THE CITY OF SAN DIEGO

DATE: July 22, 2021

TO: Honorable Members of the Audit Committee

FROM: Andy Hanau, City Auditor

SUBJECT: **Annual Citywide IT Risk Assessment and Audit Work Plan – Fiscal Year 2022**

Attached is the IT Risk Assessment and Work Plan proposed by the Office of the City Auditor for Fiscal Year 2022. 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 regarding the IT System and Network Portfolios' associated departments, applications, processes, and risks.. The assessment utilized the nine 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
5) Citywide IT Service Delivery Effectiveness Survey

IT Department Ranking

6) Business Alignment
7) Technical Architecture
8) Supportability

Department Criticality Ranking

9) 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 lowest by combining the risks scores from the three identified categories to identify the highest risk systems for our review.

Carry Over Audits:

The IT Application Audit of the Fire Department's Emergency Response Management System is currently in the planning stage and requires 570 hours in FY 2022 to Complete.

Planned Audits:

1) **IT Performance Audit of Fire-Safety Department's Network Security**

   The tentative objective of this audit is to assess the network security of the Fire-Safety Department's network. Estimated 1,000 Hours.

2) **IT Integrated Performance Audit of the San Diego Police Department – Body Camera Usage**

   The tentative objective of the IT audit component of this audit is to assess IT controls over SDPD Body Camera Footage in coordination with the Performance Audit of San Diego Police Department – Body Camera Usage. Estimated 300 Hours*.

3) **IT Integrated Performance Audit of Get It Done Application**

   The tentative objective of the IT component of this audit is to assess the integration of the Get It Done Application with SAP Enterprise Asset Management (EAM) and identify operational improvements to help improve the accuracy and efficiency of the information reported through the Get It Done Application. Estimated 900 audit hours*.

*IT audit hours for integrated audits are identified and allocated within the Performance Audit Work Plan.

Replaced Audits:

The Audit of the IT Procurement and Vendor Management Process was scoped to focus on the IT central contracts (formerly Atos, CGI, and Zensar) and IT procurement process. The IT central contracts are being replaced this fiscal year and the procurement system is undergoing significant update and process improvements that impact how the IT portion of procurement will function. As a result, we are removing this audit from the FY 2021 carryover to FY 2022 and will conduct it in a future work plan when these contracts and systems are not undergoing significant changes.

IT Audit Reports Issued in FY 2021:

1) CONFIDENTIAL – IT Audit of Legacy Applications
2) IT Performance Audit of IT Legacy Applications
3) IT Performance Audit of IT Service Delivery Effectiveness

Respectfully submitted,

Andy Hanau
City Auditor

cc: Honorable Mayor Todd Gloria
Honorable Members of the City Council
Honorable City Attorney, Mara Elliott
Andrea Tevlin, Independent Budget Analyst
Jay Goldstone, Chief Operating Officer
Jeff Sturak, Assistant Chief Operating Officer
Matthew Helm, Chief Compliance Officer
Jonathan Behnke, Chief Information Officer