TCP management was aware of development challenges and system needs.

According to OCIE management, OCIE and TCP relied on the SEC's Office of Information Technology for system development efforts, and followed the agency's prescribed capital planning and investment control process.

GAO's *Standards for Internal Control in the Federal Government* states that management should design an entity's information system and related control activities to achieve objectives and respond to risks, and consider the defined information requirements for each of the entity's operational processes. SEC guidance[17] also prescribes policies, requirements, and responsibilities for the SEC's capital planning and investment control process, including the following:

- Reassessing business cases in light of changing requirements and improved knowledge of costs and risks.

- Assigning responsibilities for developing business requirements and for preparing business cases for information technology investments. Specifically, the business sponsor is responsible for guiding the investment from initial approval through successful implementation, and the business lead is responsible for the constructive and timely participation of the right personnel with the knowledge to ensure the project's approved scope meets applicable business needs.

- Structuring the process so that the SEC can, among other things, prevent redundancy of existing or shared information technology capabilities.

[16] According to TRACER's investment proposal, the amount of custom coding required for TCP to use TRENDS would cost more than building TRACER. However, agency personnel could not provide us with analysis supporting this statement.

[17] SEC Administrative Regulation 24-02, Rev. 2.1, *Information Technology Capital Planning and Investment Control* (CPIC) (May 2017).

Between September 2015 and January 2018, TCP spent nearly $780,000[18] developing TRACER. In January 2018, TCP's Associate Director halted any additional funding for TRACER development while he and other OCIE senior management assessed whether it would be more beneficial for TCP to move to TRENDS or continue to develop TRACER. TCP's Associate Director met with OCIE's Business Management Office and Office of Technology Services on February 28, 2018, to discuss options and costs. According to the Associate Director, management sought to determine what TRACER system updates TCP still needed, the cost of those updates, and what other options might be, including moving to TRENDS. On May 4, 2018, TCP management decided to discontinue developing the TRACER system and transition its examination program to TRENDS. OCIE's analysis noted that maintaining two systems of record required duplicative efforts and added costs and that there would be several benefits of transitioning TCP to TRENDS, including greater consistency in the application of NEP controls and seamless integration with reporting applications. In July 2018, OCIE's Office of Technology Services estimated that it would cost about $359,800 to transition TCP to TRENDS, which would result in savings related to system development and maintenance. According to TCP management, TCP will continue to use TRACER until the transition to TRENDS is complete, which is scheduled for late 2018.

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

To address the issues we observed, we recommend that the Director of the Office of Compliance Inspections and Examinations:

**Recommendation 1:** Ensure Technology Controls Program management updates the Technology Controls Program Examination Manual in a timely manner following the transition to the Tracking and Reporting Examination National Documentation System.

> **Management's Response.** Management concurred with the recommendation. Once the Technology Controls Program transitions to the Tracking and Reporting Examination National Documentation System as its examination workflow and tracking tool, the Office of Compliance Inspections and Examinations will update and incorporate Technology Controls Program changes to its existing National Examination Program Examination Manual and the Office of Compliance Inspections and Examinations will retire the Technology Controls Program Examination Manual. Management's complete response is reprinted in Appendix II.

[18] Through its system development contract, TRACER phase 2 began on September 17, 2015, and incurred costs of $339,840. TRACER phase 3 began on September 19, 2016, and incurred costs of $439,200. These costs do not include costs associated with SEC personnel who worked on TRACER development or initial TRACER development completed under the direction of TM.

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

**Recommendation 2:** Identify and document the risks and controls related to Technology Controls Program operations, and update the Office of Compliance Inspections and Examinations' risk and control matrix accordingly.

**Management's Response.** Management concurred with the recommendation. In addition to the existing controls in the fiscal year 2018 risk and control matrix, which the Office of Compliance Inspections and Examinations assesses and updates annually, Technology Controls Program management will reassess risks and controls in future Office of Compliance Inspections and Examinations risk and controls matrices as it moves to the Tracking and Reporting Examination National Documentation System. Management's complete response is reprinted in Appendix II.

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

**Recommendation 3:** Ensure Technology Controls Program management properly plans and documents the transition to the Tracking and Reporting Examination National Documentation System, and retains in a central location all relevant materials, including contracts, system requirements, and plans.

**Management's Response.** Management concurred with the recommendation. Office of Compliance Inspections and Examinations management will work with the U.S. Securities and Exchange Commission's Office of Information Technology to retain this information. Management's complete response is reprinted in Appendix II.

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

# Other Matters of Interest

During our evaluation, other matters of interest that did not warrant recommendations came to our attention. We discussed these matters with agency management for their consideration.

**TCP Training.** At the outset of our evaluation, TCP's Associate Director explained the need for enhanced training for TCP staff and that efforts were underway to establish baseline training and identify any skills gaps. In July 2018, TCP's Associate Director stated that a three-year training plan (dependent on budgetary limitations) was completed.

About 53 percent of the staff who responded to our survey[19] indicated that they either did not receive adequate training (16 percent) or only sometimes received adequate training (37 percent). For example, some respondents noted that training was compressed into short presentations with little time for discussion and that there is a need for specialized information technology training to stay aware of new developments and trends. We encourage TCP management to continue to review TCP staff training and ensure staff have the knowledge and skills necessary to perform TCP examinations of SCI entities.

**OA's File Review Process and eFile Checklist.** SEC Operating Procedure 10-15, *Contracting Officer's Representative* (March 30, 2018), states that CORs must upload all documents to eFile—the SEC's electronic contracting filing system—including documents related to inspection and acceptance of contract deliverables, contractor non-disclosure agreements, and correspondence concerning contractor performance. We reviewed the CyberWatch blanket purchase agreement call and, among other things, assessed how TCP's COR performed required duties. Although we were able to obtain from other sources certain documents, including deliverable inspection and acceptance documents, the CyberWatch contractor's non-disclosure agreements, and contractor communication, we did not find these documents in eFile. The responsible contract specialist reviewed eFile entries for the CyberWatch contract in February 2018 and documented similar exceptions on a checklist used for such reviews.

We discussed our observations with Office of Acquisitions (OA) personnel who stated that the eFile checklist is an optional tool that contracting personnel can use to review COR files and to promote conversation with the COR. OA personnel indicated that the completed checklist (with any deficiencies noted) should be provided to the COR, but for the CyberWatch blanket purchase agreement call, was not provided to the correct

[19] This reflects 10 of the 19 survey respondents who answered this question.

COR because of an administrative error.[20] Furthermore, according to OA personnel, contracting officers are not required to follow up or verify that the COR addressed the exceptions noted on the checklist.

OA's proactive review of contractor files using a checklist is a positive step toward ensuring CORs upload all required documents to the official contracting files. However, we suggest that OA consider establishing follow-up procedures to ensure CORs correct any deficiencies identified.

[20] OA personnel stated that they provided the completed CyberWatch eFile checklist to the base blanket purchase agreement COR instead of the call-level (CyberWatch) COR. After our discussion, the call-level COR received the checklist.

# Appendix I. Scope and Methodology

We conducted this evaluation from December 2017 through September 2018 in accordance with the Council of the Inspectors General on Integrity and Efficiency *Quality Standards for Inspection and Evaluation (2012).* Those standards require that we plan and perform the evaluation to obtain evidence sufficient to provide a reasonable basis for our findings and recommendations. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objectives.

**Scope and Objective.** The evaluation covered TCP activities and program management from the inception of the program in OCIE in February 2014 through September 2018. The overall objective was to assess the SEC's OCIE TCP and determine whether the program provided effective oversight of entities' compliance with Regulation SCI. Specifically, we sought to:

- review the controls (including systems, policies, and procedures) in place for monitoring Regulation SCI compliance;
- evaluate the TCP examination process to determine (a) how risks are identified and entities are selected for inspection, and (b) if TCP examinations are performed and documented consistently and in accordance with established controls; and
- review TCP's management and oversight of its CyberWatch program contractor.

We conducted fieldwork at the SEC's headquarters in Washington, DC, and we interviewed TCP staff in Chicago and New York via telephone.

**Methodology.** To assess OCIE's TCP and determine whether it provided effective oversight, we reviewed:

- Federal laws relevant to the SEC's authority to conduct inspections and examinations, including the Securities and Exchange Act of 1934[21] and the Dodd-Frank Act;[22]
- regulations that apply to TCP, specifically Regulation SCI;[23]

[21] Pub. L. No. 73-291(codified as amended at 15 U.S.C. §§ 78a-78qq).

[22] Pub. L. No. 111-203 (codified as amended at 12 U.S.C. §§ 5301-5641).

[23] 17 C.F.R. §§ 240, 242, and 249.

- OCIE and TCP policies and procedures, including guidance and forms used to complete examinations and manage the CyberWatch function;

- information technology systems and applications used by TCP, including Archer, TRACER, the Threat Analysis Tool, and other subscription services available to TCP staff;

- guidance and decisions related to TRACER, including the TRACER policy manual, release notes, privacy analysis worksheets, and plans for TCP's transition from TRACER to TRENDS; and

- SEC administrative regulations pertaining to contract management, oversight, CORs, and internal controls.

We also interviewed TCP managers and staff to understand how TCP conducts inspections under Regulation SCI, and to evaluate the controls in place for monitoring Regulation SCI compliance. Specifically, we met with TCP's Associate Director, Assistant Directors, Branch Chiefs, and examination staff, and we interviewed TCP's COR who oversees the CyberWatch program. We conducted a walkthrough of the CyberWatch program to understand how the contractor assists TCP in maintaining effective oversight of entities' compliance with Regulation SCI. This included obtaining copies of certain contractor deliverables such as monthly, quarterly, and annual reports that summarized the contractor's work and findings on SCI entities.

To understand the services to be provided by the CyberWatch contractor, deliverables and due dates, key personnel, and other requirements, we reviewed the blanket purchase agreement and executed call order for CyberWatch support services, including the COR's and contracting officer's files. We interviewed the contracting officer and other members of OA management to understand the SEC's eFile requirements and the voluntary checklist discussed in the Other Matters section of this report.

We interviewed staff from OCIE's Office of Technology Services and the SEC's Office of Information Technology to understand how TCP chose TRACER as its system of record and determined to transition to TRENDS. We also interviewed staff from OCIE's Office of Strategy and Operational Risk to understand if and how they conduct annual reviews of OCIE's internal controls, including internal controls for TCP.

Finally, between May 2018 and June 2018, we administered a voluntary, anonymous survey to 23 members of TCP staff, excluding the Associate Director and his counsel. The survey included eight open- and close-ended questions that asked staff their opinions on, among other things, training, consistency in TCP's exam process, suggestions for improvements/changes to the TCP system of record, usefulness of the CyberWatch program, and TCP's effectiveness in overseeing entities' compliance with Regulation SCI. We received 19 responses (an overall response rate of about 83 percent). We analyzed the survey results, which we included as part of our overall

analysis of TCP's oversight of Regulation SCI. We also provided a summarized and sanitized version of the survey results to TCP management for their consideration.

**Internal Controls.** To assess internal controls relative to our objectives, we reviewed the SEC's management assurance statements and RCMs covering OCIE for FYs 2016 and 2017. As noted in this report, even though TCP examinations appear to have similar risks and internal controls as other OCIE examinations, the FY 2016 OCIE RCM we reviewed did not identify or document comparable control activities specific to TCP examinations. Staff from the Office of Strategy and Operational Risk, not TCP management, created a new TCP-specific control activity encompassing three significant controls included in OCIE's FY 2017 RCM. Further, we reviewed TCP's written examination manuals and, as discussed in this report, found TCP's Examination Manual and system user manual in effect at the outset of our evaluation to be outdated and not reflective of current practices. Our recommendations, if implemented, should correct the weaknesses we identified.

**Computer-processed Data**. We did not rely significantly on computer-processed data to address our objectives. Therefore, we did not test system controls or the reliability of any computer-processed data.

**Prior Coverage**. Between 2016 and 2017, the SEC OIG and GAO issued the following reports of particular relevance to this evaluation:

SEC OIG:

- *Audit of the Office of Compliance Inspections and Examinations' Investment Adviser Examination Completion Process* (Audit Report No. 541; July 21, 2017).

GAO:

- *Management Has Enhanced Supervisory Controls and Could Further Improve Efficiency* (GAO-17-16, October 2016).

These reports can be accessed at: https://www.sec.gov/oig (SEC OIG) and https://www.gao.gov (GAO).

# Appendix II. Management Comments

**MEMORANDUM**

TO: Rebecca L. Sharek
Deputy Inspector General for Audits, Evaluations, and Special Projects
Office of the Inspector General

FROM: Pete Driscoll
Director, Office of Compliance Inspections and Examinations

RE: Office of Compliance Inspections and Examination's Response to the Office of Inspector General's Report, *TCP Established Method to Effectively Oversee Entity Compliance with Regulation SCI but Could Improve Aspects of Program Management*

DATE: September 20, 2018

The Office of Compliance Inspections and Examinations ("OCIE") submits this memorandum in response to the Office of Inspector General's ("OIG") draft report titled *TCP Established Method to Effectively Oversee Entity Compliance with Regulation SCI but Could Improve Aspects of Program Management* ("Report").

Over the last four years, OCIE has transformed the Technology Controls Program ("TCP") from a voluntary program under the Division of Trading and Markets to a full-fledged examination program responsible for overseeing technology compliance at some of the most critical market participants. OCIE appreciates the OIG's finding that TCP provides effective oversight of entity compliance with Regulation SCI. OCIE also appreciates the OIG's acknowledgement of the comprehensiveness of its CyberWatch program.

As noted in the Report, current TCP management identified areas of improvement and began initiating significant changes prior to the audit which were, in some cases, completed during the audit, including (1) adopting a new TCP Examination Manual, (2) transitioning the tracking of all TCP examinations to OCIE's Tracking and Reporting and Examinations National Documentation System ("TRENDS")[1] at which point TCP will adopt the National Examination Program Examination Manual, which is used by all other OCIE programs, (3) implementing a three-year training plan for TCP staff, and (4) completing a process to make TCP staff available for consultation and analysis to other OCIE and SEC staff.

OCIE welcomes the OIG's recommendations to improve certain aspects of TCP internal processes. Our response to the recommendations is below.

[1] TRENDS is currently the workflow tracking and reporting system for all OCIE examination programs, except TCP. Since its inception in 2012, the U.S. Government Accountability Office and the OIG have audited TRENDS. See, e.g., U.S. Government Accountability Office, *Management Has Enhanced Supervisory Controls and Could Further Improve Efficiency,* (GAO-17-16, October 2016) and SEC OIG, *Audit of the Office of Compliance Inspections and Examination's Investment Adviser Examination Completion Process*, (Audit Report No. 541, July 21, 2017).

***Recommendation 1:*** *Ensure Technology Controls Program management updates the Technology Controls Program Examination Manual in a timely manner following the transition to the Tracking and Reporting Examination National Documentation System.*

OCIE concurs with this recommendation. Once TCP transitions to TRENDS as its examination workflow and tracking tool, OCIE will update and incorporate TCP changes to its existing NEP Examination Manual and OCIE will retire the TCP Examination Manual.

***Recommendation 2:*** *Identify and document the risks and controls related to Technology Controls Program operations, and update the Office of Compliance Inspections and Examination's risk and control matrix accordingly.*

OCIE concurs with this recommendation. In addition to the existing controls in the fiscal year 2018 risk and control matrix (RCM), which OCIE assesses and updates annually, TCP management will reassess risks and controls in future OCIE RCMs as it moves to TRENDS.

***Recommendation 3:*** *Ensure Technology Controls Program management properly plans and documents the transition to the Tracking and Reporting Examination National Documentation System, and retains in a central location all relevant materials, including contracts, system requirements, and plans.*

OCIE concurs with this recommendation. OCIE management will work with the SEC's Office of Information Technology to retain this information.

We appreciate the opportunity to review and comment on the Report. Please contact Keith Cassidy, Associate Director and head of the TCP Program, if you have any questions.

## Major Contributors to the Report

Carrie Fleming, Audit Manager

John Gauthier, Lead Auditor

Suzanne Heimbach, Auditor

Leann Harrier, Assistant Counsel

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

Web: https://www.sec.gov/oig

Telephone: (833) SEC-OIG1 (833-732-6441)

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.