DELAWARE RIVER PORT AUTHORITY
STEWARDSHIP. SERVICE. COMMUNITY.

One Port Center
PO Box 1949
2 Riverside Drive
Camden, NJ 08101

(856) 968-2000
(856) 968-2001 Fax
www.drpa.org

David J. Aubrey, CIA, CFE
Acting Inspector General
Office of the Inspector General

OIG Memorandum

TO: K. A. LaMarca, Director, Information Services

FROM: D. J. Aubrey, Acting Inspector General

SUBJECT: Review of Service Organization Controls (SOC) Reports for Microsoft Office 365 (October 2016 – February 2018)

DATE: May 17, 2018

As part of the Office of the Inspector General (OIG) IT audit focus, we have reviewed the most current and available Service Organization Controls reports for the Microsoft Office 365 Service Provider (see attachments; the attached reports are noted for "Restricted Use" and should be treated accordingly). This review was performed by R. McReynolds, IT Auditor, with reports provided by Kevin LaMarca, Director, Information Services. The objective of this review is to provide reasonable assurance that the service provider for the Microsoft Office 365 systems has controls in place to mitigate risk regarding security, availability, processing integrity, confidentiality, privacy, and that the controls have been tested and any material issues remediated. Microsoft is the contracted service provider for email, Office, Sharepoint, OneDrive and Skype applications for the Authority's cloud-based back office systems. To accomplish this review OIG has reviewed the following audit reports:

- SOC2 Type 2 Report (SOC2), and Statement on Standards for Attestations Engagements (SSAE) 18 Report;
- SOC2 Type 1 Additional Services Report (SOC2), and Statement on Standards for Attestations Engagements (SSAE) 18 Report;
- SOC1 Type 2 and Statement on Standards for Attestations Engagements (SSAE) 18 Report; and,
- SOC Bridge Letter 1Q 2018.

The scope of the reports provided and reviewed were valid from October 1, 2016 through September 30, 2017, with a bridge letter for the period October 1, 2017 through February 7, 2018.

These independent audit reports are control attestations provided by the third-party service provider to provide assurance to their clients (in this case, the Authority) that the contracted services and facilities have an adequate control environment in place to protect our data. The reports also document the testing and results of the controls by the independent attesting organization.

Microsoft's (the cloud application provider) policies and procedures were evaluated for system access and operations controls. Microsoft locations were reviewed for adherence to policy and procedures for logical access to systems, physical security, network security, environmental protection, power backup, fire alert and suppression capabilities, application hosting, disaster recovery and data backup.

For the period October 1, 2016 through September 30, 2017, the independent attesting organization, Deloitte from Seattle, WA, reported two exceptions based on their testing of the controls for Microsoft within their report dated December 22, 2017:

1. "One of 65,928 users was identified as terminated from Microsoft during the audit period had maintained "active" account status in IDM after their termination date." Microsoft Management's response: "*In response to the finding Microsoft management indicated that the user was terminated manually after discovery."*

2. "Management noted that static analysis security testing was not being performed on changes deployed to production to one branch of the Exchange code repository from October 2016 - March 2017." Microsoft Management's response: "*In response to the finding Microsoft management indicated that both branches were brought up to standard as part of a continual improvement investment prior to the issue being discovered. The O365 security team ran the security static analysis tool on all builds released to production from those branches to bring them up to par with production code."*

Both reported exceptions were addressed by Microsoft in a timely and effective manner.

The bridge letter from Microsoft states that the controls have not changed from October 1, 2017 through February 7, 2018. Based on review of the reported results from the independent attesting organization, OIG concurs with the conclusion that an appropriate control environment exists at Microsoft. No further actions are required.

OIG has discussed the results of this review with IS management and will continue to work with IS management in review of third-party provider IT controls as the annual SOC audits conducted and reports made available.

Attachments (*restricted use*)
(Note: The noted attachments have not been included due to their proprietary and confidential nature.)

cc: R. Boyer
J. Nash
E. DePasquale
R. Taylor
S. Murphy
A. Nelson
J. Hanson
M. Wing
R. Santarelli
R. McReynolds