MOBILITY DEPARTMENT
PARKING DIVISION
FLHSMV DATA EXCHANGE MOU
AUDIT 23-08
FEBRUARY 16, 2023

City of Tampa
Jane Castor, Mayor

Internal Audit Department
315 E. Kennedy Boulevard
Tampa, Florida 33602
Office (813) 274-7159

February 16, 2023

Honorable Jane Castor
Mayor, City of Tampa
1 City Hall Plaza
Tampa, Florida

RE: Memorandum of Understanding for Driver's License and/or Motor Vehicle Record Data Exchange, Audit 23-08

Dear Mayor Castor:

Attached is the Internal Audit Department's report on the Florida Highway Safety and Motor Vehicles Data Exchange Memorandum of Understanding (MOU).

The internal controls governing the use and dissemination of personal data have been evaluated considering the requirements of the MOU and applicable laws. Based on this review, the internal controls are adequate to protect the personal data from unauthorized access, distribution, use, modification, or disclosure. This includes both policies/procedures in place for personnel to follow and data security procedures/policies in place to protect personal data. Internal Audit certifies that the data security procedures/policies have been approved by a Risk Management IT Security Professional.

We thank the management and staff of the Parking Division for their cooperation and assistance during this audit.

Sincerely,

/s/ Christine Glover

Christine Glover, MS, MBA, CIA, CFE, CGAP
Internal Audit Director

cc: John Bennett, Chief of Staff
Jean Duncan, Administrator of Infrastructure and Mobility
Dennis Rogero, Chief Financial Officer
Vik Bhide, Mobility Director
Russell Haupert, Chief Technology Officer
Fed Revolte, Parking Division Manager
Carl Brody, Assistant City Attorney

MOBILITY DEPARTMENT
PARKING DIVISION
FLHSMV DATA EXCHANGE MOU
AUDIT 23-08

/s/ Vivian N Walker

Vivian N Walker, MPA, CGAP, CICA
Lead Senior Auditor

/s/ Christine Glover

Christine Glover, MS, MBA, CIA, CFE, CGAP
Audit Director

/s/ Jane Castor

Honorable Jane Castor
Mayor

MOBILITY DEPARTMENT
PARKING DIVISION
FLHSMV DATA EXCHANGE MOU
AUDIT 23-08

BACKGROUND

The Parking Division (Division) of the Mobility Department is responsible for the operation of all City of Tampa (City) public parking. The Division develops parking policy and specific facility expansion plans to serve the parking demand in the central business district and adjacent commercial areas. The Division's processes require an exchange of information; motor vehicle tag information is forwarded to the Florida Department of Highway Safety and Motor Vehicles (FLHSMV) and data is accessed from the Driver and Vehicle Information Database (DAVID).

The audit was conducted pursuant to Section VI., Compliance and Control Measures, Part A, Internal Control and Data Security Audit, Memorandum of Understanding (MOU) between the FLHSMV and the City of Tampa-Mobility-Parking Division, adopted on January 28, 2022. The MOU requires that continued access to personal data by the Division is contingent upon appropriate internal controls to protect data received from the FLHSMV from unauthorized access, distribution, use, modification, or disclosure. City Council adopted the MOU, by issuing Resolution 2022-59, accepting the requirements documented in the MOU.

STATEMENT OF OBJECTIVES

This audit was conducted upon the request from the Management of the Infrastructure and Mobility Department. The objectives of the audit were to assess that:

1. Internal controls, including policies and procedures, are adequate to ensure the use and dissemination of personal data are protected from "unauthorized access, distribution, use, modification, or disclosure."

2. Data security procedures/policies have been approved by a Risk Management IT Security Professional.

3. Employee access is appropriate for job responsibilities and is routinely monitored.

4. Data obtained from DAVID was for a valid reason.

5. Employees are trained and made aware of information security best practices.

6. The transport layer security version used as the encryption protocol, during transmission of FLHSMV data, is at least 1.2.

7. Security patches and updates are installed on the Division's computers in a timely manner.

8. There is a formal information security event reporting policy and procedure.

9. The IT Infrastructure Disaster Recovery Plan includes the Division's systems that contain parking violation data.

STATEMENT OF SCOPE

The audit scope covered DAVID user activity from January 2022 through December 2022. Both qualitative and quantitative assessments were performed to determine if the Division was fulfilling its stated duties and responsibilities as required by Section VI. Of the MOU. A data reliability analysis for completeness of information generated by DAVID was performed during the previous audit (21-04 Parking Data Exchange). Original records as well as copies were used as evidence and verified through observation and physical examination.

STATEMENT OF METHODOLOGY

The following steps were performed to determine compliance with the stated objectives:

- Interviewed both the Parking Division Manager and the City's Security Officer.
- Reviewed data security protocols and other information security documentation to evaluate compliance with cybersecurity requirements.
- Reviewed authorized DAVID user list to ensure only current Division employees had access.
- Reviewed user access and traced to supporting documentation of a parking violation.
- Reviewed documentation maintained to support periodic monitoring of user access by Technology & Innovation Department personnel.

STATEMENT OF AUDITING STANDARDS

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.

AUDIT CONCLUSIONS

Based upon the test work performed, we conclude that:

1. Internal controls, including policies and procedures, are adequate to ensure the use and dissemination of personal data are protected from "unauthorized access, distribution, use, modification, or disclosure."
2. Data security procedures/policies have been approved by a Risk Management IT Security Professional.
3. Employee access is appropriate for job responsibilities and is routinely monitored.

4. Data obtained from DAVID was for a valid reason.

5. Employees are trained and made aware of information security best practices.

6. The transport layer security version used as the encryption protocol, during transmission of FLHSMV data, is at least 1.2.

7. Security patches and updates are installed on the Division's computers in a timely manner.

8. There is a formal information security event reporting policy and procedure.

9. The IT Infrastructure Disaster Recovery Plan includes the Division's systems that contain parking violation data.