SOUTH FLORIDA WATER MANAGEMENT DISTRICT

Audit of DMV File Security

Project # 18-11

Prepared by
Office of the Inspector General

J. Timothy Beirnes, CPA, Inspector General
Daniel Sooker, CPA, Chief Investigator

sfwmd.gov

SOUTH FLORIDA WATER MANAGEMENT DISTRICT

November 7, 2018

Audit and Finance Committee Members:

Re: Audit of the Department of Motor Vehicles File Security – *Project No. 18-11*

This audit was performed pursuant to the Inspector General's authority set forth in Chapter 20.055, F.S. Our objective was to determine whether District internal controls related to employee driver license information received from the DMV are adequate to ensure that the DMV records are protected from unauthorized use. Dan Sooker and I prepared this report.

Sincerely,

J. Timothy Beirnes, CPA
Inspector General

TABLE OF CONTENTS

BACKGROUND

In accordance with Section V. *Safeguarding Information* (F) of the Memorandum of Agreement (MOU) between the District and the Department of Highway Safety and Motor Vehicles (DMV), our Office conducted an audit of District internal controls related to employee DMV records that are received monthly. The MOU requires the District to physically secure driver license data and to ensure proper and authorized use of the DMV records. The District's Occupational Safety Manager is responsible for reviewing the DMV records for current driver's license suspensions, and other major infractions to ensure that employees operating District vehicles have valid Florida driver licenses.

OBJECTIVE, SCOPE AND METHODOLOGY

Our primary objective was to determine whether District internal controls related to driver license information received from the DMV are adequate to ensure that the DMV records are protected from unauthorized access, distribution, use, modification or disclosure. To accomplish our objectives, we performed the following:

- Documented and assessed the internal controls related to DMV records.
- Reviewed the DMV electronic transfer process.
- Interviewed Information Technology staff responsible for security of the DMV records.

We conducted this performance 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.

AUDIT RESULTS

Executive Summary

The District is required to establish a system of internal controls related to the monthly DMV Report to ensure that driver's license information is secured against unauthorized access, distribution, use, modification or disclosure. Our examination of this system found that adequate internal controls are in place to secure the DMV records. As a result, the District is in full compliance with the MOU. A summary of the key District internal controls over the monthly DMV Report is as follows:

- The DMV sends the monthly DMV Report to the District's FTP secured server. Access to this server is restricted.
- The monthly DMV Report file is zipped, and password protected.
- The monthly DMV Report was distributed only to the District's Occupational Safety Manager.
- The e-mail and attached monthly DMV Report is blocked from retention in the Enterprise Vault.
- The e-mail with the monthly DMV Report is marked "exempt from public record" to ensure that the e-mail is not inadvertently sent in a public records request.

Internal Controls Over the Monthly DMV Report Process

We reviewed the internal controls related to the security of the monthly DMV Report that the District receives from the DMV. The automated process starts on the 3rd of the month, when SAP submits a monthly batch job and sends an outbound UNIX file of District employee driver's license numbers, which is zipped, and password protected, to a District FTP server. Four staff in the Emergency Management and Safety Section, Human Resources Bureau, and the Database Services Unit are e-mailed a notice that the outbound file has been sent to a FTP server. On the 5th of the month, DMV looks for the outbound UNIX file on the District's server site, processes it by adding employee name, address, date of birth, driver's license number, infraction information and other personal information in the DMV record and then places the updated password protected DMV Report back to the FTP server. On the 6th of the month, a SAP program job runs the monthly DMV Report from the District's server site, processes it through an ABAP program that formats the report and separates the new infractions from previously reported violations and invalid driver's license numbers (see Appendix 1 for DMV Report process).

The formatted monthly DMV Report is sent to the Human Resources secure server, ZHRBTC01, and then e-mailed to the District's Occupational Safety Manager, who is responsible for reviewing it for current Driver's license suspension, and other major infractions. If the monthly DMV Report indicates that an employee has a driver license suspension or other major infraction, the Occupational Safety Manager informs the employee's supervisor but does not forward the DMV Report record to the employee's supervisor since the report contains confidential information. When the Occupational Safety Manager completes his review, the e-mail and the monthly DMV Report attachment is deleted.

The e-mail and monthly DMV Report is blocked from retention in the Enterprise Vault when it was added to the "ACE Discard" group. However, if the e-mail with the monthly DMV Report is forwarded by the Occupational Safety Manager to District staff, the e-mail is preserved in Enterprise Vault archive. As an additional security measure, the e-mail with the monthly DMV Report is marked "exempt from public record" to ensure that the e-mail is not inadvertently sent in a public records request.

In order to determine whether the monthly DMV Report was restricted to the Occupational Safety Manager, we conducted a search of the e-mail Enterprise Vault archives containing the term "monthly DMV Report" for period March 2017 through March 2018 with Symantec Discovery Accelerator. We found that for the period under review, the e-mail file was restricted to the Occupational Safety Manager and was not forwarded to any District staff.

DMV Infraction Report Process