Follow-up Review of Audit of Drivers' License and Motor Vehicle Record Data Exchange Usage by the Environmental and Consumer Protection Division

Office of the County Auditor

Follow-up Review Report

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

Review Conducted by:
Gerard Boucaud, CIA, CISA, CDPSE, Audit Manager
Muhammad Ramjohn, CISA, Information Technology Auditor

Report No. 20-19
September 29, 2020

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

September 29, 2020

Honorable Mayor and Board of County Commissioners

We have conducted a follow-up review of our Audit of Drivers' License and Motor Vehicle Record Data Exchange Usage by the Environmental and Consumer Protection Division. (Report No. 19-07). The objective of our review was to determine the implementation status of our previous recommendations.

We conclude that all eight of our previous recommendations were implemented. We **commend** management for implementing our recommendations. The status of each of our recommendations is presented in this follow-up report.

We conducted this review in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the review to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our review objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our review objectives.

We appreciate the cooperation and assistance provided by the staff of the Environmental Consumer Protection and Enterprise Technology Services Divisions throughout our review process.

Respectfully submitted,

Bob Melton
County Auditor

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

TABLE OF CONTENTS

IMPLEMENTATION STATUS SUMMARY

Implementation Status of Previous Recommendations From
Audit of Drivers' License and Motor Vehicle Record Data Exchange Usage by the Environmental and Consumer Protection Division

REC. NO.	PREVIOUS RECOMMENDATION	IMPLEMENTED	PARTIALLY IMPLEMENTED	NOT IMPLEMENTED	NOT APPLICABLE
1A.	Ensure established procedures for requesting, removing, and modifying user access to the DLS application are consistently followed.	☑			
1B.	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.	☑			
1C.	Review user access to DLS application at least annually. The review should be documented to demonstrate management's due diligence.	☑			
2.	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.	☑			

REC. NO.	PREVIOUS RECOMMENDATION	IMPLEMENTED	PARTIALLY IMPLEMENTED	NOT IMPLEMENTED	NOT APPLICABLE
3.	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.	☑			
4A.	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.	☑			
4B.	Document procedures for managing data searches and addressing consumer complaints.	☑			
4C.	Update agency procedures to include requirements for providing state employee information.	☑			

INTRODUCTION

Scope and Methodology

The Office of the County Auditor 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.

We conducted a follow-up review of our Audit of Drivers' License and Motor Vehicle Record Data Exchange Usage by the Environmental and Consumer Protection Division. (Report No. 19-07). The objective of our review was to determine the implementation status of previous recommendations for improvement.

We conducted this review in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the review to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our review objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our review objectives.

Our follow-up review included such tests of records and other auditing procedures, as we considered necessary in the circumstances. The follow-up testing was performed for the period June 1, 2020 through September 23, 2020. However, transactions, processes, and situations reviewed were not limited by the audit period.

Overall Conclusion

We conclude that all eight of our previous recommendations were implemented. We **commend** management for implementing our recommendations. The status of each of our recommendations is presented in this follow-up report.

OPPORTUNITIES FOR IMPROVEMENT

This section reports actions taken by management on the Opportunities for Improvement in our previous review. The issues and recommendations herein are those of the original review, followed by the current status of the recommendations.

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.

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. 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. 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.

We recommended 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.

Implementation Status:

A. **Implemented.**

B. **Implemented.**

C. **Implemented.**

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 recommended 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.

Implementation Status: Implemented.

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 recommended 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.

Implementation Status: Implemented.

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.

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 recommended 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.

Implementation Status:

A. **Implemented.**

B. **Implemented.**

C. **Implemented.**