City of Miami

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

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

May 27, 2022

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

Re: Audit of Driver and Vehicle Information Database System Data Security
Report No. 22-06

Executive Summary

We have completed an audit of the City of Miami's (City's) Department of Risk Management's (RM) compliance with requirements set forth in the Memorandum of Understanding (MOU) between the RM and the Florida Department of Highway Safety and Motor Vehicles (HSMV). The MOU provides RM personnel with access to the HSMV's Driver and Vehicle Information Database (DAVID) system, effective December 26, 2018 for a period of six (6) years. Our audit primarily covered the period from October 1, 2020 through September 30, 2021.

The objectives of the audit were to assess whether the City's internal controls complied with the requirements set forth in *Section V – Safeguarding Information*, of the MOU. We tested the design and operating effectiveness of internal controls over access to the DAVID system; use of data; protection of information, applications, resources, services, and data in electronic and physical formats; and compliance with the City's information security policies. As a result of the audit, we did not identify any observations that should be addressed in order to enhance RM's compliance with the data security requirements of the DAVID MOU.

We wish to express our appreciation for the cooperation and courtesies extended to us during the audit by personnel in RM and the City's Department of Innovation and Technology.

Sincerely,

Theodore P. Guba

Theodore P. Guba, CPA, CIA, CFE
Independent Auditor General
Office of the Independent Auditor General

C: The Honorable Mayor Francis Suarez
Art Noriega, V, City Manager
Nzeribe Ihekwaba, Deputy City Manager
Victoria Mendez, City Attorney
Todd Hannon, City Clerk
Fernando Casamayor, Assistant City Manager/Chief Financial Officer
Natasha Colebrook Williams, Assistant City Manager
Ann-Marie Sharpe, Director, Risk Management Department
Otto Contreras, Assistant CIO/Assistant Director, Department of Innovation and Technology
Members of the Audit Advisory Committee
Audit Documentation File

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

Audit reviewed by: Mala Khilnani, CPA, CISA, Audit Supervisor

AUDIT OF DRIVER AND VEHICLE INFORMATION DATABASE SYSTEM DATA SECURITY

OCTOBER 1, 2020 THROUGH SEPTEMBER 30, 2021

REPORT No. 22-06

TABLE OF CONTENTS

SCOPE, OBJECTIVES AND METHODOLOGY

The scope of the audit was to assess the City's internal controls applicable to the information security requirements set forth in Section V – Safeguarding Information, of the MOU. The MOU was effective on December 26, 2018, for a period of six (6) years. Our audit primarily covered the period from October 1, 2020 through September 30, 2021 and focused on the following objectives:

- To evaluate the internal controls protecting the personal data received from the DAVID system from unauthorized access, distribution, use, modification, or disclosure.
- To determine whether internal controls related to the following areas are properly designed and operating effectively:
    - access to the DAVID system.
    - protection of DAVID's applications, resources, services, and information.
    - disposal of printed information from DAVID.
    - compliance with the City's and other applicable information security policies.
- To ensure that any deficiencies found during the audit were remediated and that measures were implemented to prevent their reoccurrence.

The methodology of the audit included:

- Reviewing the DAVID MOU between RM and the HSMV.
- Reviewing the City's policies and procedures related to the safeguarding of electronic and physical data transfers, data storage and data access.
- Interviewing key personnel to understand the DAVID processes.
- Testing internal controls related to the requirements of the MOU.
- Detailed testing of relevant records, reports, and activities.
- Verifying that management has implemented corrective actions for deficiencies identified in prior audits.
- 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 states that City employees driving City vehicles must possess 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 RM shall conduct a bi-monthly review of the Driver's License status of all employees operating a motor vehicle in the course of City business.

To review the Driver's License status pursuant to APM 3-99, RM executed Memorandum of Understanding (MOU) HSMV-0310-19 with the Florida Department of Highway Safety and Motor Vehicles (HSMV) for access to HSMV's Driver and Vehicle Information Database (DAVID) system. The MOU was effective on December 26, 2018, for a period of six (6) years.

Section V – Safeguarding Information, of the MOU states that the information provided to RM by HSMV is confidential and information security requirements are provided. Section VI – Compliance and Control Measures, of the MOU states that RM must submit an Attestation Statement from the City's Internal Auditor on or before the third and sixth anniversary of the MOU; the Attestation Statement shall indicate that the internal controls over personal data have been evaluated and are adequate to protect the persona l data from unauthorized access, distribution, use, modification, or disclosure. The Attestation Statement shall also certify that any and all deficiencies/issues found during the review have been corrected and measures enacted to prevent recurrence. RM management requested that our Office perform the attestation; this report contains the results of our audit of the controls in place pursuant to the MOU.

AUDIT CONCLUSION

As a result of the audit, we did not identify any observations that should be addressed in order to enhance RM's compliance with the data security requirements of the DAVID MOU.

Summary Schedule of Internal Controls Tested

Department of Risk Management Controls		
Control Type	**Control Descriptions**	**Testing Results**
Access Provisioning	▪ RM personnel maintain a list in current status of all persons authorized to access DAVID information. ▪ Access is granted on a least-needs basis. ▪ Access is promptly removed when no longer required. ▪ Access to the system is reviewed and recertified on a semi-annual basis.	Controls are Effective
Data Security	▪ Acknowledgements of the criminal and civil penalties for any and all misuse of DAVID information are kept in a current status. ▪ Information from DAVID is not printed or maintained in hardcopy format. ▪ A designated location has been established as the only place for information from HSMV. ▪ The designated location is secured to prevent unauthorized persons from viewing, retrieving, or printing the information, and activity is logged. ▪ Physical access to data assets is controlled by key badge readers, CCTV monitoring and security guards.	Controls are Effective
User Training & Compliance	▪ All users with access to the DAVID system have been provided with training on the confidentiality and proper utilization of DAVID data in accordance with the MOU. ▪ Quarterly Quality Control Reviews ▪ Internal Control Attestations are requested as needed.	Controls are Effective

Department of Innovation and Technology Controls		
Incident Response	▪ The Department of Innovation and Technology (DoIT) has implemented formal Incident Response plans and procedures.	Controls are Effective.
Network Logging and Monitoring	▪ Logging and auditing functions are enabled on all in-scope entities; and system logs are monitored for unauthorized access and irregular activity. ▪ Automated mechanisms to monitor system capacity and data integrity have been implemented.	Controls are Effective.
Change Management	▪ Changes are documented, tested, and classified prior to implementation to identify the effects of changes within the environment.	Controls are Effective.
Backup and Redundancy	▪ Backup and restoration procedures have been established and are tested periodically.	Controls are Effective.
Physical and Logical Security	▪ Access to physical devices is restricted to authorized individuals and additional integrity monitoring is in place to detect changes to critical system files associated with hardware devices. ▪ At data centers, badge access and cameras have been implemented. ▪ Firewalls, file integrity, and antivirus software have been implemented to restrict unauthorized software and access to the internal network. ▪ Active Directory authentication is utilized	Controls are Effective.
System Maintenance	▪ Hardware is maintained in accordance with its useful life, and a patch management policy is in place.	Controls are Effective.
Policies and Procedures	▪ DoIT has identified regulatory requirements and individuals responsible for managing requirements. ▪ A risk assessment process has been implemented to monitor and facilitate improvement of security controls currently in place. ▪ DoIT has implemented policies and procedures to ensure proper requirements are addressed during procurement activities.	Controls are Effective.