THE CITY OF SAN DIEGO

DATE: June 24, 2019

TO: Honorable Members of the Audit Committee

FROM: Kyle Elser, Interim City Auditor

SUBJECT: **Annual Citywide IT Risk Assessment and Audit Work Plan - Fiscal Year 2020**

Attached is the IT Risk Assessment and Audit Work Plan proposed by the Office of the City Auditor for Fiscal Year 2020. This report will be presented at the July 10th Audit Committee meeting for your review and consideration. The IT Audit Work Plan was developed by identifying and ranking the major risks associated with the City's significant information systems and corresponding processes. We designed our IT Audit work plan to address what we considered to be risk areas, while limiting the scope of work to what we can realistically accomplish with the IT staff resources available. For security reasons, the detailed risk scoring for each application and IT process was not included in this report.

Risk assessment is a process of systematically scoring (or rating) the relative impact of a variety of "risk factors." A risk factor is an observable or measurable indicator of conditions or events that could adversely affect the organization. Risk factors can measure inherent risks or organizational vulnerability.

Creating the IT Risk Assessment

The first step in creating the City's IT Risk Assessment model is to define the IT audit universe. The IT audit universe is a listing of all City information systems and corresponding processes both automated by those systems and supporting those systems. We utilized the IT Department's application portfolio and accompanying information to identify the known active information systems in the City's network.

The next step in creating the risk assessment model was to identify and rank the major risks associated with each of the City's information systems and corresponding processes. To achieve this, the Auditors requested information from the IT Department on the information system and network portfolios regarding department, application, process and various risk information to perform a risk assessment. The assessment utilized the eight measurable risk factors outlined below:

Auditor Ranking

1) Inherent Sensitivity of IT Process
2) IT Process Audit Risk Scores Compiled from Previous IT Audits
3) Significance of Major Modifications to the IT Landscape
4) Core IT Service Providers Independent Auditor Attestation Assessment

IT Department Ranking

5) Business Alignment
6) Technical Architecture
7) Supportability

Department Criticality Ranking

8) Mission Criticality of Applications and Supported Business Processes

Scoring the IT Universe

The score assignment relates to the impact to the City if an application or network service were compromised or hacked and the corresponding processes they supported were compromised as a result. For example, the City Library rated their catalogue system as mission critical to their operations; however, the City would not experience significant risk if this system were hacked based on the data contained in the system. Conversely, the impact of the data theft from a financial or human capital supporting system could be incredibly damaging and open the City to costly litigation if it contained personal information such as social security numbers, while the business criticality may be very low.

The final step in completing the Citywide IT Risk Assessment was to calculate the total risk score for each application and IT process in order of highest risk score to the lowest by combining the risks scores from the three identified categories to identify the highest risk systems for our review.

IT Audit Work Plan FY2020

Based on our IT Risk Assessment, we are proposing two Carry Over Audits and two new Planned Audits for a combined total of 2,300 Audit Hours.

<u>Carry Over Audits:</u>

1) IT Audit of Network Perimeter Controls:

Estimated 400 Audit Hours. **In Fieldwork stage**.

The objective of this IT Audit is to assess the security of the City's network perimeter controls.

2) IT Audit of Citywide Sensitive Data Encryption Standards and Data Classification:

Estimated 415 Audit Hours. **In Planning Stage**.

The objective of this IT Audit is to assess the maturity of the City's sensitive data encryption and data classification process.

Planned Audits:

1) IT Audit of Legacy Applications: Estimated 600 Audit Hours

The tentative objective of this IT Audit is to assess the impact of the legacy applications to the City's IT security posture and assess additional impacts.

2) Audit of IT Service Delivery Effectiveness: Estimated 885 Audit Hours

The tentative objective for this audit is to review the strengths and weaknesses of the IT Departments service delivery from an internal customer's perspective. Because the subject matter is broad, this is the first of a series of audits reviewing various aspects of IT service deliveries.

Respectfully submitted,

Kyle Elser
Interim City Auditor

cc: Honorable Mayor Kevin Faulconer
Honorable Members of the City Council
Kris Michell, Chief Operating Officer
Stacey LoMedico, Assistant Chief Operating Officer
Ron Villa, Assistant Chief Operating Officer
Jessica Lawrence, Director of Council Affairs
Mara Elliott, City Attorney
Andrea Tevlin, Independent Budget Analyst
Jonathan Behnke, Chief Information Officer