



Audit of
Drivers' License and Motor Vehicle
Record Data Exchange Usage by the
Environmental and Consumer
Protection 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, CISA, Information Technology Auditor

Report No. 19-07
March 20, 2019



OFFICE OF THE COUNTY AUDITOR

115 S. Andrews Avenue, Room 520 • Fort Lauderdale, Florida 33301 • 954-357-7590 • FAX 954-357-7592

March 20, 2019

Honorable Mayor and Board of County Commissioners

At the request of management, we conducted an audit of the internal controls over Environmental and Consumer Protection 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,

A handwritten signature in blue ink, appearing to read "Bob Melton", is written over a light blue circular stamp.

Bob Melton
County Auditor

cc: Bertha Henry, County Administrator
Andrew Meyers, County Attorney
Monica Cepero, Deputy County Administrator
Henry Sniezek, Director Environmental Protection and Growth Management
Jeff Halsey, Director Environmental and Consumer Protection

Broward County Board of County Commissioners

Mark D. Bogen • Lamar P. Fisher • Beam Furr • Steve Geller • Dale V.C. Holness • Nan H. Rich • Tim Ryan • Barbara Sharief • Michael Udine
www.broward.org

TABLE OF CONTENTS

INTRODUCTION.....	2
Scope and Methodology.....	2
Overall Conclusion.....	3
Background.....	3
OPPORTUNITIES FOR IMPROVEMENT.....	5
1. Access to Drivers’ License Data Should be Restricted Based on Job Responsibilities and Segregation of Duties to Prevent Unauthorized Activity.....	5
2. Individuals With Access to DAVE Data Stored on County Systems Should Acknowledge the Confidentiality of the Information and Criminal Sanctions for Unauthorized Use.....	6
3. Application Logs Should be Generated and Periodically Reviewed to Identify Unusual Activity Relevant to the MOU.....	7
4. Policies and Procedures Should be Developed to Ensure Compliance With MOU Requirements...	7
MANAGEMENT’S RESPONSE.....	8

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 Environmental and Consumer Protection 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 (MOU) along with the adequacy of internal control to ensure compliance, we obtained and reviewed user requirements, including review of the Memorandum of Understanding (MOU) 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 January 1, 2018 through

December 31, 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 (MOU) with DHSMV, and internal controls are adequate to ensure compliance. Opportunities for Improvement are included within the report.

Background

In October 2014, the Environmental and Consumer Protection Division (ECPD) 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 November 2017 giving the ECPD 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.

Environmental and Consumer Protection 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.

ECPD, a division of the Environmental Protection and Growth Management Department (EPGMD), uses DAVE for chauffeur registration background checks. Section 22½-8, Chapter 22½ - Motor Carriers, of the Broward County Code of Ordinances requires background checks prior to issuing a Broward County chauffeur's registration. The background check includes a review of driving records.

Audit of Driver's License and Motor Vehicle Record Data Exchange Usage
by the Environmental and Consumer Protection Division

County employees do not have direct access to the DAVE application. The County has created a data interface called the Driver's License Search (DLS) system that automatically downloads drivers' license data for chauffeur's license applicants once a driver's license number is manually entered. Each submission to the State of Florida is considered a transaction whether valid or invalid. If the driver's license number is valid, a web page is returned with the information requested, which is then exported to an encrypted network location. If the driver's license number is invalid, no data is returned to the user.

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 DLS application, we noted the following :

- A. Management has a process for authorizing logical access to the DLS application using a user access request form. However, for the one user account created and granted user access to the DLS application during the audit period, an authorized user access request form was not used. 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 DLS application is not appropriate in some instances. During our review, we noted the following concerns:
 - i. One DLS application administrator also had the ability to perform 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. User administration functions should be segregated from business functions. As of March 14, 2019, this user's ability to perform transactions was removed.
 - ii. Two DLS application users also had the ability to perform application development activities. This combination of access represents a segregation of duties conflict increasing the risk of inappropriate activity. Application development functions should be segregated from business user functions to ensure established procedures are followed. As of February 26, 2019, these two users had their application access removed.
- C. Annual reviews of user access to DAVE's data are not performed to ensure that access to confidential information is restricted based on job responsibilities. Our review noted one of 24 (4%) users with access to the encrypted network drive where DAVE Data is stored

no longer required access. 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 established procedures for requesting, removing, and modifying user access to the DLS application are consistently followed.
- B. Ensure the appropriateness of privileged user access to the DLS application.
 - i. Restrict administrators from performing business transactions within the DLS application.
 - ii. Ensure application development functions and business user functions are segregated.
- C. Review user access to DLS application 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, sixteen of 37 (43%) ECPD employees and hearing officers 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, responding to violations of confidentiality by employees, and reducing the risk of violation of the terms of the MOU.

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 Generated and Periodically Reviewed to Identify Unusual Activity Relevant to the MOU.

The DLS application and its associated user access management system does not generate activity logs in order to facilitate the identification and follow-up of unusual activity relevant to the MOU, specifically:

- A. The date and time users are added or removed from the DLS application.
- B. Failed log-in attempts.
- C. Data transfer status and errors.
- D. Searches performed along with the individual performing each search.

Without the generation and periodic review of application logs, inappropriate or unauthorized activity may remain undetected.

We recommend management implement procedures to generate activity logs for the DLS application and its associated user management system related to the MOU. In addition, management should implement procedures to periodically review application logs for discrepancies or suspicious activity and document the review as evidence of their due diligence.

4. Policies and Procedures Should be Developed to Ensure Compliance With MOU Requirements.

During our review, we noted that policies and procedures needed to be developed to ensure compliance with MOU Requirements, specifically;

- A. Management has implemented a process to track, and monitor incidents reported by users; however:
 - i. The process is informal and is not documented.
 - ii. The process does not facilitate coordination between ETS and ECPD to identify, track, or monitor incidents handled by ETS that may be reportable to the DHSMV under this MOU.

Audit of Driver's License and Motor Vehicle Record Data Exchange Usage
by the Environmental and Consumer Protection Division

- B. Management has implemented processes for managing data searches and addressing consumer complaints regarding the misuse of Florida Driver Privacy Protection Act (DPPA) protected information; however, these procedures are not documented.
- C. Management does not have documented policies and procedures to address releasing state employee information without the express written consent of the state. Upon inquiry, key personnel were unaware of the requirement that a written consent is required before providing state employee information (name, email address, telephone number) to third party end users as dictated by the MOU. Management indicated that there have been no such instances during the audit period.

We recommend management:

- A. Document incident management policies and procedures that includes coordination with ETS to ensure all incidents that may be reportable to DHSMX under this MOU are appropriately handled.
- B. Document procedures for managing data searches and addressing consumer complaints.
- C. Update agency procedures to include requirements for providing state employee information.

MANAGEMENT'S RESPONSE

Audit of Driver's License and Motor Vehicle Record Data Exchange Usage
by the Environmental and Consumer Protection Division



BERTHA W. HENRY, County Administrator

115 S. Andrews Avenue, Room 409 • Fort Lauderdale, Florida 33301 • 954-357-7362 • FAX 954-357-7360

TO: Robert Melton, County Auditor

FROM: Bertha W. Henry, County Administrator

A handwritten signature in blue ink that reads "B.W. Henry for B. Henry".

DATE: March 19, 2019

SUBJECT: Response to County Auditor's Audit Report on Driver's License and Motor Vehicle Record Data Exchange (DAVE) Usage by the Environmental and Consumer Protection Division

The above referenced County Auditor's report has been received and reviewed. Management accepts the Auditor's findings and agrees to implement all the recommended improvements.

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

Recommendation A: *Ensure established procedures for requesting, removing, and modifying user access to the DLS application are consistently followed.*

Management's Response: Management concurs. Procedures will be documented in the Division DAVE Standard Operating Procedure (SOP), to be completed by 3rd quarter of Fiscal Year 2019.

Recommendation B: *Ensure the appropriateness of privileged user access to the DLS application.*

- i. *Restrict administrators from performing business transactions within the DLS application.*
- ii. *Ensure application development functions and business user functions are segregated.*

Management's Response: Management concurs and has implemented. Administrators have been restricted to administrative access only. No current user possesses both application development and business user functions.

Recommendation C: *Review user access to DLS application at least annually. The review should be documented to demonstrate management's due diligence.*

Management's Response: Management concurs. As will be indicated in the Division DAVE SOP, access review will be completed quarterly and documented.

Improvement Opportunity 2: *Individuals With Access to DAVE Data Stored on County Systems Should Acknowledge the Confidentiality of the Information and Criminal Sanctions for Unauthorized Use.*

Recommendation: *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.*

Broward County Board of County Commissioners

Mark D. Bogen • Lamar P. Fisher • Beam Furr • Steve Geller • Dale V.C. Holness • Nan H. Rich • Tim Ryan • Dr. Barbara Sharief • Michael Udine

Broward.org

March 19, 2019

Response to County Auditor's Report – DAVE Data at ECPD

Management's Response: Management concurs. Acknowledgment forms have been distributed to those users without a completed form; no user will be able to maintain access to DAVE information without a completed form. In the future, all new users will complete the form as part of onboarding to the system and this requirement will be reflected in the Division DAVE SOP.

Improvement Opportunity 3: *Application Logs Should be Generated and Periodically Reviewed to Identify Unusual Activity Relevant to the MOU.*

Recommendation: *Implement procedures to generate activity logs for the DLS application and its associated user management system related to the MOU. In addition, management should implement procedures to periodically review application logs for discrepancies or suspicious activity and document the review as evidence of their due diligence.*

Management's Response: Management concurs. Electronic application logs are currently being developed and are anticipated to go live within the 3rd Quarter of FY 2019. Application log review procedures will be documented in the Division DAVE SOP, to be completed within the 3rd Quarter of FY 2019.

Improvement Opportunity 4: *Policies and Procedures Should be Developed to Ensure Compliance With MOU Requirements.*

Recommendation A: *Document incident management policies and procedures that include coordination with ETS to ensure all incidents that may be reportable to DHSMX under this MOU are appropriately handled.*

Recommendation B: *Document procedures for managing data searches addressing consumer complaints.*

Recommendation C: *Update agency procedures to include requirements for providing state employee information.*

Management's Response to A, B and C: Management concurs. All procedures will be documented within the DAVE SOP, to be completed by 3rd Quarter of FY2019. This documentation will incorporate resolution of a potential inconsistency noted during the audit exit meeting, wherein polices are requested for releasing state employee information without the express written consent of the state, yet public records laws may not require such a consent.

cc: Monica Cepero, Deputy County Administrator
Kevin Kelleher, Deputy CFO/Deputy Director, Finance and Administrative Services Department
John Bruno, Chief Information Officer, Enterprise Technology Services
Henry Sniezek, Director, Environmental Protection and Growth Management Division
Lenny Vialpando, Deputy Director, Environmental and Growth Management Division
Jeffery Halsey, Director, Environmental and Consumer Protection Division