ORANGE COUNTY TRANSPORTATION AUTHORITY

MANAGEMENT LETTER

JUNE 30, 2012

Board of Directors
Orange County Transportation Authority
Orange, California

We have audited the financial statements of the Orange County Transportation Authority (OCTA) as of and for the year ended June 30, 2012 and have issued our report thereon dated October 29, 2012. In planning and performing our audit of the financial statements of the OCTA, we considered internal control over financial reporting in order to determine our auditing procedures for the purpose of expressing our opinions on the financial statements and not to provide an opinion on the internal control over financial reporting. An audit does not include examining the effectiveness of internal control and does not provide assurance on internal control. We have not considered internal control since the date of our report.

During our audit, we noted certain matters involving internal controls and other operational matters that are presented for your consideration. These comments and recommendation, 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.

Our audit procedures are designed primarily to enable us to form opinions 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 OCTA gained during our work to make comments and suggestions that we hope will be useful to you.

We would be pleased to discuss these comments and recommendations with you at any time. This report is intended for the information and use of the Board of Directors, and OCTA's management 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 29, 2012

25231 Paseo De Alicia, Suite 100 Laguna Hills, CA 92653 Tel: 949.768.0833 Fax: 949.768.8408 www.vtdcpa.com
FRESNO • LAGUNA HILLS • PALO ALTO • PLEASANTON • RANCHO CUCAMONGA • RIVERSIDE • SACRAMENTO

ORANGE COUNTY TRANSPORTATION AUTHORITY
OBSERVATIONS RELATED TO INTERNAL CONTROL OVER FINANCIAL REPORTING
FOR THE YEAR ENDED JUNE 30, 2012

CURRENT YEAR OBSERVATIONS

1. MANAGING THIRD PARTY SERVICES

OBSERVATION

OCTA relies on the information system of Cofiroute, USA to track and report financial activities related to the 91 Express Lanes. OCTA has not required Cofiroute to obtain a Service Organization Report (SOC 1, Type II report). An SOC 1, Type II audit reports on the fairness of the presentation of management's description of the service organization's system and the suitability of design and operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period.

RECOMMENDATION

We recommend that OCTA require an SOC 1, Type II report from Cofiroute, USA on a periodic basis. It was noted that as of the date of this letter, the agreement between OCTA and Cofiroute was amended requiring Cofiroute to provide OCTA with an SOC 1, Type II report by the end of fiscal year 2012-2013.

MANAGEMENT'S RESPONSE

OCTA management agreed with the auditor's recommendation and executed an amendment to Agreement C-5-0300 on October 1, 2012 with Cofiroute USA, LLC. The amendment requires Cofiroute to provide OCTA with a Service Organizational Control 1, Type II report by the end of fiscal year 2012-13.

2. INFORMATION TECHNOLOGY PASSWORD MANAGEMENT

OBSERVATION

Passwords are used to authenticate users of operating systems, applications, hardware, and remote access solutions. In the prior year, recommendations to OCTA's password requirements were implemented to improve password management. However, during the performance of the current audit, we noted that passwords are set to expire after 180 days (OCTA Access Control Security Policy states 60 days) and multiple logins can be attempted without risk of lockout.

RECOMMENDATION

We recommend OCTA implement procedures to ensure password management practices are in accordance with OCTA Policy.

MANAGEMENT'S RESPONSE

Management understands the recommendations, yet believes that OCTA's current password management practice provides an equivalent level of security to that of the recommendation and is sufficient to protect OCTA. Management also agrees with the auditor's recommendation regarding "lockout" and will implement when a resolution regarding mobile devices is determined.

In February 2012, Information Systems (IS) implemented strong passwords to continue to improve OCTA's password management. The new strong passwords required that users insert alpha-numeric, case sensitive and special characters, and increase the minimum number of characters in their password from eight (8) to ten (10). Based upon information provided by various internet-based password strength tools, the new strong passwords allowed IS to increase the expiration time from ninety (90) to one-hundred and eighty (180) days, still provide the same level of security, while minimizing disruption to the business units.

The "lockout" rule within the password policy was not enabled due to issues experienced with mobile devices such as smart phones and tablets. These devices would lock out a user account the moment the password was changed on the network if their mobile device's password wasn't immediately changed as well. The IS department will continue to research this issue for resolutions which would eliminate the possibility of lockouts on mobile devices. Until that time, IS recommends that the "lockout" rule remain disabled.

The "Access Control Security Policy (FA-IS-900.07ACCESSCONT)" will be modified so that it is consistent with the statements listed above.

3. SECURITY CONFIGURATION CHECKLIST

OBSERVATION

Vulnerabilities in Information Technology (IT) products surface nearly every day, and many ready-to-use exploits are widely available on the Internet. Because IT products are often intended for a wide variety of audiences, restrictive security controls are usually not enabled by default, so many IT products are immediately vulnerable out of the box. OCTA was unable to provide security configuration checklists (also called a lockdown, hardening guides, or benchmarks) for their firewalls, routers, switches, servers and desktops. The use of well-written, standardized checklists can markedly reduce the vulnerability exposure of IT products.

RECOMMENDATION

We recommend that OCTA use security configuration checklists to emphasize both hardening of systems against software flaws (e.g. by applying patches and eliminating unnecessary functionality) and configuring systems securely to help reduce the number of ways in which the systems can be attacked, resulting in greater levels of product security and protection from future threats. Typically, checklists are created by IT vendors for their own products.

MANAGEMENT'S RESPONSE

Management concurs with the auditor's recommendation that utilizing a security configuration checklist, particularly SP 800-70 authored by the National Institute of Standards and Technology (NIST) as a tool to assist OCTA's Information Systems (IS) department in making our environment less vulnerable to exploits would be a good business practice. At this time, however, OCTA lacks the necessary resources to fully implement this recommendation. Instead, management has implemented other mitigating controls believed to be sufficient to safeguard OCTA. Some of these mitigating controls include hardened AD GPOs (Active Directory Group Policy Objects) that are applied to all new desktop deployments. The GPOs and hardening are based on research and industry best practices. Policies also take into account specific business needs and security requirements at OCTA. The use of AD GPOs allows OCTA to apply changes to all desktops in an environment or only to certain groups of desktops as needed. In the event of a new security threat or vulnerability, OCTA can quickly respond by changing the GPO and pushing the change to any machines that may be impacted. In addition, OCTA has implemented intrusion detection and prevention measures that further protect the organization against vulnerabilities.

ORANGE COUNTY TRANSPORTATION AUTHORITY
PRIOR YEAR MANAGEMENT LETTER COMMENTS
FOR THE YEAR ENDED JUNE 30, 2012

Summarized below is the current status of observations reported in the 2011 Management Letter:

	Topic	**Current Status**
1	ARBA Trust Account Reconciliation	Implemented
2	Investment Policy	Implemented
3	Managing Third Party Services	Partially Implemented – See Management Letter Comment 1
4	Information Technology User Access Review	Implemented
5	Information Technology Password Management	Partially Implemented – See Management Letter Comment 2
6	Server and Desktop Patches to Prevent the Exploitation of IT Vulnerabilities	Implemented