January 23, 2017

To: Members of the Board of Directors

From: Laurena Weinert, Clerk of the Board

Subject: Fiscal Year 2015-16 Management Letter

Finance and Administration Committee Meeting of January 11, 2017

Present: Directors Do, Hennessey, Jones, Pulido, Spitzer, and Steel
Absent: None

Committee Vote

This item was passed by the Members present.

Committee Recommendations

A.   Receive and file the Orange County Transportation Authority Management Letter June 30, 2016.

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

Committee Discussion

Chairman Spitzer asked for clarification on Orange County Transportation Authority's (OCTA) responses to the external auditor's management letter recommendations for improvement to internal controls related to cyber security. Chairman Spitzer was concerned that management's responses did not demonstrate a firm enough commitment to rectifying the three issues outlined in the report, especially in light of the cyber event that occurred at OCTA last year. Chairman Spitzer was satisfied with the verbal responses provided by staff and directed that those responses be memorialized in writing.

The first issue identified related to server and desktop patches to prevent the exploitation of information systems vulnerabilities. Staff reaffirmed its agreement with the auditor recommendation and explained that extra effort and resources have been assigned to the patching process. Staff also reaffirmed that patch management is one of the highest priorities in OCTA's cybersecurity program and provided a firm commitment to follow the auditor's recommendations.

The second issue related to management's frequency of penetration testing and the auditor's recommendation for social engineering testing. Staff also reaffirmed agreement with the auditor's recommendation and mentioned that social engineering (internal Phishing) will be performed when mandatory cybersecurity training is completed. Mandatory cybersecurity training has been rolled out to all OCTA administrative employees and will be complete by the end of the fiscal year. Staff stated that penetration tests are valuable but that the amount of resources required to perform these tests is considerable. Staff acknowledged that OCTA will perform more than one penetration test per year; however, the number of tests will be determined by need and available resources.

The last recommendation related to the need for "disaster recovery laptops." Staff noted that devices will be made available and that OCTA's Continuity of Operations Plan (COOP) will dictate the quantity and location for the chosen devices. The COOP plan is scheduled for completion at the end of the fiscal year at which time the appropriate devices for disaster recovery will be identified.

Lastly, Chairman Spitzer asked that a brief report on this item be provided to the full Board of Directors.