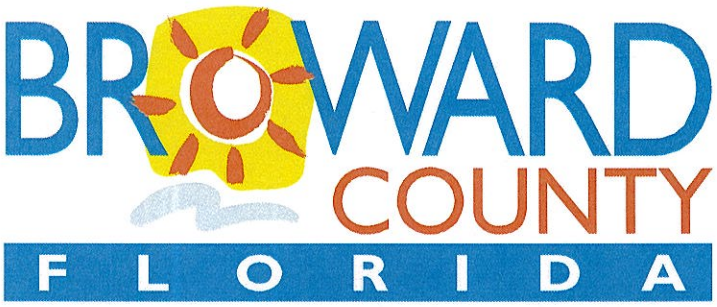
Exhibit 1



Audit of Driver's License and Motor Vehicle Record Data Exchange 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. 18-27
August 30, 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 30, 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's License and Motor Vehicle Record Data Exchange (DAVE) provided by the Florida Department of Highway Safety and Motor Vehicles (DHSMV).

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

We conclude that the use of DAVE complies with the terms of the Memorandum of Understanding with DHSMV, and internal controls are adequate to ensure compliance. Opportunities for Improvement are included within the report.

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's License and Motor Vehicle Record Data Exchange (DAVE) provided by the Florida Department of Highway Safety and Motor Vehicles (DHSMV). Our audit objectives were to determine whether:

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

To determine whether the use of DAVE 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 user access review, user administration, change management, incident management, data backup, and continuity of operations procedures. We validated user access permissions, data interfaces, monitoring practices, and the security of information storage on County systems.

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

We conclude that the use of DAVE complies with the terms of the Memorandum of Understanding with DHSMV, and internal controls are adequate to ensure compliance. Opportunities for Improvement are included within the report.

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's License and Motor Vehicle Record Data Exchange (DAVE), which provides remote electronic access to driver license and motor vehicle information. This agreement was renewed in February 2018 giving the RMD continued access for an additional three years.

As the information provided through the data exchange is confidential, 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.

Risk Management Division's Data Exchange 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.*

RMD, a division of the Finance and Administrative Services Department (FASD), uses DAVE to verify the driver's license status of current County employees.

County employees do not have direct access to the DAVE application. The County has created a data interface that automatically downloads drivers' license data for current County employees using a secure file transfer protocol (SFTP). Once downloaded, this information is transferred to the Safety and Health Investigative and Liability Database (SHIELD) application, which is used to manage employee personal information, and generate and distribute reports of suspended licenses to County management.

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. Access to Drivers' License Data Should be Restricted Based on Job Responsibilities and Segregation of Duties to Prevent Unauthorized Activity.

During our review of access to DAVE data within the SHIELD application, we noted the following concerns:

A. Management has a process for authorizing logical access to SHIELD using a user access request form. However, this process is not formally documented and is not consistently followed. We noted that one employee hired during the audit period was granted access to SHIELD without an authorized user access form. Providing user access without an appropriately authorized user access request form increases the risk of unauthorized or inappropriate access. Established user administration procedures should be followed to document the level of access an employee is authorized to have as well as management's approval of that access.

B. Privileged access to the SHIELD application is not appropriate in some instances. During our review, we noted the following concerns:

   i. Three of 27 (11%) SHIELD administrators are also operational users performing day to day transactions. This combination of access allows these users to bypass application controls and represents a segregation of duties conflict. As a result, inappropriate activities could occur without timely detection. Application administration functions should be performed by information technology personnel using established user administration procedures rather than operational user staff.

   ii. Two employees had the ability to perform application development activities as well as application administration. This combination of access allows these employees to bypass established change management procedures and represents a segregation of duties conflict. As a result, inappropriate changes could be made to the application without timely detection. Application development functions should be segregated from application administration functions to ensure established change management procedures are followed.

C. Annual reviews of user access to the SHIELD application are not performed to ensure that access to confidential information is restricted based on job responsibilities. Chapter 5, Section H of the MOU requires that all access to the information must be monitored on an ongoing basis. Failure to periodically review access to County systems may allow employees to retain inappropriate access after a change in job function, termination from Broward County, functional or security changes to applications, and organization structural changes.

We recommend management:

A. Ensure formal procedures for requesting, removing, and modifying user access to SHIELD using access request forms are consistently followed.

B. Restrict business users from performing application administration for the SHIELD application. In addition, application development and administration functions should be segregated.

C. Review user access to SHIELD at least annually. The review should be documented to demonstrate management's due diligence.

2. Individuals With Access to DAVE 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 24 of 24 (100%) employees with access to DAVE information stored on 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 DAVE information stored on County systems formally acknowledge their understanding of the confidential nature of the information and the criminal sanctions for unauthorized use.

3. Application Logs Should be Periodically Reviewed to Identify Unusual Activity.

Management does not perform a periodic review of application logs to identify and follow-up on any unusual activity identified. The SHIELD application has logging enabled; however, management has not implemented a process to periodically review the logs in order to obtain timely notification of inappropriate or unauthorized activity. Without a periodic review of application logs, inappropriate or unauthorized activity may remain undetected.

We recommend management implement procedures to periodically review activity logs for the SHIELD application. In addition, we recommend that management document the review.

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's License and Motor Vehicle Record Data Exchange (DAVE) Usage by the Risk Management Division

At the request of Management, the County Auditor's Office was engaged to audit the Risk Management Division's (RMD) access and usage of Driver's License and Motor Vehicle Record Data Exchange (DAVE) provided by the Florida Department of Highway Safety and Motor Vehicles (DHSMV). The access and usage of the DAVE 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 DAVE 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 DAVE complies with the terms of the MOU with DHSMV, and internal controls are adequate to ensure compliance. The Auditor's Report identified three opportunities for improvement which are addressed herein as management's response.

Opportunities for Improvement

1. **Access to Drivers' License Data Should be Restricted Based on Job Responsibilities and Segregation of Duties to Prevent Unauthorized Activity.**

   Recommendations

   a. Ensure formal procedures for requesting, removing, and modifying user access to SHIELD (Safety and Health Investigative, and Liability Database – the County's system) using access request forms are consistently followed.

      Management agrees.

   b. Restrict business users from performing application administration for the SHIELD application. In addition, application development and administration functions should be segregated.

      Management agrees that the business users will not be performing user access application administration for the SHIELD application. Additionally, the application development and administration functions will be separated.

Date: August 30, 2018
To: Robert Melton, County Auditor
From: Bertha Henry, County Administrator
Re: Management Response to Audit of Driver's License and Motor Vehicle Record Data Exchange (DAVE) Usage by the Risk Management Division

c. Review user access to SHIELD at least annually. The review should be documented to demonstrate management's due diligence.

Management agrees.

2. **Individuals with Access to DAVE 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 DAVE information 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 DAVE data stored on the County system that an acknowledgement would not be necessary for those who do not have access to the data.

3. **Application Logs Should be Periodically Reviewed to Identify Unusual Activity.**

Management agrees to implement procedures to periodically review activity logs.

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.

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