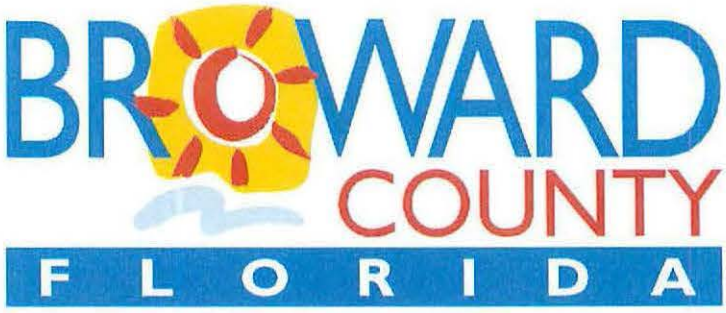
Exhibit 1




# Audit of Driver and Vehicle Information Database Usage by the Risk Management Division

## Office of the County Auditor

### Audit Report

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

Audit Conducted by:
Gerard Boucaud, CISA, Audit Manager
Muhammad Ramjohn, Staff Auditor

**Report No. 18-28**
**August 31, 2018**

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

August 31, 2018

Honorable Mayor and Board of County Commissioners

At the request of management, we conducted an audit of the of the internal controls over Risk Management Division's access and usage of the Driver and Vehicle Information Database (DAVID) system provided by the Florida Department of Highway Safety and Motor Vehicles (DHSMV).

The objective of our review was to determine whether the use of the DAVID system complies with the terms of the Memorandum of Understanding with DHSMV along with the adequacy of internal controls to ensure compliance.

Except as noted in our report, we conclude that the use of DAVID complies with the terms of the Memorandum of Understanding with DHSMV, and internal controls are adequate to ensure compliance.

We conducted this 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.

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

Respectfully submitted,

Bob Melton
County Auditor

cc: Bertha Henry, County Administrator
Andrew Meyers, County Attorney
Monica Cepero, Deputy County Administrator
George Tablack, Chief Financial Officer
Wayne Fletcher, Director Risk Management
Roger Moore, Assistant Director Risk Management

# TABLE OF CONTENT

# 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 management, we conducted an audit of the of the internal controls over Risk Management Division's access and usage of the Driver and Vehicle Information Database (DAVID) system provided by the Florida Department of Highway Safety and Motor Vehicles (DHSMV). Our audit objectives were to determine whether:

1. The use of the DAVID system complies with the terms of the Memorandum of Understanding with DHSMV along with the adequacy of internal controls to ensure compliance.
2. Any opportunities for improvement exist.

To determine whether the use of the DAVID system complies with the terms of the Memorandum of Understanding along with the adequacy of internal control to ensure compliance, we obtained and reviewed user requirements, including review of the Memorandum of Understanding and audit guidelines, reviewed employee acknowledgements of policies and procedures on confidentiality and criminal sanctions. We inspected quality control reviews and user rights, duties or obligations documentation. We validated information usage, user access permissions, and the security of information storage.

We conducted this 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.

Our audit included such tests of records and other auditing procedures as we considered necessary in the circumstances. The audit period was July 1, 2017 through June 30, 2018. However, transactions, processes, and situations reviewed were not limited by the audit period.

## Overall Conclusion

Except as noted in our report, we conclude that the use of DAVID complies with the terms of the Memorandum of Understanding with DHSMV, and internal controls are adequate to ensure compliance.

## Background

In December 2014, the Risk Management Division (RMD) entered into a Memorandum of Understanding (MOU) with Department of Highway Safety and Motor Vehicles (DHSMV) to obtain access to the Driver and Vehicle Information Database (DAVID), which provides information relating to driver records and motor vehicle information and history. This agreement was renewed in February 2018 giving the RMD continued access to DAVID for an additional six years.

As the information provided in DAVID is confidential, the MOU has requirements to ensure the 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.

### Risk Management Division's DAVID Usage

Pursuant to section of 119.0712(2), Florida Statute, 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.*

RMD, a division of the Finance and Administrative Services Department (FASD), uses DAVID to perform the following:

- Verify candidate employee information.
- Verify current and candidate employee driver license status.
- Verify vehicle insurance requirements.
- Perform Vehicle Identification Number (VIN) searches.

RMD had a total of nine active users in the DAVID system during the audit period; two of these users were made inactive during the period. Active users can request, view, and print drivers'

license and vehicle information. Each request made through DAVID is logged and stored by the system indefinitely. One user is registered as the Point of Contact (POC) with the DHSMV for RMD. The POC can approve access to the system, assign user roles, deactivate terminated employees and perform reviews of user activity.

# 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. Information Obtained From DAVID Should be Used For Legitimate Business Purposes Only.

During our review of personal information requests in DAVID, we noted the following concerns:

A. On two separate occasions within the audit period, one user utilized their DAVID access to perform searches for a relative and close friend for personal reasons in violation of the MOU, which states:

> *"Information Exchanged will not be used for any purpose not specially authorized by this MOU. Unauthorized use includes, but is not limited to, queries not related to a legitimate business purpose, business use, personal use, or the dissemation, sharing, copying or passing of this information to unauthorized persons."*

Although these situations appear to be isolated instances, misuse of DAVID database increases the County's legal risk and may lead to the revocation of access to DAVID and unilateral termination of the MOU by the DHSMV.

B. For eight of 60 (13%) searches reviewed, evidence supporting the business justification for the search was not retained. Upon further inquiry with management, we noted that these searches pertained to validating employee driver's license status based on a report from the SHIELD application; however, these reports are not retained to provide justification for the search performed. Without the maintenance of appropriate evidence to support the business justification for searches, management is unable to demonstrate compliance with MOU requirements and inappropriate searches may remain undetected.

**We recommend** management:

A. Implement appropriate procedures to ensure the DAVID database is used for legitimate business purposes related to RMD's objectives.

B. Ensure that appropriate documentation is maintained and retained to support the business justification for DAVID searches.

## 2. Quarterly Quality Control Reviews Should be Performed, Documented and Retained in Accordance With DHSMV's Audit Guidelines.

During our evaluation of the Quarterly Quality Control Review process, we noted the following concerns:

A. Appropriate segregation of duties are not enforced to ensure the integrity of the review. We noted quality control reviews are performed by the Program Manager, who is a frequent user of DAVID. This combination of responsibilities creates a conflict as this individual is potentially reviewing his or her own activity. Segregation of duties is a preventive control designed to preclude improper activity and is essential to ensure that errors or irregularities are detected timely during the normal course of business. Failure to implement appropriate segregation of duties increase the risk of error and inappropriate activity.

B. Adequate documentation of the quality control reviews is not created or maintained by management in order to demonstrate management's due diligence activities. The MOU requires that, effective February 2018, the quality control review report must be documented within 10 days after the end of each quarter and maintained for two years. Without adequate documentation of quarterly control reviews, management is unable to demonstrate compliance with specific requirements of the MOU increasing the County's legal risk.

C. Employees have the ability to access DAVID over the internet from computers outside of the County's network; however, the quality control review does not include procedures to monitor this activity. Employees should only access DAVID information from outside of the County's network when authorized by management. Failure to periodically monitor the location (IP Address) from which DAVID is accessed increases the risk that inappropriate activity may remain undetected.

**We recommend** management:

A. Ensure job duties are adequately segregated to help ensure errors and irregularities are prevented or detected on a timely basis.

B. Document the results of quarterly quality control reviews in accordance with the requirements of the MOU.

C. Enhance quality control review procedures to include a review of the location from which DAVID is accessed. Management should investigate any such occurrences and document the outcome.

## 3. Individuals With Access to DAVID and DAVID Data Stored on County Systems Should Acknowledge the Confidentiality of the Information and Criminal Sanctions for Unauthorized Use.

During our review of employee confidentiality acknowledgements, we noted the following concerns:

A. Two of 7 (29%) active DAVID users have not formally acknowledged their understanding of the confidential nature of the information and criminal sanctions for unauthorized use.

B. Two of 6 (33%) users with access to DAVID data transferred to County Systems have not formally acknowledged their understanding of the confidential nature of the information and criminal sanctions for unauthorized use.

The MOU requires the County to protect and maintain the confidentiality and security of the data received from the DHSMV. Formal acknowledgement of the confidentiality of the information and criminal sanctions for unauthorized use assists management in demonstrating its due diligence and responding to violations of confidentiality by employees.

**We recommend** management ensure all users with access to DAVID and DAVID data stored on County systems formally acknowledge their understanding of the confidential nature of the information and the criminal sanctions for unauthorized use.

## 4. Physical Security Controls Should be Enhanced to Adequately Protect Confidential Information.

Risk management uses combination door locks to restrict access to workstation areas; however, we noted that procedures have not been implemented to periodically change the combination lock. As a result, management has not changed the combination lock in the past four years. Broward County IT Administration Policy Volume 7: Chapter 3, Section 4.2 requires access rights to secure areas be revoked immediately for personnel terminated or who no longer require access. Combinations to locks must be changed. Failure to periodically change combination locks increase the risk of inappropriate access to confidential data.

**We recommend** management implement a process to periodically change combination locks. Management should maintain a log of these changes.

## 5. Terminated Employee Access Should be Revoked Immediately Upon Termination.

One employee retained access to DAVID for 30 days after their termination from the County. The MOU requires that employee access be immediately deactivated following termination. Terminated employee access to DAVID may result in a breach of confidential information and violate the terms of the MOU. Upon further review, we noted that the employee did not access DAVID after the termination date.

**We recommend** management ensure that appropriate procedures are in place to immediately disable terminated employee access.

# APPENDIX – Management's Response

BERTHA W. HENRY, County Administrator
115 S. Andrews Avenue, Room 409 • Fort Lauderdale, Florida 33301 • 954-357-7362 • FAX 954-357-7360

## MEMORANDUM

To: Robert Melton, CPA/CIA/CFE/CIG, County Auditor

From: Bertha Henry, County Administrator

Date: August 30, 2018

Re: Management Response to Audit of Driver and Vehicle Information Database (DAVID) Usage by the Risk Management Division

At the request of County management, the County Auditor's Office was engaged to audit the Risk Management Division's access and usage of the Driver and Vehicle Information Database (DAVID) provided by the Florida Department of Highway Safety and Motor Vehicles (DHSMV). The access and usage of the DAVID system are pursuant to a Memorandum of Understanding (MOU) with the DHSMV, which provides for an audit to ensure compliance. Accordingly, the purpose of this audit was to determine whether the County's use of the DAVID system complies with the terms of the MOU with DHSMV.

Management is pleased and agrees with the overall conclusion of the Auditor's Report that the use of DAVID complies with the terms of the MOU with DHSMV, and internal controls are adequate to ensure compliance. The Auditor's Report identified five opportunities for improvement which are addressed herein as management's response.

### Opportunities for Improvement

1. **Information Obtained from DAVID Should be Used for Legitimate Business Purposes Only.**

   **Recommendations**

   a. Implement appropriate procedures to ensure DAVID database is used for legitimate business purposes related to RMD's objectives.

      ***Management agrees.***

   b. Ensure that appropriate documentation is maintained and retained to support the business justification for DAVID searches.

      ***Management agrees.***

Date: August 30, 2018
To: Robert Melton, County Auditor
From: Bertha Henry, County Administrator
Re: Management Response to Audit of Driver and Vehicle Information Database (DAVID) Usage by the Risk Management Division

---

2. **Quarterly Quality Control Reviews Should be Performed, Documented and Retained in Accordance with DHSMV's Audit Guidelines.**

   **Recommendations:**

   a. Ensure job duties are adequately segregated to help ensure errors and irregularities are prevented or detected on a timely basis.

      ***Management agrees*** to have quality control reviews be performed by an individual other than the Program Manager, who is a frequent user of DAVID.

   b. Document the results of quarterly quality control reviews in accordance with the requirements of the MOU.

      ***Management agrees.***

   c. Enhance quality control review procedures to include a review of the location from which DAVID is accessed. Management should investigate any such occurrences and document the outcomes.

      ***Management agrees.***

3. **Individuals With Access to DAVID and DAVID Data Stored on County Systems Should Acknowledge the Confidentiality of the Information and Criminal Sanctions for Unauthorized Use.**

   ***Management agrees*** to have all users with access to DAVID and DAVID data stored on County systems formally acknowledge the confidential nature of the information and the criminal sanctions for unauthorized use. This is with the understanding that if the County system can be segregated to prohibit user access to DAVID data stored on the County system that an acknowledgement would not be necessary for those who do not have access to the data.

4. **Physical Security Controls Should be Enhanced to Adequately Protect Confidential Information.**

   ***Management agrees*** to implement procedures to periodically change combination locks.

5. **Terminated Employee Access Should be Revoked Immediately Upon Termination.**

   ***Management agrees*** and will ensure that appropriate procedures are in place to immediately disable terminated employee access. It is further noted that the one individual identified in the report for having access after termination has been removed and access reports reveal that the individual did not access the system after termination.

Thank you for conducting this Audit, as requested by management, and the opportunity to respond and provide comments. Should you have any questions, please do not hesitate to contact me.

Date: August 30, 2018
To: Robert Melton, County Auditor
From: Bertha Henry, County Administrator
Re: Management Response to Audit of Driver and Vehicle Information Database (DAVID) Usage by the Risk Management Division

---

c: Monica Cepero, Deputy County Administrator
Andrew Meyer, County Attorney
George Tablack, Chief Financial Officer
Kevin Kelleher, Deputy CFO/Deputy Director, Finance and Administrative Services Department
Wayne Fletcher, Director, Risk Management Division
John Bruno, Chief Information Officer, Enterprise Technology Services