January 24, 2018

To: Finance and Administration Committee

From: Darrell Johnson, Chief Executive Officer

Janet Sutter, Executive Director
Internal Audit Department

Subject: Fiscal Year 2016-17 Management Letter

Overview

In connection with the annual audit of the Orange County Transportation Authority's financial statements for fiscal year 2016-17, Vavrinek, Trine, Day & Company, LLP, has issued a management letter with five recommendations for improvement to internal controls.

Recommendations

A. Receive and file the Orange County Transportation Authority Management Letter June 30, 2017, as an information item.

B. Direct staff to implement auditor recommendations related to the information technology environment and procurement.

Background

Pursuant to Section 28770 of the Public Utilities Code, the Orange County Transportation Authority (OCTA) prepares an annual set of financial statements presenting OCTA's results of operations and financial position at fiscal year-end. OCTA is required to obtain an independent auditor's opinion on the Comprehensive Annual Financial Report (CAFR), as well as various fund financial statements. The audit was performed by Vavrinek, Trine, Day and Company, LLP (VTD), an independent accounting firm. In connection with the audit, VTD has issued a management letter, as required by the American Institute of Certified Public Accountants (AICPA), *Statement on Auditing Standards Number 115*.

Discussion

VTD has completed annual audits of OCTA's CAFR and various fund financial statements and schedules, and has issued an independent auditor's opinion thereon for the fiscal year (FY) ended June 30, 2017. In connection with the audit, VTD has issued a management letter identifying five control deficiencies as defined by the AICPA, *Statement on Auditing Standards Number 115*.

VTD reported that a sustainable patch management framework had not been established and recommended that a formal implementation plan, assessment of resources, and timeline be established. Management agreed and responded that a schedule for server, desktop, and mobile device patching has been documented, and a sustainable maintenance window for servers has been established. In addition, management indicated that firewall, router, hubs, and switches have an established patch management framework.

It was also observed that the last external penetration test was performed in 2015. VTD recommended management perform external penetration tests at least annually and consider performing social engineering tests to further strengthen information systems security. Management responded that a penetration test was recently completed in November 2017 and that remediation activities are currently being prioritized. A follow-up penetration test, along with unannounced social engineering testing, is planned for calendar year 2018.

VTD also reported that a documented disaster recovery tabletop test and walk-through had not been performed in the current year. VTD recommended that OCTA document annual testing of the disaster recovery plan to include a disaster recovery checklist, walk-through, table top exercise, and technical test; as well as documentation of the results, lessons learned, and needed improvements. Management indicated that a disaster recovery test had been performed, but agreed that documentation of the exercise, including the scope, walkthrough, and final results should be prepared.

Finally, VTD observed a monitor in the hallway of one of the OCTA headquarters floors which is connected to a production network and had not been configured to restrict access. VTD recommended that management strengthen its hardening procedures for such access points or other networkable devices. While the building is access-controlled, management agreed that implementation of networked equipment in more "public" areas will receive more scrutiny in the future. Also, management indicated that all netwok ports that are unused, even in secure areas, have been shut off.

With regard to procurement, VTD found that two of 26 files reviewed lacked evidence that a public notice was published in a newspaper of general circulation, as required by OCTA policy. VTD recommended that procedures be consistently followed. Management responded that additional steps have been included to the quality assurance process to ensure that evidence of publication is on file prior to release of the formal solicitation.

The management letter for FY 2016-17 is included herewith as Attachment A.

Summary

In connection with the annual audit of OCTA's financial statements for FY 2016-17, VTD has issued a management letter, which identified five recommendations for improvement to internal controls. Management has responded that these items will be addressed.

Attachment

A. Orange County Transportation Authority Management Letter for the Year Ended June 30, 2017

Prepared by:

Janet Sutter
Executive Director, Internal Audit
714-560-5591