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

OFFICE OF
INSPECTOR GENERAL

May 31, 2017

TO: Stephanie Avakian, Acting Director, Division of Enforcement, and Chair, TCR Oversight Board

Scott Bauguess, Acting Director and Chief Economist, Division of Economic and Risk Analysis

Kenneth Johnson, Acting Chief Operating Officer

FROM: Carl W. Hoecker, Inspector General

SUBJECT: *Final Management Letter: Progress on the SEC's Tips, Complaints, and Referrals Intake and Resolution System Redesign and Vulnerability Remediation Efforts*

In May 2015, the U.S. Securities and Exchange Commission (SEC or agency) Office of Inspector General (OIG) reported observations about the SEC's Tips, Complaints, and Referrals Intake and Resolution System (TCR system) and the agency's project to redesign the system.[1] Since that time, we have continued to monitor the SEC's progress toward implementing a redesigned TCR system and addressing information security vulnerabilities in the current system. We have not conducted an audit in conformance with generally accepted government auditing standards. However, based on the work performed, we are reporting additional observations that warrant management's attention.[2] We are also requesting that the SEC provide information about its (1) actions to stabilize its Oracle (b) (7)(E) platform[3] and establish consistent Oracle environments, (2) actions to finalize the redesigned TCR system requirements, (3) plans for addressing unresolved information security vulnerabilities in the current TCR system while it continues to operate, and (4) plans for reviewing the planning and management of the SEC's project to redesign the TCR system to identify lessons learned.

Executive Summary

We previously reported that, due to various factors, the project to redesign the SEC's TCR system experienced cost increases and schedule delays. As stated in our May 20, 2015,

[1] U.S. Securities and Exchange Commission, Office of Inspector General, *Final Management Letter: Observations Noted During TCR System Audit Support Engagement*; May 20, 2015.

[2] The full version of this management letter includes non-public information about the SEC's information security program and therefore could not be publicly released. To create this public version, the OIG redacted (deleted) the non-public information and indicated where those redactions were made.

[3] The SEC uses Oracle (b) (7)(E) to run certain applications and systems, and plans to deploy the redesigned TCR system on the platform.

management letter, the value of the SEC's contract for developing the redesigned TCR system had increased by nearly $4 million, and the project was at least 10 months behind schedule. In addition, final user acceptance and system implementation dates were not established, and the current TCR system continued to operate with unresolved information security vulnerabilities (that is, Plan of Action and Milestones [POA&M] items). In response to our May 20, 2015, management letter, the SEC reported that the redesigned TCR system, initially scheduled to go live July 21, 2014, would go live August 24, 2015.

As of the date of this management letter, the SEC has successfully tested and conditionally accepted the redesigned TCR system. However, the agency has not implemented the system, as the system's multiple users are considering new requirements and enhancements not previously required in the development effort. Therefore, the SEC does not expect the redesigned TCR system to go-live until October 2, 2017 (more than 3 years behind schedule). Moreover, the value of the SEC's contract to implement the system has increased by another $8.5 million, for an overall increase of about $12.2 million, or 170 percent. To date, the SEC has obligated about $16.6 million and expended about $14.4 million of the total contract value, or twice the amount initially planned. The contract cost will likely continue to rise as the agency continues to pursue new system requirements and enhancements.

In addition to establishing new system requirements, the most recent delays in accepting and implementing the redesigned TCR system were due, in part, to instability in the SEC's Oracle (b) (7)(E) platform caused by a lack of effective governance in the Office of Information Technology's (OIT) configuration management process.[4] The instability in the SEC's Oracle platform may have also impacted the agency's ability to test and deploy at least two other systems.

At the same time, the SEC has continued to operate the current TCR system but has not timely remediated some of the system's security vulnerabilities. For example, at least two of the system's POA&M items remained open for more than 2,000 days (or about 6 years) as the SEC anticipated implementing the redesigned TCR system. According to system security documents, these vulnerabilities increased the likelihood that suspicious activities would go undetected and reduced the trustworthiness of information. In March 2017, OIT closed one of these two items (which OIT considered low risk[5]), and downgraded the other item from moderate risk to low risk (OIT previously considered the item high risk). Two other POA&M items, identified in December 2016, also remain open and are considered low risk.

The SEC should (1) ensure that OIT adequately addresses known issues with the Oracle (b) (7)(E) platform and environment, (2) finalize its requirements for the redesigned TCR system, and (3) remediate information security vulnerabilities in the current TCR system

[4] Configuration management is the process by which changes to an information technology environment are documented, tested, and managed.

[5] The National Institute of Standards and Technology, Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, defines the following three levels of potential impact should there be a loss of information or information system confidentiality, integrity, or availability: (1) a severe or catastrophic adverse effect (high), (2) a serious adverse effect (moderate), or (3) a limited adverse effect (low).

while it continues to operate. In addition, the SEC should conduct a comprehensive review of its planning and management of the project to redesign the TCR system to identify lessons learned. Doing so should improve the agency's efforts to develop and modernize its information technology systems and to manage other information technology acquisitions.

Background

The SEC encourages the public to file complaints or submit tips of possible securities law violations, broker or firm misconduct, or unfair practices in the securities industry that pose a risk of harm to investors (collectively referred to as tips, complaints, and referrals [TCRs]). According to the SEC, it receives, on average, 15,000 TCRs every year from multiple sources in a variety of ways. These include TCRs from, among others, the public, attorneys, and members of the regulated community, including broker-dealers, investment advisers, self-regulatory organizations, and public companies.

In 2009, the SEC reviewed the sources of TCRs and the decentralized nature of its processes for receiving, recording, tracking, and acting on them. Based on this review, the agency determined that it needed a centralized system for TCR intake, triage, and resolution. In March 2011, the SEC deployed the current TCR system. The SEC's Division of Economic and Risk Analysis (DERA) is the system's business owner, whereas the SEC's OIT is the system owner.[6] The TCR Oversight Board—a decision-making body composed of senior officials—meets regularly and provides high-level strategic direction and governance to SEC management, and monitors and manages the agency's TCR program.[7]

Although the current TCR system is operational, SEC stakeholders determined that a more robust, flexible, and scalable system was needed to better support the agency's needs, mission, and policies as they evolve. In September 2013, the SEC awarded to Guident Technologies, Inc. (Guident)[8] a contract to elicit requirements, design, and deploy a redesigned TCR system.

On May 20, 2015, we reported that, due to various factors,[9] the project to implement the redesigned TCR system was at least 10 months behind schedule and the value of the SEC's contract with Guident had increased by nearly $4 million (from about $7.2 million to about

[6] The business owner serves as a steward, with the information system owner, in ensuring the confidentiality, integrity, and availability of an information system. The information system owner (or system owner) is responsible for the overall procurement, development, integration, modification, operation, and maintenance of an information system.

[7] Since June 2016, the TCR Oversight Board has been chaired by the Acting Director of the Division of Enforcement and includes a senior representative from each of the following SEC divisions and offices: (1) the Division of Corporation Finance, (2) DERA, (3) the Division of Enforcement, (4) the Division of Investment Management, (5) the Division of Trading and Markets, (6) the Office of the Chief Operating Officer, (7) the Office of Compliance Inspections and Examinations, (8) OIT, and (9) the Office of Investor Education and Advocacy. There is also one member representing the SEC's regional offices.

[8] Guident is a wholly owned subsidiary of Salient CRGT.

[9] These factors included unacceptable contractor performance and a lack of adequate contractor and government resources to timely address concerns.

$11 million). We also reported that final user acceptance and system implementation dates were not established, and the current TCR system continued to operate with unresolved information security vulnerabilities. As a result, we requested that management provide:

1. current dates for user acceptance, quality control testing, and implementation of the redesigned TCR system;

2. its plans to address the current TCR system's information security vulnerabilities (that is, open POA&M items and penetration testing results); and

3. a description of the actions the SEC would take to remediate the known information security vulnerabilities in the event the agency did not implement the redesigned system as planned.

In its May 27, 2015, response, management provided highlights from its draft project plan and stated that the redesigned TCR system, initially scheduled to go live July 21, 2014, would go live August 24, 2015. In addition, management stated that the redesigned TCR system is not based on the current TCR system or code. Therefore, the redesigned system will not inherit the current system's information security vulnerabilities. However, management stated that it would review all open POA&M items for the current TCR system and ensure the current system operated at an acceptable risk level if the redesigned TCR system was not implemented by August 24, 2015.

Between May 2015 and May 2017, we continued to monitor the SEC's progress toward implementing a redesigned TCR system and addressing information security vulnerabilities in the current system. In February 2017, we interviewed personnel from the SEC's Office of Acquisitions, OIT, and DERA, and the Chair of the TCR Oversight Board. We also reviewed documents supporting contract actions executed since May 2015, and the results of system security assessments. Although the work performed did not constitute an audit in conformance with generally accepted government auditing standards, the observations noted warrant management's attention and response.

Results

The TCR System Redesign Project Has Continued To Experience Difficulties and Delays. Since our May 20, 2015, management letter, the TCR system redesign project—one of the SEC's multi-year, mission-critical technology projects—has continued to experience difficulties and delays, resulting in additional cost increases. The SEC performed user acceptance testing of the redesigned system seven times between July 2014 and March 2017 and repeatedly identified deficiencies either with the system's code or, more recently, with the SEC's information technology environment (that is, the Oracle (b) (7)(E) platform on which certain SEC applications and systems operate). Furthermore, according to OIT and DERA personnel, new requirements and service requests, in part, delayed testing and acceptance of the redesigned TCR system.

For example, during the August 2016 user acceptance tests, users identified instability and performance issues including slow performance, unresponsive pages, and server issues. In addition, OIT (b) (7)(E)

[redacted]. Instability in the Oracle (b) (7)(E) platform was caused, in part, by a lack of effective governance in OIT's configuration management processes. Moreover, the platform's instability further delayed the SEC's ability to test and accept the redesigned TCR system, and potentially impacted the agency's ability to test and deploy at least two other systems.[10]

The Oracle (b) (7)(E) platform is the software platform used by at least five SEC systems currently in production.[11] The redesigned TCR system and two other systems that are undergoing or awaiting testing will also use the Oracle platform. Proper configuration change control ensures that changes to existing information technology systems or newly developed systems are tested and validated in a secure pre-production (or staging) environment before those changes are released to the production environment. According to the SEC's Chief Information Officer, during the August 2016 user acceptance testing for the redesigned TCR system, OIT determined that there were inconsistent configurations in the SEC's Oracle staging and production environments. The inconsistencies between these environments made it difficult to determine whether issues identified during user acceptance testing resulted from deficiencies in the redesigned TCR system's code or from the environment itself. As a workaround, in October 2016, OIT assessed and accepted the risk of isolating the redesigned TCR system in a firewalled portion of the SEC's more stable Oracle production environment, allowing system tests to proceed.

In November 2016, user acceptance testing of the redesigned TCR system resumed. During testing, users identified issues with the system's search function, and seven Oracle-related defects that OIT considered critically necessary to fix before implementing the redesigned TCR system. Since then, Guident has resolved the search function issue, and OIT has addressed the Oracle defects.

In March 2017, DERA, with OIT's assistance, conducted another round of user acceptance testing of the redesigned TCR system. According to DERA and OIT personnel, the testing was successful but identified several new defects. In addition, the system's multiple users are considering new, unanticipated requirements and enhancements that will make the system more efficient when it is finally implemented. As of the date of this management letter, the SEC has conditionally accepted the system and is working with Guident to remediate the defects and address the agency's newest requirements, including "general usability issues." Therefore, the SEC does not expect the redesigned TCR system to go-live until October 2, 2017, which is more than 3 years behind schedule.

As we previously reported, between September 2013 and May 2015, the SEC added about $4 million to its contract with Guident to develop and implement the redesigned TCR system.

[10] These two systems are the: (b) (7)(E) [redacted]

[11] These five systems are the: (b) (7)(E) [redacted]

(The contract value increased from about $7.2 million to about $11 million during that period.) Since our May 20, 2015, management letter, the SEC has issued 14 additional contract modifications to extend the period of performance, provide testing support, and add even more funding. As a result, the SEC increased Guident's contract value by another $8.5 million (from about $11 million in May 2015 to about $19.5 million to date), for an overall increase in contract value of about $12.2 million, or 170 percent. To date, the SEC has obligated about $16.6 million and expended about $14.4 million of the total contract value, or twice the amount initially planned. The contract cost will likely continue to rise as the agency continues to pursue new system requirements and enhancements.

The SEC Has Continued To Operate the Current TCR System But Has Not Timely Remediated Some Information Security Vulnerabilities. As we previously reported, delays in implementing the redesigned TCR system are important because the SEC has continued to operate the current TCR system but has not timely remediated some of the system's information security vulnerabilities. In the agency's response to our May 20, 2015, management letter, management stated that the SEC would review all open POA&M items for the current TCR system and address those that posed the highest level of operational risk. In December 2016, as part of its normal certification and accreditation cycle, OIT assessed the security of the current TCR system and identified seven new vulnerabilities (one moderate risk and six low risk). Although OIT has taken steps to address many of the prior and newly issued POA&M items, the SEC allowed the following two POA&M items to remain open for more than 2,000 days (or about 6 years) as the agency anticipated implementing the redesigned TCR system:

- (b) (7)(E) According to POA&M documents, (b) (7)(E) The vulnerability was identified as early as December 2010 (b) (7)(E) in December 2011 in anticipation of the redesigned TCR system going live. Finally, on March 16, 2017, OIT (b) (7)(E) and closed the vulnerability.
- (b) (7)(E) The current TCR system's (b) (7)(E) As we reported in May 2015, this vulnerability was identified as early as December 2010. According to OIT's December 2016 Security Assessment Report, OIT previously rated the vulnerability as high risk before downgrading it to moderate risk. On March 30, 2017, (b) (7)(E) which led to OIT further downgrading the vulnerability from moderate risk to low risk. The vulnerability remains open.

Two other POA&M items, identified in December 2016, also remain open and are considered low risk. (b) (7)(E)

(b) (7)(E) [redacted]

On May 17, 2017, we provided SEC management with a draft of our management letter for review and comment. In its May 26, 2017, response, management acknowledged that the TCR system redesign project has continued to experience difficulties and delays. Yet, given the critical nature of the information handled by the TCR system and the large number of agency staff that use it, the SEC will address certain recently identified usability issues before implementing the redesigned system. Management established a new timetable and stated that it is working diligently toward a go-live date of October 2, 2017. Management's comments are included as an attachment to this final management letter.

To help us determine whether further action by the OIG is warranted, we request that management provide the OIG, no later than June 14, 2017, a description of the actions the agency has taken or plans to take to:

1. stabilize the SEC's Oracle (b) (7)(E) [redacted] platform and establish consistent Oracle environments;
2. finalize the redesigned TCR system requirements;
3. address unresolved information security vulnerabilities in the current TCR system; and
4. review the planning and management of the SEC's project to redesign the TCR system to identify lessons learned.

We appreciate management's cooperation and look forward to receiving the information requested above. If you have questions, please contact 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
Jaime Klima, Chief Counsel, Office of Chairman Clayton
Peter Uhlmann, Managing Executive, Office of Chairman Clayton
Michael S. Piwowar, Commissioner
Richard Grant, Counsel, Office of Commissioner Piwowar
Kara M. Stein, Commissioner
Robert Peak, Advisor to the Commissioner, Office of Commissioner Stein
Robert B. Stebbins, General Counsel
Keith Cassidy, Director, Office of Legislative and Intergovernmental Affairs
John J. Nester, Director, Office of Public Affairs
Rick A. Fleming, Investor Advocate
TCR Oversight Board Members (voting)
Jennifer Diamantis, Chief, Office of Market Intelligence, Division of Enforcement
Pamela C. Dyson, Chief Information Officer, Office of Information Technology
Robert Fisher, Managing Executive, Office of Compliance Inspections and Examinations
Mary S. Head, Deputy Director, Office of Investor Education and Advocacy

Michele W. Layne, Regional Director, Los Angeles Regional Office
Elizabeth Murphy, Associate Director, Office of the Associate Director (Legal) Division of Corporation Finance
Douglas Scheidt, Associate Director and Chief Counsel, Division of Investment Management
Heather Seidel, Acting Director, Division of Trading and Markets
Vance Cathell, Director, Office of Acquisitions
Michael Whisler, Assistant Director, Office of Acquisitions
Darlene L. Pryor, Management and Program Analyst, Office of the Chief Operating Officer

Attachment

MEMORANDUM

May 26, 2017

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

From: Kenneth Johnson, Acting Chief Operating Officer
Stephanie Avakian, Acting Director, Division of Enforcement, and Chair, TCR Oversight Board

Scott Bauguess, Acting Chief Economist and Director, Division of Economic and Risk Analysis

Pam Dyson, Chief Information Officer

Re: Management's Response to the Office of Inspector General's May 17, 2017 Draft Management Letter, *Progress on the SEC's Tips, Complaints, and Referrals Intake and Resolution System Redesign and Vulnerability Remediation Efforts*

Thank you for the opportunity to review and provide comments on the Office of Inspector General's draft management letter: *Progress on the SEC's Tips, Complaints, and Referrals Intake and Resolution System Redesign and Vulnerability Remediation Efforts* ("the Draft Management Letter"). We appreciate the courtesy your staff has extended to us.

A mission of the U.S. Securities and Exchange Commission is to protect investors. In furtherance of that mission, the Agency receives and triages thousands of tips, complaints, and referrals ("TCRs") each year. These TCRs are effectively managed and triaged in our existing TCR system. The objective of TCR System Modernization ("TCR 3.0") is to enhance our current TCR system to improve its flexibility, scalability, and support the SEC's needs and policies as they evolve over time.

We acknowledge, as you describe in your letter, that the TCR system redesign project has continued to experience difficulties and delays. And as you also note in the management letter, TCR 3.0 passed the March 2017 User Acceptance Testing ("UAT") performed by the Division of Economic and Risk Analysis ("DERA"). In May 2017, DERA accepted TCR 3.0, conditioned upon the remediation of certain identified defects. Those defects are currently either remediated

in the development environment, or have been accepted as appropriate for training or preventive action.[12]

During and after the March 2017 UAT, because TCR 3.0 was stable and functioning well, users were able for the first time to effectively simulate the entirety of their existing work processes in TCR 3.0. As a result, users identified system usability issues in the new system that could adversely impact the efficiency and accuracy of current work processes, but that were not addressed by existing requirements. Thus, addressing these issues will require enhancements to the TCR 3.0 system as tested.

Given the critical nature of the information handled by the TCR system and the large number of Agency staff that use it, we determined in consultation with the TCR Oversight Board to address certain usability issues prior to implementing TCR 3.0 ("go-live"). We have established a new timetable and are working diligently towards a go-live date of October 2, 2017.

Thank you again for the opportunity to respond to the Draft Management Letter. We remain committed to successfully implementing a modernized system and look forward to providing a description of the actions the agency has taken and plans to take to address the items identified on page seven of the Draft Management Letter

[12] DERA will consider the defects remediated for acceptance purposes when DERA successfully tests the remediation in the production environment. We expect to be able to do so in July 2017.