ATTACHMENT A

ORANGE COUNTY TRANSPORTATION AUTHORITY

MANAGEMENT LETTER

FOR THE YEAR ENDED JUNE 30, 2016

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, 2016, 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, 2016, in accordance with *Government Auditing Standards*. This letter does not affect our report dated October 31, 2016, 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 MANAGEMENT LETTER 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.

RECOMMENDATION:

Generally, patch management is a critical risk area of the IS environment. Per inquiry, management has considered different approaches but this is an area that continues to require attention. A formal implementation plan, assessment of required resources and timeline should be established so that patches are prioritized and brought current. In addition, OCTA should consider expanding its utilization of tools it has available to sort and prioritize patches that require remediation in a timely manner.

MANAGEMENT'S RESPONSE:

Information Systems agrees to continually improve the processes and procedures for patch management. After the recent cyber incident, staff has substantially increased the frequency of patching our systems. The goal is to have all of our Microsoft Windows based servers and desktops patched monthly.

In addition to conversations with Microsoft to possibly engage their Software Update Management service, staff has permanently increased resources to its cyber security team by adding an additional full time position to it. The purpose of these engagements will be to streamline our software update management cycle and create a documented, disciplined process that will help us keep our systems up to date, especially with the latest security patches. If Microsoft is not engaged, staff will seek other vendors to perform this service. The added staff resource will implement and maintain the processes and procedures recommended by the engaged vendor to keep software patches up to date.

2. EXTERNAL AND INTERNAL TESTING FREQUENCY AND REPORTING:

OBSERVATION:

Based on our inspection of third party external penetration testing and internal vulnerability reports, it was noted that only a sample of external and internal assets were tested. Further, these third party assessments were performed on an annual basis.

RECOMMENDATION:

Given the size and complexity of OCTA's IS environment, OCTA should evaluate more frequent external penetration and internal vulnerability assessments. With respect to internal vulnerability assessments, OCTA performs monthly scans from Qualys but the scans should be configured to generate more frequent internal vulnerability reports. Qualys maintains the capability of providing assessments daily. Vulnerabilities and risks should be prioritized with timely corrective action and leveraged for third party exams.

Annual vendor testing should consider including all assets on the external facing and internal facing networks. The purpose of this third party testing is to validate OCTA's procedures, security posture and reduce the risk with IS assets. Further, following a breach or incident, a more aggressive testing schedule should be performed.

In addition, while OCTA has rolled out an employee education program on IS risks, OCTA should consider performing social engineering testing as an additional tool for strengthening OCTA's IS security.

MANAGEMENT'S RESPONSE

Information Systems agrees with the recommendation and will evaluate the request to increase the frequency of both the external penetration testing and the internal vulnerability assessments in order to improve our overall security posture. We will also consider adding social engineering techniques into the external penetration testing.

Information Systems will work with Dell SecureWorks, our Managed Security provider to optimize usage of the Qualys network security and vulnerability management toolset. We will also engage with Dell Secure Works to determine the changes in scope for our penetration testing to include all assets both on our external facing and internal facing networks.

Information Systems is already in the process of procuring consulting services for an Industrial Control System (ICS) Cyber Assessment. By doing so we will be able to better gauge the risk associated with our ICS components and put in the proper monitoring procedures to better protect those assets.

In response to more aggressive testing after the security incident, Information Systems did engage with Microsoft's advanced security team to determine the impact of the event. IS decided not to perform additional penetration testing due to the incident but will review and update our procedures if we deem that the additional testing will add value.

3. BUSINESS RESUMPTION AND DISASTER RECOVERY STRATEGY:

OBSERVATION:

It was noted that OCTA maintains documentation for business resumption and disaster recovery procedures. However, we noted that OCTA has not established "disaster recovery laptops".

RECOMMENDATION:

As OCTA evaluates its continuity of operations and disaster recovery plans, we recommend that OCTA consider establishing disaster recovery (DR) laptops or designating current laptop computers as DR personal computers (PC) to aid in business resumption. The DR laptops, tablets or DR virtual PCs should have all required scripts, usernames, passwords, software dependencies, vendor contacts, recovery and backup paths, master images, group policy objects, active directory configuration settings, connectivity paths and any other supporting information that may be required to restore the IS environment. The data on these laptops should utilize password vaults, software and script libraries, and be encrypted. Documentation of each designated PC, tablet or laptop should be recorded within the current recovery procedures so that if a disaster is declared, the disaster recovery team is aware of the assets. These assets should also be incorporated in the annual DR testing plan.

MANAGEMENT'S RESPONSE:

Information Systems agrees that having key information listed above readily available during the event of a disaster would be beneficial to the success of the recovery. Our concern with using laptops is that they may get stored away and not function properly when needed. Information Systems will go forward with the recommendation but evaluate what would be the best media available to store the information. No matter the media determined to be used, processes will need to be put in place to regularly test the equipment to ensure that it is fully functional during the event of a disaster.

4. ENCRYPTED EMAIL COMMUNICATIONS:

OBSERVATION:

OCTA has asserted that outbound email is encrypted. However, OCTA does not provide an email encryption portal or path for stakeholders.

RECOMMENDATION:

OCTA should consider providing stakeholders and external contacts an encrypted path for sending emails to OCTA.

MANAGEMENT'S RESPONSE

Information Systems will engage with both Microsoft (our primary email provider) and Gartner (our IS Advisory Service) in guiding us how to properly meet the recommendation of allowing our external partners a way to securely send email to OCTA. Microsoft has stated that the majority of third party email service providers encrypt their messages in transit via Transport Layer Security (TLS). Staff will confirm this as part of our research.

****

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, 2016