INTERNAL AUDIT DEPARTMENT

Audit No. 1908-F

September 8, 2020

To: Chairwoman Michelle Steel, Supervisor, 2nd District
Vice Chairman Andrew Do, Supervisor, 1st District
Supervisor Donald P. Wagner, 3rd District
Supervisor Doug Chaffee, 4th District
Supervisor Lisa A. Bartlett, 5th District
Members, Audit Oversight Committee

From: Aggie Alonso, CPA, CIA, CRMA
Internal Audit Department Director

Subject: OCIT Ransomware Readiness Self-Assessment

Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website. With the significant increase of ransomware attack threats to various levels of U.S. government entities and its computer systems infrastructure in recent times, it is vital that comprehensive ransomware readiness controls exist and are constantly evaluated to prepare and mitigate the risk of such an attack.

Internal Audit worked with OCIT to complete a self-assessment of OCIT's ransomware readiness as of March 31, 2020. Based on our review, we concluded controls were generally effective to provide reasonable assurance that OCIT is prepared to mitigate the risk of a ransomware attack for the agencies under their direct control and oversight. While this assessment was conducted at a point in time, we encouraged OCIT to continue to stay abreast with the constantly evolving landscape of ransomware threats and vulnerabilities, and to continue to self-assess their own ransomware readiness.

We identified opportunities for OCIT to enhance internal controls and included them in a separate memo (issued to OCIT) not subject to public release due to the sensitive nature of the specific findings.

cc: CEO Distribution
Foreperson, Grand Jury
Robin Stieler, Clerk of the Board
Eide Bailly LLP, County External Auditor