Audit of Driver and Vehicle Information Database Usage by the Resilient Environment Department Consumer Protection Division

Office of the County Auditor

Audit Report

Robert Melton, CPA, CIA, CFE, CIG
County Auditor

Audit Conducted by:
Kathie-Ann Ulett, CPA, CFE, Deputy County Auditor
Gerard Boucaud, CIA, CISA, CDPSE, Audit Manager
Luis Martinez, CISA, CDPSE, CFE, Information Technology Audit Supervisor

Report No. 25-09
February 6, 2025

OFFICE OF THE COUNTY AUDITOR
115 S. Andrews Avenue, Room 520 • Fort Lauderdale, Florida 33301 • 954-357-7590 • FAX 954-357-7592

February 6, 2025

Honorable Mayor and Board of County Commissioners

At the request of management, we conducted an audit of the internal controls over the Broward County Resilient Environment Department (RED), Consumer Protection Division's (CPD) access and usage of the Driver and Vehicle Information Database (DAVID) provided by the Florida Department of Highway Safety and Motor Vehicles (FLHSMV).

The objectives of our audit were to determine whether the use of DAVID complies with the terms of the Memorandum of Understanding (MOU) with the FLHSMV, and to determine whether the internal controls safeguarding the use and dissemination of personal data are adequate to prevent unauthorized access, distribution, or modification, in accordance with the MOU and relevant legal requirements.

We conclude that the use of DAVID complies with the terms of the MOU with the FLHSMV. We conclude that, except as noted in this report, internal controls over personal data are adequate to prevent unauthorized access, distribution, or modification, in accordance with the MOU and relevant legal requirements.

We appreciate the cooperation and assistance provided by the Consumer Protection and Enterprise Technology Services Divisions throughout the course of our audit.

Respectfully submitted,

Bob Melton
County Auditor

cc: Monica Cepero, County Administrator
Andrew Meyers, County Attorney
Dr. Kimm Campbell, Deputy County Administrator
Lenny Vialpando, Director Resilient Environment
Philip McChesney, Director Consumer Protection

TABLE OF CONTENTS

INTRODUCTION

Scope and Methodology

The County Auditor's Office conducts audits of Broward County's entities, programs, activities, and contractors to provide the Board of County Commissioners, Broward County's residents, County management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

At the request of the Resilient Environment Department (RED), Consumer Protection Division (CPD), we conducted an audit of the of the internal controls over the Division's access and usage of the Driver and Vehicle Information Database (DAVID) provided by the Florida Department of Highway Safety and Motor Vehicles (FLHSMV). Our audit objectives were to determine whether:

- The use of the Data Exchange complies with the terms of the MOU with FLHSMV
- Internal controls safeguarding the use and dissemination of personal data are adequate to prevent unauthorized access, distribution, or modification, in accordance with the MOU and relevant legal requirements.
- Any opportunities for improvement exist.

To determine whether the use of DAVID complies with the terms of the MOU, we reviewed all users with access to the data both physically and electronically for appropriateness based on job responsibilities and that no data was shared with parties not subject to the MOU. We reviewed employee acknowledgements of policies and procedures on confidentiality and criminal sanctions. We reviewed a sample of the type of searches performed by system users to evaluate that data exchange data is used only for the expressed purposes described in the MOU.

To determine whether Internal controls safeguarding the use and dissemination of personal data are adequate to prevent unauthorized access, distribution, or modification, in accordance with the MOU and relevant legal requirements we reviewed internal control and data security procedures against the requirements of the MOU, we obtained and reviewed password configurations, assessed general and application controls, inspected user administration, change management policies, physical security, and monitoring procedures.

We conducted this audit in accordance with Generally Accepted Government Auditing Standards except for the requirement for an external peer review which is planned for the current fiscal

year. The standards require that we plan and perform the audit to obtain sufficient and 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 conclusions based on our audit objectives.

Our audit included such tests of records and other auditing procedures as we considered necessary in the circumstances. The audit period was April 1, 2022, through January 14, 2025. However, transactions, processes, and situations reviewed were not limited by the audit period.

Overall Conclusion

We conclude that the use of DAVID complies with the terms of the MOU with the FLHSMV. We conclude that, except as noted in this report, internal controls over personal data are adequate to prevent unauthorized access, distribution, or modification, in accordance with the MOU and relevant legal requirements.

Background

In March 2022, the Broward County Consumer Protection Division (CPD) renewed the Memorandum of Understanding (MOU) with Department of Highway Safety and Motor Vehicles (FLHSMV) to obtain access to the Driver and Vehicle Information Database (DAVID), which provides remote electronic access to driver license and motor vehicle information.

Personal information contained in motor vehicle or driver license records is confidential and exempt from disclosure under the Driver's Privacy Protection Act, 18 United States Code section 2721. Personal information in a motor vehicle or driver's license record includes, but is not limited to, social security numbers, driver's license or identification numbers, name, address, medical, disability information. Personal information does not include information related to driving violations and driver status. The MOU has requirements to ensure the physical and logical security of the information. These requirements include, but are not limited to, inactivation of terminated users, acknowledgements of information confidentiality as well as criminal sanctions for confidentiality violations, professional use of the information, annual user training, and periodic reviews and audits of user activity.

CPD's DAVID Usage

Pursuant to Section 119.0712(2), Florida Statutes, as outlined in 18 United States Code, section 2721, personal information in motor vehicle and driver license records can be released:

> *For use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a Federal,*

State, or local agency in carrying out its functions.

CPD is a government agency who at the time of our review utilized the data to identify alleged violators of the Broward County Code of Ordinances and to proceed with the appropriate enforcement action. Broward County will also use DAVID for oversight of the Electric Vehicle Charging Station program to identify alleged violators and unauthorized usage.

OPPORTUNITIES FOR IMPROVEMENT

Our audit disclosed certain policies, procedures and practices that could be improved. Our audit was neither designed nor intended to be a detailed study of every relevant system, procedure, or transaction. Accordingly, the Opportunities for Improvement presented in this report may not be all-inclusive of areas where improvement may be needed.

1. DAVID Information is Released to an Entity not Authorized Under the MOU.

DAVID information is released to the Broward County Clerk of Courts (Clerk of Courts) and subsequently posted on their public-facing website. The Resilient Environment Department (RED) works with the Clerk of Courts to process citation payments, which currently involves posting unredacted citations online. We observed instances where posted citations included protected personal information, such as driver license numbers, names, and addresses, as defined by the FLHSMV Driver Privacy Protection Act.

MOU Section IV.B.5 states that the Requesting Party agrees to, not share, provide, or release any DAVID information to any law enforcement, other governmental agency, person, or entity not a party or otherwise subject to the terms and conditions of this MOU.

Noncompliance with the MOU could result in immediate revocation of access to the DAVID information. Additionally, the release of personal information publicly poses significant risks, including identity theft, privacy invasion, financial fraud, reputation damage, and safety risks.

We recommend management seek FLHSMV's guidance on maintaining MOU compliance. This may involve updating the MOU or adjusting the business process.

Implementation Status: Remediation in Progress (See Appendix A: Remediation Status)

2. User Access to DAVID Information was not Consistently Authorized as Required by the MOU.

User access to DAVID information was not consistently authorized as required by the MOU. RED agencies stored DAVID information for enforcement activities in electronic repositories which were accessible by unauthorized employees. This situation arose because management was unaware of the various locations where the information was retained and lacked a clear policy on information storage requirements.

The FLHSMV External Information Security Policy (EISP) (Section B-02, 2.0, 5) mandates that each user must agree in writing to utilize access solely for its intended purpose. Furthermore, Section A-02, 3.0 of the policy requires that all users with access to the information be uniquely identified, authenticated, and authorized.

The MOU stipulates that all parties must maintain the confidentiality of all information received. Section V emphasizes that the willful and knowing disclosure of any information in violation of the agreement can result in both criminal and civil penalties.

Without adequate oversight, management may be unaware of the full extent of access granted, potentially exceeding the principle of least privilege and increasing security risks. Excessive access heightens the chances of unauthorized modification, misuse of information, and significant damage if a user's account is compromised.

We recommended management limit DAVID access to individuals with a legitimate business need, and ensure all employees with access to the information have been authorized to access the information retained, have acknowledged in writing the intended use, the confidential nature of DAVID data, and the potential civil and criminal penalties for unauthorized use.

Additionally, we recommended management enhance the existing DAVE/DAVID Standard Operating Procedure (SOP) to direct users on designated data repositories where data must be stored and limit access to those locations, while clearly prohibiting sensitive data entry into unprotected areas.

Implementation Status: Remediated (See Appendix A: Remediation Status)

3. Logical Access Controls Require Enhancement to Comply with the MOU.

During our review of access controls designed to safeguard DAVID information we noted the following:

A. The database and various data repositories used to store DAVID information are not encrypted in accordance with the FLHSMV's EISP Section B-01, 4.0.

B. The settings for failed login attempts were not configured according to the FLHSMV's EISP Section A-04, 2.0.10.

C. While workstation password authentication and lockout settings were enabled, the inactivity timeout was not configured according to EISP Section A-04, 2.0.9.

Failing to adhere to FLHSMV regulations may result in the immediate revocation of data exchange access. Moreover, inadequate failed login attempt settings elevate the risk of an unauthorized access e.g. allowing a hacking technique where an attacker attempts to gain access to a system

by systematically trying every possible combination of passwords, encryption keys, or login credentials until they find the correct one. In addition, an inadequate lockout period can create more opportunities for unauthorized individuals to access an unattended workstation.

We recommend management establish user access controls that fully adhere to FLHSMV requirements, including:

A. databases and file repository encryption,

B. failed login attempts and

C. workstation inactivity lockout settings.

Implementation Status: Partially Remediated (See Appendix A: Remediation Status)

4. Access to DAVID was not Consistently Revoked Timely as Required by the MOU.

Access to the DAVID system was not immediately disabled upon termination for one of the five employees whose access was revoked during the audit period. Specifically, one terminated employee's access was revoked five days after their termination. Management informed us that this was caused by a delayed communication to the DAVID administrator. While the user's access was not revoked timely, we noted the account was not used to access the system after the account holder's termination.

MOU Section IV.B.8 includes the following criteria: "Immediately inactivate user access/permissions following termination or the determination of negligent, improper, or unauthorized use or dissemination of information and to update user access/permissions upon reassignment of users within five (5) business workdays.

Failure to revoke access for terminated users results in non-compliance with the MOU's requirements, which can result in management losing access to DAVID information. Additionally, failure to revoke access timely increases the risk of data breaches, data theft, and regulatory non-compliance. Accounts that belong to terminated users become possible entry points for malfeasance, including data theft.

We recommended management re-issue DAVID policy and procedures to agency compliance point of contacts to reinforce required timelines and ongoing compliance.

Implementation Status: Remediated (See Appendix A: Remediation Status)

APPENDIX A: REMEDIATION STATUS

During our audit, as required by the MOU, we performed procedures to certify that all deficiencies/issues found during the review have been corrected and measures enacted to prevent recurrence. The following table shows the Opportunities for Improvement identified during the audit and along with its remediation status.

OFI NO.	Opportunity for Improvement (OFI)	Has the OFI Been Corrected?	Corrective Action Taken	Date of Corrective Action	If not Corrected, Estimated Date of Completion
1.	DAVID Information was Released to an Entity not Authorized Under the MOU.	No	Management contacted FLHSMV for an opinion, and FLHSMV confirmed that the inquiry is under review by upper management. As of January 2025, management is still awaiting a response.	N/A	See OFI No. 1
2.	User Access to DAVID Information was not Consistently Authorized as Required by the MOU.	Yes	Access has been restricted following the principle of least privilege. Management has created controlled and secured environments for DAVID information storage, with corresponding access controls in place. Additionally, management has authorized user access and obtained acknowledgment forms from all users accessing DAVID information stored outside the DAVID system.	January 14, 2025	

OFI NO.	Opportunity for Improvement (OFI)	Has the OFI Been Corrected?	Corrective Action Taken	Date of Corrective Action	If not Corrected, Estimated Date of Completion
3.	Logical Access Controls Require Enhancement to Comply with the MOU.	Partially	A. Management has established encrypted file repositories for storing electronic documents. Additionally, management plans to implement database encryption for DAVID information within the RED system of record for enforcement activities by March 2025. (Not Remediated) B. Failed login lock settings have been configured according to (EISP) Section A-04, 2.0.10. (Remediated) C. Workstation inactivity settings have been configured according to EISP Section A-04, 2.0.9. (Remediated)	B & C. November 14, 2024	A. March 2025
4.	Access to DAVID was not Consistently Revoked Timely as Required by the MOU.	Yes	Management re-issued the DAVID policy and procedures to agency compliance point of contacts reinforcing the required timelines and ongoing compliance.	December 3, 2024	