ORANGE COUNTY TRANSPORTATION AUTHORITY

MANAGEMENT LETTER

FOR THE YEAR ENDED JUNE 30, 2017

VAVRINEK, TRINE, DAY & CO., LLP
Certified Public Accountants

VALUE THE *difference*

Board of Directors
Orange County Transportation Authority
Orange, California

In planning and performing our audit of the basic financial statements of the Orange County Transportation Authority (OCTA) as of and for the year ended June 30, 2017, in accordance with auditing standards generally accepted in the United States of America, we considered OCTA's internal control over financial reporting (internal control) as a basis for designing auditing procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of OCTA's internal control. Accordingly, we do not express an opinion on the effectiveness of OCTA's internal control.

We have previously reported on OCTA's internal control in our report dated October 31, 2017, in accordance with *Government Auditing Standards*. This letter does not affect our report dated October 31, 2017, on the financial statements of OCTA.

During our audit we noted certain matters involving internal control or operations that are presented for your consideration. These observations and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies and are summarized on the accompanying pages.

CURRENT YEAR OBSERVATIONS

1. SERVER AND DESKTOP PATCHES TO PREVENT THE EXPLOITATION OF INFORMATION SYSTEMS (IS) VULNERABILITIES

OBSERVATION:

OCTA is in the process of applying patches to its IS environment but needs to establish a more sustainable patch management framework. We noted that OCTA has expanded the use of tools to sort, prioritize and list patches for remediation. For example, patching for Java has increased for desktops and servers. However, the patch management framework should also address firewalls, routers, switches and hubs.

RECOMMENDATION:

Patch management is a critical risk area of the IS environment. A formal implementation plan, assessment of required resources and timeline should be established so that patches are prioritized and implemented. Further, if patching can negatively impact the environment, the devices or servers in question should not be maintained in the production environment.

MANAGEMENT'S RESPONSE:

Management agrees with audit recommendations and staff has implemented and documented a sustainable and holistic schedule for server, desktop, and mobile device patching as well as prescheduled patch review meetings for all Microsoft patches. A sustainable maintenance window for all application servers has also been established. All firewall, router, hubs and switches also follow an established patch management framework. In addition, staff has implemented network segmentation as an additional compensating control to protect our network environment.

2. EXTERNAL AND INTERNAL TESTING FREQUENCY AND REPORTING:

OBSERVATION:

OCTA has not scheduled or performed external penetration testing for 2017. OCTA's last external penetration test was in 2015. External penetration testing provides OCTA the ability to assess the security of its critical resources and should be performed annually.

RECOMMENDATION:

Given the size and complexity of OCTA's IS environment, OCTA should perform external penetration testing annually.

In addition, while OCTA has rolled out an employee education program on IS risks, OCTA should consider performing social engineering test to further strengthen IS security. OCTA does require employees to watch training videos that address social engineering and IT risk issues. However, OCTA should also perform testing of this program, which may include testing employees on a random basis via email, phone, shoulder surfing and tailgating.

MANAGEMENT'S RESPONSE

Staff worked with an external vendor in completing an internal, external and wireless penetration test in November of 2017. OCTA's cybersecurity team is currently reviewing the results and prioritizing remediation activities. A follow up test is planned for the first half of calendar year 2018. OCTA has also planned unannounced phishing social engineering testing in 2018.

3. DISASTER RECOVERY TESTING:

OBSERVATION:

OCTA has not documented its disaster recovery tabletop test and walk-through of the current year. Certain aspects of the program have been tested; however, the program requires a documented scope, walk-through and results, regardless of its current state or future plans.

RECOMMENDATION:

OCTA should document its annual testing of the disaster recovery plan to include the following:

- Disaster Recovery Checklist: This is a high-level document for items in the plan such as fuel for the generator, generator maintenance and performance and ensuring all critical team member know their roles and action step.
- Disaster Recovery Walk-Through: Test and verify the call-tree for employees and vendors. Test fuel delivery schedules, physical breakdowns and failures in the actual location that may occur.
- Disaster Recovery Table-Top Testing: This step is an extension of the first two steps. In this step, remove one or two key employees, discuss significant scenarios such as a complete failure of the internet connections, radio connections, catastrophic generator failures, untimely breach or even restricting physical access to any site connected to OCTA.
- Disaster Recovery Technical Testing: Test in parallel or live at the redundant site. The objectives include execution of the technical procedures necessary to resume information systems operations. Components of the testing of the recovery plan could be performed in stages (i.e. a component each quarter).
- Execution and Reporting: Document the results of the test including lessons learned and needed improvements.

MANAGEMENT'S RESPONSE:

Staff has performed a disaster recovery (DR) test in the current year. OCTA is transitioning from hosted DR to internally managed DR and has procured equipment that enables and accelerates system recovery in the event of a disaster. In addition to table top exercises performed in support of OCTA's COOP (Continuation of Operations Plan), the equipment was successfully tested this year by recovering a mission essential application. Staff agrees with auditor's recommendation to finalize the documentation of the DR exercise performed by including its scope, the walkthrough and final results. This documentation will serve as the basis for a DR checklist and final run book for next year's test.

4. PHYSICAL SECURITY:

OBSERVATION:

We observed a large touchscreen monitor hanging in the hallway on one of the floors. The monitor was connected to a desktop PC, which was connected to the production network and had not been configured to restrict access. Such access points could results in unauthorized access to the network. Although certain compensating controls exist such as a single sided badge for building entry or access to an elevator floor, OCTA can improve its physical security over these devices.

RECOMMENDATION:

OCTA should strengthen its hardening procedures for such access points or other networkable devices.

MANAGEMENT'S RESPONSE:

Management understands that it can always improve the security for any device, and since the equipment resided in an area that already requires badge access, staff believed that this compensating control was sufficient and that no additional security improvements were need by this equipment. Due to the auditor's recommendation, future implementation of networked equipment in "more" public areas will receive added review and attention by staff. As an additional control, staff has shut off all network ports that are unused, even in secure areas.

5. PROCUREMENT

OBSERVATION:

For 2 out of 26 procurements tested, a public notice was not published in a newspaper of general circulation as required by OCTA's procurement policy.

RECOMMENDATION:

We recommend procurement policies and procedures related to public notice be consistently followed.

MANAGEMENT'S RESPONSE:

CAMM concurs with this recommendation and has implemented additional steps in the review process of each procurement file. For added quality assurance prior to release of each formal solicitation, management will review each procurement file to verify evidence of written correspondences between CAMM staff and the Orange County Register to ensure public notice requests have been received and confirmed to publish two consecutive weeks prior to solicitation closing date in accordance with procurement policies and procedures.

Summarized below is the status of observations reported in the prior year management letter:

OBSERVATION	STATUS
Server And Desktop Patches To Prevent The Exploitation Of Information Systems (IS) Vulnerabilities	In progress, refer to current year recommendation
External And Internal Testing Frequency And Reporting	In progress, refer to current year recommendation
Business Resumption And Disaster Recovery Strategy ("Crash Cart")	Implemented
Encrypted Email Communications	Management has evaluated the recommendation and believes that current pathways and compensating controls are sufficient

****

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements, and therefore may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of the Orange County Transportation Authority gained during our work to make observations and suggestions that we hope will be useful to you.

We would be pleased to discuss these observations and recommendations with you at any time. This report is intended solely for the information and use of OCTA, management, and others within OCTA and is not intended to be and should not be used by anyone other than these specified parties.

Vavrinek, Trine, Day & Co., LLP

Laguna Hills, California
October 31, 2017