City of Miami

THEODORE P. GUBA, CPA, CIA, CFE
INDEPENDENT AUDITOR GENERAL

Telephone (305) 416-2044
E-Mail: tguba@miamigov.com

April 28, 2021

Honorable Members of the City Commission
City of Miami
3500 Pan American Drive
Coconut Grove, FL 33133-5504

Re: Audit of Compliance with the Driver's License and Motor Vehicle Record Data Exchange Usage Requirements
Report No. 21-09

Executive Summary

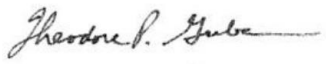
We have completed an audit of the City of Miami's (City's) compliance with the Driver's License and Motor Vehicle Record Data Exchange Usage requirements established by the Florida Department of Highway Safety and Motor Vehicles (HSMV). The City and HSMV entered into a Memorandum of Understanding (MOU), HSMV-0324-19, effective on December 31, 2018, providing for the exchange of City employees' driver's license data. Our review primarily covered the period from August 8, 2018 to January 15, 2020.

The audit objectives included determining whether the City's internal controls governing the use and dissemination of personal data have been evaluated in light of the requirements of this MOU, and applicable laws and are adequate to protect the personal data from unauthorized access, distribution, use, modification, or disclosure. We verified that the City has implemented policies/procedures for personnel to follow and data security procedures/policies to protect personal data. We confirmed that the data security procedures/policies have been approved by a Risk Management IT Security Professional and ensured that all deficiencies/issues found during the audit were corrected and that measures were enacted to prevent their recurrence.

During our audit, we identified opportunities for the City to strengthen internal controls, and we discussed our detailed findings and recommendations with the auditees. Prior to the conclusion of our fieldwork, we determined that the City's Department of Risk Management and Department of Information Technology implemented stronger internal controls to correct the issues found during the audit and complied with the MOU and applicable laws. Additionally, we also recommended that the City's Department of Human Resources improve the City's administrative policies surrounding the driver's license review processes. Details of our audit findings and recommendations are included on pages 3 through 12 of the report.

We wish to express our appreciation for the cooperation and courtesies extended to us during the audit by City personnel in the departments of Risk Management, Technology and Innovation, and Human Resources.

Sincerely,



Theodore P. Guba, CPA, CIA, CFE
Independent Auditor General

C: The Honorable Mayor Francis Suarez
Art Noriega V., City Manager
Victoria Mendez, City Attorney
Todd Hannon, City Clerk
Fernando Casamayor, Assistant City Manager/Chief of Operations
Natasha Colebrook Williams, Assistant City Manager
Nzeribe Ihekwaba, Assistant City Manager/Chief of Infrastructure
Ann-Marie Sharpe, Director, Risk Management Department
Angela Roberts, Director, Human Resources Department
Michael Sarasti, Director, Department of Innovation and Technology
Members of the Audit Advisory Committee
Audit Documentation File

Audit conducted by: Robyn Sachs, CPA, CIA, CISA, CFE, CISSP
Information Systems Audit Administrator

Audit reviewed by: Karuna (Mala) Khilnani, CPA, CISA, Assistant to the Auditor General

AUDIT OF COMPLIANCE WITH THE DRIVER'S LICENSE AND MOTOR VEHICLE RECORD DATA EXCHANGE USAGE REQUIREMENTS

AUGUST 8, 2018 THROUGH JANUARY 15, 2020

REPORT No. 21-09

TABLE OF CONTENTS

SCOPE, OBJECTIVES AND METHODOLOGY

The scope of the audit included, but was not limited to, reviewing the City of Miami's (City's) internal controls and data security activities over the driver's license data exchanged with the Florida Department of Highway Safety and Motor Vehicles (HSMV) under Memorandum of Understanding (MOU) HSMV-0324-19. The audit primarily covered the period from August 8, 2018 to January 15, 2020 and focused on the following objectives:

- To determine whether the City's internal controls governing the use and dissemination of personal data have been evaluated in light of the requirements of this MOU, and applicable laws and are adequate to protect the personal data from unauthorized access, distribution, use, modification, or disclosure.
- To verify that the City has implemented policies/procedures for personnel to follow and data security procedures/policies to protect personal data.
- To confirm that the data security policy procedures/policies have been approved by a Risk Management IT Security Professional.
- To ensure that all deficiencies/issues found during the audit were corrected and that measures were enacted to prevent their recurrence.

The methodology of the audit included:

- Reviewing MOU HSMV-0324-19 between the City and the HSMV.
- Reviewing relevant statutes and regulations, including the Driver's Privacy Protection Act.
- Completing process walk-throughs.
- Interviewing appropriate personnel.
- Performing tests of the City's internal controls over data security.
- Completing an assessment of data reliability and integrity for related computer systems.
- Detailed testing of relevant records, reports and activities.
- Verifying that correct actions have been implemented.
- Other audit procedures as deemed necessary.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

BACKGROUND

The City has implemented Administrative Policy Manual (APM) 3-99, entitled "City Vehicle Assignment, Operation, 24-hour Vehicle – City Employee Liability, Maintenance, Acquisition and Disposal." The APM states that it is the policy of the City to ensure that all operators of motor vehicles used in the course and scope of City business have and maintain a driving record that does not expose the City to undue risk.

The APM describes the criteria that must be followed for City employees driving City vehicles, including possessing a valid State of Florida driver's license at all times and immediately informing their supervisor if the employee's driving privileges have become restricted, suspended, and/or revoked. Additionally, the APM states that the Department of Risk Management shall conduct a bi-monthly driver's license record review of all employees driving City vehicles.

In order to comply with the City's requirement that the Department of Risk Management (RM Department) review the driver's license records of all employees driving City vehicles, the RM Department signed a Memorandum of Understanding (MOU) HSMV-0324-19 with the Florida Department of Highway Safety and Motor Vehicles (HSMV) on August 8, 2018. At the time the RM Department executed the MOU, they signed a Certification Statement attesting that they have appropriate internal controls in place at all times to ensure that the data exchanged under the MOU is protected from unauthorized access, distribution, use, modification and disclosure. This includes policies/procedures in place for personnel to follow and data security procedures/policies to protect personal data. The MOU requires that data security procedures/policies be approved by a Risk Management IT Security Professional.

The MOU was executed on December 31, 2018 (the date the HSMV countersigned the MOU) and required that the RM Department complete an Annual Certification Statement within fifteen (15) business days after the anniversary of the execution of the MOU or submit an Internal Control and Data Security Audit upon request by the HSMV. During any year in which the Internal Control and Data Security Audit is requested, submission of the audit may satisfy the requirement to complete an Annual Certification Statement. The MOU is for a period of three years, from December 31, 2018 through December 31, 2021.

In mid-2019, the HSMV requested that the RM Department submit an Internal Control and Data Security Audit by January 15, 2020; on January 2, 2020, the RM Department requested that our Office conduct the audit. The MOU requires that any and all deficiencies/issues found during the audit be corrected and that measures be enacted to prevent their recurrence. The audit findings were presented to auditees as they arose during the audit, however, corrective actions were not implemented by auditees within the City until March 2021. As a result, the HSMV terminated the City's access to the data exchange in February 2021.

This report contains the results of the Internal Control and Data Security Audit requested by HSMV to be conducted through the due date of the audit (January 15, 2020), including the deficiencies/issues found during the audit, corrective actions taken by the City, and measures implemented to strengthen the internal controls.

AUDIT FINDINGS AND RECOMMENDATIONS

During our audit, we identified opportunities for the City to strengthen internal controls, and we discussed our detailed findings and recommendations with the auditees. Prior to the conclusion of our fieldwork, we determined that the City's Department of Risk Management and Department of Information Technology implemented stronger internal controls to correct the issues found during the audit and complied with the MOU and applicable laws. Additionally, we also recommended that the City's Department of Human Resources improve the City's administrative policies surrounding the driver's license review processes.

Details of our audit findings and recommendations are included on pages 3 through 12 of the report.

FINDING 1: MANDATORY TRAINING WAS NOT CONDUCTED IN THE AREAS OF CONFIDENTIALITY OF INFORMATION AND CIVIL AND CRIMINAL SANCTIONS

The MOU between the City and the HSMV established the requirements that the City must follow to have access to the driver's license information maintained by the HSMV. MOU Section V. Safeguarding Information, Part F, states:

> "All personnel with access to the information exchanged under the terms of this MOU will be instructed of and acknowledge their understanding of the confidential nature of the information. These acknowledgements must be maintained in a current status by the Requesting Party [City] and provided to the Providing Agency [HSMV] within ten (10) business days of a request."

Additionally, Section V. Safeguarding Information, Part G, of the MOU states:

> "All personnel with access to the information will be instructed of an acknowledge their understanding of the civil and criminal sanctions specified in state and Federal law for unauthorized use of the data. These acknowledgements must be maintained in a current status by the Requesting Party [City] and provided to the Providing Agency [HSMV] within (10) business days of a request."

The RM Department executed the MOU and submitted a Certification Statement to the HSMV on August 8, 2018 attesting that there were "appropriate internal controls in place to ensure that the data is protected from unauthorized access, distribution, use, modification or disclosure."

However, upon audit inquiry in January 2020, we found that the training required by the HSMV in MOU Section V, Part F and Part G was not provided to any employees with access to the information exchanged under the MOU. Three (3) employees in the RM Department have access to the information via the "CMIA Risk DL Process File and View Only" responsibility in the City's Oracle Enterprise Resource Planning (Oracle) system. Nineteen (19) City employees in other departments have access to additional Oracle responsibilities that provide the ability to view and change the information.

Finally, twenty (20) employees in the City's Department of Innovation and Technology (DoIT) have access to the information through shared folders on the City's network:

- Thirteen (13) individuals in DoIT have access to the network folders utilized by the file transfer protocol (FTP) process to send/receive the information to/from the HSMV.
- Seven (7) individuals in DoIT have access to the "Documents" network folder where RM Department personnel save the driver's license reports generated by the "CMIA Risk DL Process".

As a result of not providing the mandatory training and ensuring that data is protected from unauthorized access, the HSMV may terminate or suspend the MOU.

RECOMMENDATION 1.1: DEPARTMENT OF RISK MANAGEMENT

We recommend that the RM Department work with DoIT to review the population of all individuals with access to the driver's license information through the shared folders the City's network (the FTP process and Documents folders), determine the minimum number of individuals who require access to perform their job functions, and immediately remove access from those who do not require it.

- **Auditee Response**: The Documents folder was replaced by a secured network folder. Access to this folder and the FTP folders was removed from all individuals who do not require it for their minimum job functions. Two (2) individuals in DoIT were left with access, necessary for security and operational functions. Additionally, a new process to grant future access to these specific folders was implemented to ensure that access remains only on a least-needs basis.

- **Implementation Date**: Implemented, March 2021.

RECOMMENDATION 1.2: DEPARTMENT OF RISK MANAGEMENT

The RM Department should request that DoIT query the user responsibilities in the City's Oracle system to obtain the population of individuals with access to the information through Oracle responsibilities and immediately remove access from those who do not require it.

- **Auditee Response**: In March 2021, DoIT implemented new procedures for the recertification of user access to the Oracle system. The individuals and responsibilities with access to the Driver's License information were identified; and the personnel responding to the recertification were requested to specifically review and approve this access.

- **Implementation Date**: Implemented, March 2021.

RECOMMENDATION 1.3: DEPARTMENT OF RISK MANAGEMENT

We recommend that after access to driver's license information is removed from all individuals who do not require it, that the RM Department provide the training to all personnel with access, pursuant to MOU Section V, Parts F and G. Written evidence should be maintained for all individuals that have received the training.

- **Auditee Response**: Training pursuant to MOU Section V, Parts F and G was provided to all individuals with access to the information; and these individuals signed and submitted their training acknowledgements to the RM Department.

- **Implementation Date**: Implemented, March 2021.

FINDING 2: CONFIDENTIAL INFORMATION WAS TRANSMITTED IN A PROHIBITED MANNER

The MOU states in Section V. Safeguarding Information, "The Parties [City and HSMV] shall access, disseminate, use and maintain all information received under this MOU in a manner that ensures its confidentiality and proper utilization in accordance with Chapter 11, Florida Statutes, and DPPA." The Driver's Privacy Protection Act (DPPA), 18 United States Code §2721 defines "personal information" as information that identifies an individual, including, but not limited to name and driver identification number.

Florida Statute 501.171 - Security of confidential personal information, states in paragraph (1)(g)1. "'Personal information' means either of the following: a. An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual: (II) A driver license or identification card number."

Attachment III of the MOU, HSMV External Information Security Policy, #B-01: Acceptable Encryption, 4.0 Policy, states:

> "When possible, confidential information should not be transmitted via email. If confidential information must be sent via email, it shall be encrypted. Information resources that stores or transmits sensitive or confidential data must have the capability to encrypt information. Proven, standard algorithms must be used as the basis for encryption technologies. Encryption key lengths must be at least 128 bits. The Department key length requirements will be reviewed periodically and upgraded as technology, legislation, or business needs requires."

Information the City received from the HSMV under the MOU includes City employees' names, dates of birth, and driver's license numbers. However, during the course of our audit, we found that the RM Department sends confidential personal information exchanged under the MOU (City employees' names and driver's license numbers, issue and expiration dates; driver's license status, points, and violation details) via unencrypted email without warnings/indications that the email contains confidential information, on a monthly basis. The email is sent using the City's Microsoft Exchange email system to a member of the City's Fire Department.

As a result, the MOU may be terminated or suspended by the HSMV upon finding that the terms and conditions contained in the MOU have been breached by the City. Additionally, confidential information sent via unencrypted email could be intercepted or misdirected, leading to possible civil or criminal penalties.

RECOMMENDATION 2: DEPARTMENT OF RISK MANAGEMENT

The RM Department should determine if the Fire Department requires a detailed spreadsheet of personnel operating City-owned vehicles. Access to the detailed information should be immediately removed from Fire Personnel if not required. Otherwise, the minimum amount of information needed should be determined to verify that employees operating City vehicles have a valid driver's license.

- **Auditee Response**: The information needs were discussed with personnel in the Fire Department; and a new process was implemented so that the Fire Department will no longer be provided with the detailed spreadsheet. Instead, a memo will be sent which includes only employee name and driver's license status.

- **Implementation Date**: Implemented, March 2021.

FINDING 3: A PROCESS TO MONITOR AND ENSURE COMPLIANCE WITH THE MOU WAS NOT IMPLEMENTED

The RM Department executed the MOU with the HSMV and is required to implement a process to identify all requirements of the MOU and ensure they are adhered to, within specified timelines.

However, as indicated in Findings 1 and 2, the RM Department is not in compliance with all terms of the MOU. Additionally, HSMV personnel requested an Internal Control and Data Security Audit, pursuant to the MOU in 2019, and sent reminders to RM Department personnel in September 2019 and January 2020. However, RM did not notify the City's Office of the Independent Auditor General (OIAG), of the requested audit until January 2, 2020.

As a result of not implementing a process to identify and comply with all requirements of the MOU in a timely manner, the DHSMV may terminate or suspend the MOU and remove the City's access to state driver license information.

RECOMMENDATION 3: DEPARTMENT OF RISK MANAGEMENT

We recommend that the RM Department compile the requirements of the MOU into a checklist, assign an individual of appropriate skill and experience to fulfill each requirement, and implement internal controls and processes to ensure all requirements are complied with in a timely manner. Additionally, the RM Department should consider implementing Outlook calendar reminders to ensure that all time-sensitive requirements of the MOU are identified and addressed in accordance with deadlines.

- **Auditee Response**: The recommended checklist was implemented and the due dates for all MOU requirements and deliverables were noted.

- **Implementation Date**: Implemented, March 2021.

FINDING 4: ACTUAL USAGE OF INFORMATION OBTAINED EXCEEDED AGREED UPON USAGE UNDER THE MOU

The RM Department requested and received access to HSMV confidential driver's license information via the MOU. In Attachment I of the MOU, the RM Department provided the following reason for requiring access to the information:

> "Data will be used to adhere to Labor/Management policy requiring Citywide that an employee possess both a valid Florida DL and a satisfactory driving record when operating a City vehicle."

The City implemented Labor/Management Policy (LMP) 5-82 "Valid Florida Driver's License Requirement". The purpose of this LMP is "to provide an official policy pertaining to Citywide requirements that an employee possess both a valid Florida Driver's License and a satisfactory driving record when operating a City vehicle."

However, upon review of memoranda sent by the RM Department to City offices and departments, including the Office of the City Attorney; Parks and Recreation Department; Fire Department; Solid Waste Department; Civil Services; Department of Real Estate and Asset Management; Police Department; and Human Services, we found that each memorandum contained the following language:

> "Pursuant to APM 3-99, below is a list of employees in your department whose driver's licenses are not currently valid. Employees are not permitted to drive a City vehicle without a valid Florida driver's license. This also applies to employees who drive their personal vehicle on City business."

The description provided by the Department to HSMV in Attachment I of the MOU of how the information will be used is narrower in scope than how the Department actually uses the information in practice. The description states that the information will be used when an employee is "operating a City vehicle" which aligns to Labor/Management Policy 5-82. However, the RM Department's actual usage of the information obtained exceeded agreed upon usage since it is also used to review driving records and license status of employees who drive their personal vehicle on City business.

RECOMMENDATION 4: DEPARTMENT OF RISK MANAGEMENT

We recommend that the RM Department update their description of the usage of the information obtained under the data exchange with HSMV.

- **Auditee Response**: We have notified and confirmed with the HSMV that our usage of the information obtained under the data exchange has changed.

- **Implementation Date**: Implemented, March 2021.

FINDING 5: SECURITY ACCESS TO THE INFORMATION WAS NOT MONITORED ON AN ONGOING BASIS

The MOU between the City and the HSMV states in Section V. Safeguarding Information, Part H, "All access to the information must be monitored on an ongoing basis by the Requesting Party." Additionally, Attachment III to the MOU, the HSMV External Information Security Policy, #B-20 Security Monitoring and Auditing, 3.0 states,

> "Security monitoring will be used as a method to confirm that security practices, controls, policies are functional, adhered to, and are effective. Monitoring consists of activities such as the periodic review of: automated intrusion detection system logs, firewall logs, user account logs, network scan logs, application logs, data backup recovery logs. The Department shall use automated tools to provide real time notification of detected anomalies or vulnerability exploitation. These tools will be deployed to monitor network traffic and/or operating system security parameters."

Application logs should be used to monitor who accessed/viewed or modified the information exchanged under the MOU, as well as the time and date of user activity. On a regular basis (i.e., monthly) these "audit logs" of user activity should be reviewed by the data owner or designee; evidence of their review should be created and maintained for a reasonable amount of time, and any anomalous or suspicious activity should be promptly investigated. Incidents should be handled in accordance with the City's incident handling policies and procedures, in conformance with Florida Statutes, Section 501.171.

However, user access and activity in the logical locations where confidential information provided by the HSMV is stored in the City is not logged or reviewed. The information exchanged under the MOU is kept in network folders accessible by system accounts and thirteen (13) personnel in the DoIT. The information in these network folders is used by RM Department personnel to generate reports. The reports are saved to a different network folder, which is accessed by seven (7) personnel in DoIT. Activity in these folders is not monitored as required by the MOU; and is not logged or reviewed. Automated tools to monitor network traffic and/or operating system parameters and provide real time notification of detected anomalies or vulnerability exploitation has not been implemented.

Information exchanged under the MOU is also accessible via the Oracle system. Nineteen (19) City personnel outside of the RM Department have the ability to update driver's license records in the Oracle system. However, updates made to driver's license records through Oracle are not logged or reviewed; the only information captured through Oracle is the date of the users' last logon.

As a result, unauthorized access and changes to the information may occur and go undetected; and this lack of monitoring is a violation of the MOU. Consequently, the MOU may be terminated or suspended by the HSMV if left uncorrected.

RECOMMENDATION 5.1: DEPARTMENT OF INNOVATION AND TECHNOLOGY

To comply with the security requirements of the MOU and to ensure that information exchanged will be adequately safeguarded and not used for any purposes not specifically authorized by the MOU, we recommend that DoIT implement monitoring activities, including application and security

logs, and use automated tools to provide real time notification of detected anomalies or vulnerability exploitation. Anomalous or suspicious activity should be promptly investigated by applicable DoIT and RM Department personnel; and evidence of their review should be documented and maintained for a reasonable amount of time.

- **Auditee Response**: An automated tool (Change Auditor) was implemented to monitor user access and activity in the secured network folders where the Driver's License information exchanged under the MOU is kept. Automated alerts of anomalous activity are sent to Security Analysts, and data owners if applicable, for investigation. Security logs are reviewed on an ongoing basis and will be maintained for a minimum period of one (1) year.

- **Implementation Date**: Implemented, March 2021.

RECOMMENDATION 5.2: DEPARTMENT OF INNOVATION AND TECHNOLOGY

We recommend that DoIT implement incident handling policies and procedures, in conformance with the MOU and Florida Statutes, Section 501.171.

- **Auditee Response**: DoIT has prepared, approved and fully implemented the City's Incident Response Plan, which meets the requirements of the MOU and Florida Statutes, Section 501.171. The Incident Response Plan, along with all other data security policies/procedures were approved by a Risk Management IT Security Professional.

- **Implementation Date**: Implemented, March 2021.

FINDING 6: USER ACCESS TO INFORMATION OBTAINED UNDER THE MOU WAS NOT PROPERLY RECERTIFIED

According to the MOU, Section V. Safeguarding Information, Part E: "Access to the information received from the Providing Agency [DHSMV] will be protected in such a way that unauthorized persons cannot view, retrieve, or print the information." Additionally, Attachment III of the MOU, DHSMV's External Information Security Policy, Section #B-02: Access Control, Paragraph 2.0 Policy, Part 13 states, "The RM Department utilizes the principle of least privilege for access control to information resources. All External Entities shall be limited to the access required to do their assigned tasks." Finally, best practices state, "Owners of critical business data need to ensure that all application and database user entitlements and privileges are recertified on a periodic basis to make sure that only authorized individuals have access to the information."

The DoIT conducts periodic recertifications of user access to the City's Oracle system. Access to the Oracle system also provides certain responsibilities access to the driver's license information exchanged under the MOU. The most recent recertification listed 167 unique Oracle responsibilities and contained instructions to "Click on this link to see the descriptions of each responsibility." However, the link contained only 29 Oracle responsibilities with descriptions of the actions assigned to each, and 138 Oracle responsibilities without a corresponding description.

As a result, individuals responsible for attesting to the propriety of user access in the Oracle system are unaware of the functions of 138 responsibilities in the recertification as well as the information accessed by each responsibility, including whether or not the information is confidential or personal.

Further, information exchanged under the MOU is accessible via more Oracle responsibilities than is necessary, and access provided to the responsibilities is not based on the principle of least privilege. We found that in addition to the "CMIA Risk DL Process" Oracle responsibility used by personnel in the RM Department, the following five (5) additional Oracle responsibilities have access to "CMIA_Drivers_License" information exchanged under the MOU:

CMIA ER - Director (1 user, Risk Management Department)
CMIA ER - Director's Office (6 users, Human Resources Department)
CMIA ER - Testing and Validation (8 users, Human Resources Department)
CMIA ER Power User (1 user, Human Resources Department)
US Super HRMS Manager (4 users, Department of Innovation and Technology)

A total of 19 unique users have access through these five (5) Oracle responsibilities.

As a result, information exchanged under the MOU could be used for purposes not specifically authorized by the MOU. Unauthorized use includes, but is not limited to, queries not related to a legitimate business purpose, personal use, and the dissemination, sharing, copying or passing of this or any unauthorized information to unauthorized persons. Also, if the City is found to be non-compliant with the terms of the MOU, the HSMV may terminate or suspend the agreement.

RECOMMENDATION 6: DEPARTMENT OF INNOVATION AND TECHNOLOGY

We recommend that the Department of Information Technology add descriptions for the six (6) Oracle responsibilities with access to “CMIA_Drivers_License” information to the Oracle recertification in order for departmental personnel to know that these roles provide users with access to the Driver’s License information, prior to making recertification decisions.

- **Auditee Response**: DoIT prepared a list of all Oracle responsibilities having access to the Driver’s License information, and a list of all personnel who are responsible for recertifying user access to these responsibilities. During the March 2021 Oracle recertification, said list of Oracle responsibilities and descriptions of the data accessible through these responsibilities, were sent to the personnel required to recertify user access. Additionally, DoIT implemented an automated reminder to ensure that this list of responsibilities and data access descriptions are sent to recertifying personnel during the twice-yearly recertifications of user access to the Oracle system. Lastly, the recertification policies and procedures were updated to include the steps to query to the Oracle database to obtain current lists of responsibilities with access to the Driver’s License information at the start of each recertification.

- **Implementation Date**: Implemented, March 2021.

OTHER FINDINGS AND RECOMMENDATIONS

FINDING 7: THE CITY'S LABOR/MANAGEMENT POLICY WAS OUTDATED

During the course of our audit of the City's compliance with the MOU, we also reviewed the City policies underlying the RM Department's need for the driver's license information from the HSMV. These policies should be maintained and updated to reflect current operating processes and procedures. The City implemented Labor/Management Policy (LMP) 5-82 "Valid Florida Driver's License Requirement" to provide an official policy pertaining to Citywide requirements that an employee possess both a valid Florida Driver's License and a satisfactory driving record when operating a City vehicle. The RM Department cited this policy's purpose in Attachment I of the MOU when providing support to the HSMV for requesting access to the driver's license information maintained by the HSMV.

However, we found that LMP 5-82 "Valid Driver's License Requirement" has not been updated since October 21, 1994. The LMP describes an outdated process instead of the data exchange process and current communication process between the RM Department and other City offices and departments concerning the validation of driver's licenses and other related information.

The LMP states in Section 1. Obtaining Driver's License Violation Records:

> Part C, "Whenever the department determines that they need a Driver License Violation Record on one of their drivers or potential drivers, a green "Driver Information" card (attached) is to be completed and sent to the Safety Coordinator. The Safety Coordinator will send to Tallahassee for the desired record and will send the record and the green card back to the department when received."

This description does not reflect current operating processes in the City, since green "Driver Information" cards are no longer circulated internally among City departments (i.e., employee end-user departments and the Risk Management Department) or sent to Tallahassee along with a request for the Driver's License Violation Record. The process to obtain a Driver's License Violation Record on a City driver or potential driver falls under the electronic data exchange program between the City and the HSMV.

Also, the LMP states in Section 1, Part E, "The Driver's License records of these employees operating City vehicles will be reviewed every year or sooner, if necessary." The current process in the City is to review the Driver's License records of City employees on a bi-monthly basis. Although bi-monthly is "sooner" than a year, the LMP does not correctly reflect the current process.

Finally, we found that the City has a second policy that addresses driver's licenses, Administrative Policy Manual (APM) 3-99 "City Vehicle Assignment, Operation, 24-Hour Vehicle - City Employee Liability, Maintenance, Acquisition and Disposal." The APM's purpose is to "establish uniform policies and procedures for City of Miami employees who drive City-owned vehicles or their own personal vehicles for City business." The scope of APM 3-99 is broader than LMP 5-82 since it addresses both City employees who drive their own personal vehicles for City business in addition to City employees who drive City-owned vehicles. Lastly, APM 3-99 states, "The Department of

Risk Management shall conduct a “bi-monthly driver license record review” of all employees driving City vehicles" while LMP 5-82 states that the review will occur "every year or sooner.”

As a result, the City has two inconsistent policies covering the same subject matter. Without a relevant policy that is congruent with current operating processes, departmental personnel may not have the information necessary to make a decision about whether to approve personnel to operate City vehicles or use their own vehicle on City business. Consequently, employees with driver license violations, revocations or suspensions could expose the City to undue risk. Additionally, outdated policies may not incorporate current laws, regulations, technologies and best practices.

RECOMMENDATION 7: **DEPARTMENT OF HUMAN RESOURCES**

We recommend that the City consolidate LMP 5-82 into APM 3-99 and review and update APM 3-99 so that there is one, up-to-date City policy document that reflects current operating processes and procedures.

- **Auditee Response**: The LMP requires the participation and agreement of the unions, therefore they are not easily amended or updated. Additionally, if all 4 unions do not agree to the required changes necessary to the LMP, HR will only be able to update APM 3-99.

- **Implementation Date**: As you are aware, the City is currently undergoing fiscal constraints that have become the City and the Unions top priority. HR will do our best to consolidate the two policies. However, please know that due to the fiscal constraints and the coronavirus it may take time to obtain input and agreement from all the necessary parties. HR may not be able to implement the above requirement until mid-year 2021.