



**DIVISION OF INSPECTOR GENERAL**  
Ken Burke, CPA  
Clerk of the Circuit Court and Comptroller  
Pinellas County, Florida



# AUDIT OF RISK MANAGEMENT DRIVER LICENSE TRANSCRIPT DATA EXCHANGE



Melissa Dondero, CPA, CIA, CIG, CIGA, CIGI, CITP, CRMA, CFS, CECFE, CGI  
Inspector General/Chief Audit Executive

**Audit Team**  
Robert Poynter, CIGA, CIGI, CISA, CCA, CECFE, CFS - Assistant Inspector General  
Shawn Phillips, CIGA, CIGI, CECFE - Inspector General I

REPORT NO. 2021-04  
FEBRUARY 17, 2021



## Ken Burke, CPA

CLERK OF THE CIRCUIT COURT AND COMPTROLLER  
PINELLAS COUNTY, FLORIDA

Clerk of the County Court  
Recorder of Deeds  
Clerk and Accountant of the Board of County Commissioners  
Custodian of County Funds  
County Auditor

## Division of Inspector General

510 Bay Avenue  
Clearwater, FL 33756  
Telephone: (727) 464-8371  
Fax: (727) 464-8386  
Fraud Hotline: (727) 45FRAUD (453-7283)  
Clerk's website: [www.mypinellasclerk.org](http://www.mypinellasclerk.org)

February 17, 2021

Joseph Lauro, Director, Department of Administrative Services

We have conducted an audit of the Risk Management Driver License Transcript Data Exchange per management request.

We identified no Opportunities for Improvement as a result of the audit.

We appreciate the cooperation shown by the staff of the Risk Management Division during the course of this review.

Respectfully Submitted,

*Melissa Dondero*

Melissa Dondero  
Inspector General/Chief Audit Executive

Approved:

Ken Burke, CPA\*  
Clerk of the Circuit Court and Comptroller  
Ex Officio County Auditor  
\*Regulated by the State of Florida

cc: The Honorable Chairman and Members of the Board of County Commissioners  
Barry Burton, County Administrator  
Kevin Knutson, Assistant County Administrator  
Merry Celeste, Director, Purchasing and Risk Management Division



An Accredited Office of  
Inspector General

# TABLE OF CONTENTS

<b>INTRODUCTION</b>	<b>4</b>
<i>Abbreviations</i>	4
<i>Executive Summary</i>	5
<i>Background</i>	6
<b>SCOPE AND METHODOLOGY</b>	<b>11</b>
<b>OBJECTIVES AND OUTCOMES</b>	<b>13</b>

# INTRODUCTION

## *Abbreviations*

<b>Administrative Services</b>	Department of Administrative Services
<b>BCC</b>	Board of County Commissioners
<b>BTS</b>	Business Technology Services
<b>County</b>	Pinellas County
<b>COVID-19</b>	Coronavirus Disease 2019
<b>DHSMV</b>	Florida Department of Highway Safety and Motor Vehicles
<b>DL</b>	Driver License
<b>DPPA</b>	Driver's Privacy Protection Act
<b>FTP</b>	File Transfer Protocol
<b>FY</b>	Fiscal Year
<b>MOU</b>	Memorandum of Understanding
<b>OPUS</b>	Oracle Project Unified Solution
<b>ORION</b>	Online Registration and Identity Operating Network
<b>OTI</b>	Office of Technology and Innovation
<b>Risk Management</b>	Purchasing and Risk Management Division
<b>SFTP</b>	Secure File Transfer Protocol
<b>VDQ</b>	Vehicle Driver Qualification

## ***Executive Summary***

At the request of the Purchasing and Risk Management Division (Risk Management), we conducted an audit of the Risk Management Memorandum of Understanding (MOU) with the Florida Department of Highway Safety and Motor Vehicles (DHSMV) for the batch driver license (DL) transcript data exchange via batch job \$DTR305B. The MOU (contract number HSMV-0233-20) was fully executed by the DHSMV on February 20, 2020.

The objectives of our audit were to:

1. Ensure the compliance of Risk Management with the data security requirements in the data exchange MOU and applicable data protection statutes, codes, and policies.
2. Ensure adequate policies and procedures were in place to protect personal data provided to Risk Management by the DHSMV through the DL transcript process.
3. Ensure adequate security over the access of Risk Management, Business Technology Services, and the Office of Technology and Innovation to DHSMV data through the batch DL transcript process.
4. Ensure adequate security over the distribution, use, modification, and disclosure of DHSMV data obtained through the batch DL transcript process.

The internal controls governing the use and dissemination of personal data obtained from the DL transcript data exchange have been evaluated in light of the requirements of the DHSMV MOU and applicable laws and are adequate to protect the personal data from unauthorized access, distribution, use, modification, and disclosure. This includes policies and procedures for personnel to follow and data security policies and procedures in place to protect personal data. The data security policies and procedures have been reviewed by a Risk Management IT Security Professional and found to be acceptable to protect personal data.

Our review revealed Risk Management used the DHSMV's DL transcript data exchange solely to support the issuance of County DLs and safe driver awards. We identified no issues regarding Risk Management's adherence to the MOU requirements.

## Background



The Purchasing and Risk Management Division (Risk Management) is one of three divisions in the Department of Administrative Services (Administrative Services). Administrative Services provides the following services for all departments under the Board of County Commissioners (BCC), select appointing authorities, and select constitutional officers as needed or required:

- Procurement and contracting
- Facility and real property management
- Risk management
- Fleet services

Risk Management's mission is to protect and safeguard Pinellas County (County) assets from property, casualty, and occupational risks. Risk Management follows steps to develop, manage, and secure the County's most valuable assets in accordance with statutes, ordinances, and laws. Risk Management provides services to all County departments and agencies, the BCC, the constitutional officers, and the citizens. Risk Management has three divisions as follows:

- Safety
- Claims
- Insurance & Contractual Risk Transfer

The Safety Division coordinates safety policies, loss control, and safety training. Services include training in occupational safety, equipment operation safety, cardiopulmonary resuscitation and first aid, supervisor training, and new hire orientation safety training.

The Claims Division provides claims adjusting for workers' compensation claims, property claims, auto liability claims, and general liability claims. The Claims Division is also responsible for reporting requirements to the State of Florida for purposes of claims self-administration. Services include recovering money owed to the County for damages or injuries caused by others.

The Insurance & Contractual Risk Transfer Division manages the insurance program for County departments, the BCC, and constitutional officers. Services include placement and administration of over 50 insurance policies. Also, contractual risk transfer services include reviewing most County contracts and agreements for risk assessment and to assign insurance requirements for special events, contractors, service providers, and vendors conducting business with the County.



During fiscal year (FY) 2020, Risk Management's performance resulted in accomplishments that helped the County's employees and citizens. Specifically, Risk Management successfully completed a pilot to keep employees who work alone in the field safe through a Lone Worker with Incapacitation program. In addition, Risk Management recovered over \$300,000 in claims due from County-damaged property, vehicles, and workers' compensation in FY 2020. During FY 2020, Risk Management received 736 new claims and closed 746 claims. Flood policy renewals also increased 14% in FY 2020. To mitigate further increase, Risk Management is updating the statement of values for County-owned properties by inspecting property sites and working with County departments to determine whether flood coverage is needed.

Risk Management has supported Coronavirus Disease 2019 (COVID-19) response by providing guidance and hands on assistance to field employees in departments such as Public Works and Utilities. All employees are following the Centers for Disease Control and Prevention social distancing policies and best practices. This has transitioned staff attention away from their safety audits and typical training activities.

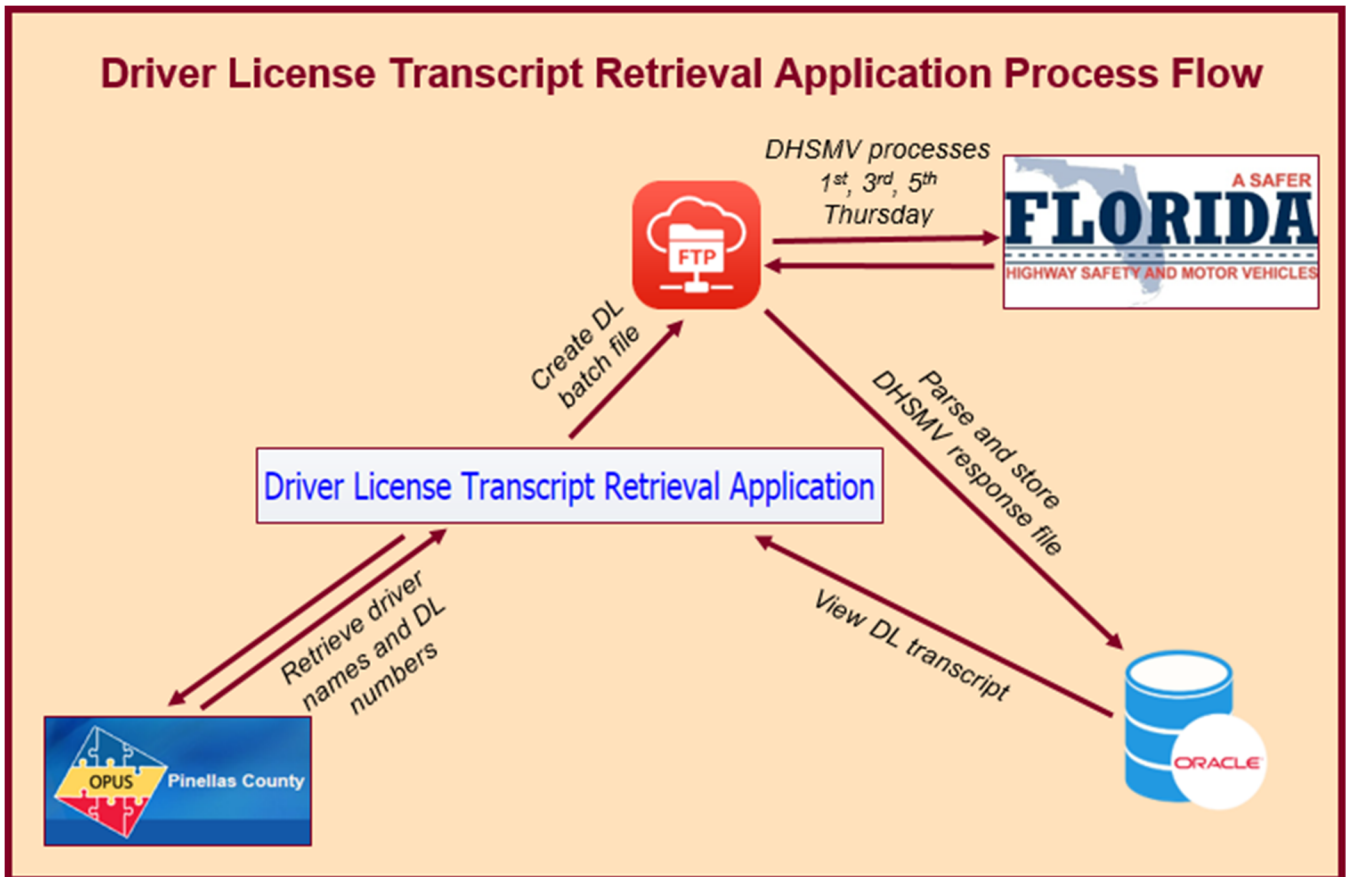
At the time of publishing the FY 2021 Adopted Budget, Risk Management's Safety staff had devoted approximately 200 hours to COVID-19 response in support of field personnel and staff countywide. Additionally, Risk Management had a staff nurse devoted to workers' compensation injuries, working with employees and physicians to get employees back to a healthy state of work. Risk Management's nurse had devoted approximately 700 hours, establishing protocols and screening processes for the BCC and Pinellas County Sheriff's Office staff at the County 9-1-1 Communications Center during COVID-19.

Risk Management obtains driver license (DL) transcripts to support the issuance of County DLs. Risk Management's process to obtain DL transcripts from the Florida Department of Highway Safety and Motor Vehicles (DHSMV) is as follows:

- A County employee or prospective County employee signs and submits a Vehicle Driver Qualification (VDQ) form to Risk Management authorizing the County to perform a DL check
- Risk Management staff enters the new or existing employee's driver information from the VDQ form into the Oracle Project Unified Solution (OPUS) application
- Risk Management staff accesses the in-house DL Transcript Retrieval application and requests a list of drivers
- The DL Transcript Retrieval application connects to a data view of OPUS and returns a list of drivers for Risk Management staff
- Once Risk Management staff selects the desired drivers and executes a batch command, the DL Transcript Retrieval application places a file containing associated DL numbers in a directory on a County file transfer protocol (FTP) server
- The DHSMV accesses the directory via secure FTP (SFTP) on the first, third, and fifth Thursday, as applicable, of each month, to download the request file
- The DHSMV processes the Risk Management request file and responds by uploading the associated driver history to the County FTP server via SFTP
- Risk Management staff reviews any drivers with a history in the DL Transcript Retrieval application

- As applicable, Risk Management staff may speak to an employee's supervisor to discuss the driver history information
- If Risk Management staff determines an employee qualifies for a County DL, staff accesses OPUS to print the DL
- All VDQ forms are shredded when no longer needed, and driver license files are deleted periodically


Following is an illustration of the DL Transcript Retrieval application process used to obtain and review DL transcripts:



The DL Transcript Retrieval application has additional functionality to allow Risk Management to print safe driver award certificates for eligible employees.



## Memorandum of Understanding

DocuSign Envelope ID: 630350E3-1CBD-4A73-B7B5-4742D714D0E6	
	<b>Florida Department of Highway Safety and Motor Vehicles</b>
Contract / Agreement Review	
DHSMV Contract No.:	<u>HSMV-0233-20</u> Division: <u>Motorist Services</u> Date: <u>2/3/2020</u>
Contractor Name:	<u>Pinellas County Dept of Administrative Services, Purchasing and Risk Management</u>

The DHSMV provides services by partnering with County tax collectors and local, state, and federal law enforcement agencies to promote a safe driving environment. The department coordinates with its partners to issue DLs and identification cards, facilitate motor vehicle transactions, and provide services related to consumer protection and public safety. The DHSMV is composed of four divisions overseen by the Office of the Executive Director:

- Florida Highway Patrol
- Motorist Services
- Administrative Services
- Information Systems Administration

In carrying out its statutorily mandated duties and responsibilities, the DHSMV collects and maintains personal information that identifies individuals. Therefore, the DHSMV is subject to the disclosure prohibitions contained in 18 U.S.C. §2721, the Driver's Privacy Protection Act (DPPA), Sections 119.0712(2) and 501.171, Florida Statutes, and other statutory provisions.

The DHSMV Motorist Services Division has a data exchange Memorandum of Understanding (MOU) with Administrative Services Purchasing and Risk Management dated February 3, 2020. Administrative Services signed the agreement on December 21, 2019, and it was fully executed by the DHSMV on February 20, 2020. The agreement (contract number HSMV-0233-20) has a term of three years.

The DHSMV data exchange MOU provides Risk Management access to three-year batch DL transcripts to be used in validating the driving records of current or prospective County employees in accordance with the Motor Vehicle and Driver License Employment Guidelines. The FTP batch job is \$DTR305B. The job is executed through the DHSMV's SFTP service.

As part of the agreement with the DHSMV, Risk Management must secure all data associated with the data exchange. Section III., Legal Authority, of the MOU states the following:

*"Under this MOU, [Risk Management] will be provided, via remote electronic means, information pertaining to driver licenses and vehicles, including personal information authorized to be released pursuant to Section 119.0712(2), Florida Statutes and DPPA. By executing this MOU, [Risk Management] agrees to maintain the confidential and exempt status of any and all information provided by the [DHSMV] pursuant to this MOU and to ensure that any Third Party End Users accessing or utilizing said information shall do so in compliance with Section*

*119.0712(2), Florida Statutes and DPPA. Highly restricted personal information shall only be released in accordance with DPPA and Florida law."*

Section VI., Compliance and Control Measures, Subsection A. of the MOU states the following pertaining to the required internal control and data security audit:

***"Internal Control and Data Security Audit – This MOU is contingent upon [Risk Management] having appropriate internal controls in place at all times that data is being provided/received pursuant to this MOU to ensure that the data is protected from unauthorized access, distribution, use, modification, or disclosure. [Risk Management] must submit an Internal Control and Data Security Audit from a currently licensed Certified Public Accountant, on or before the first anniversary of the execution date of this MOU or within one hundred twenty (120) days from receipt of a request from the [DHSMV]. Government agencies may submit the Internal Control and Data Security Audit from their Agency's Internal Auditor or Inspector General. The audit shall indicate that the internal controls governing the use and dissemination of personal data have been evaluated in light of the requirements of this MOU, and applicable laws and are adequate to protect the personal data from unauthorized access, distribution, use, modification, or disclosure. This includes both policies/procedures in place for personnel to follow and data security procedures/policies in place to protect personal data. The audit shall certify that the data security procedures/policies have been approved by a Risk Management IT Security Professional. The audit shall also certify that any and all deficiencies/issues found during the audit have been corrected and measures enacted to prevent recurrence."***

As part of the DHSMV's modernization efforts, deployment of phase 1 of the new Online Registration and Identity Operating Network (ORION) occurred in December 2020. The new ORION system implementation changed how the County accessed the DHSMV system. Moving forward, the connection to the DHSMV will occur via a web service. Previously, the County accessed the DHSMV system using an SFTP service. Although the MOU under audit was signed in anticipation of the migration to a web service, this audit's purpose is to review the internal controls and data security governing access to the SFTP service since it was in use for the majority of the MOU term to date.

# SCOPE AND METHODOLOGY

We conducted an audit of the Risk Management DL Transcript Data Exchange.

The scope of the audit covered the data exchange MOU between Risk Management and the DHSMV to obtain batch DL transcripts. Section VI. A. of the MOU requires the completion of an internal control and data security audit on or before the first anniversary of the execution date of the MOU. Based on this MOU requirement and the applicable data protection laws referenced within the MOU, our audit scope was to assess the internal controls governing the use and dissemination of personal data obtained through the batch DL transcript process.

We ensured the internal controls in place were sufficient to protect the personal data from unauthorized access, distribution, use, modification, and disclosure. We ensured that any and all deficiencies and issues found during the audit were corrected and measures enacted to prevent recurrence.

In December 2020, there was a change to the method in which Risk Management obtained DL transcripts from the DHSMV. Specifically, a web service replaced the batch SFTP DL transcript service. Although the MOU under audit was signed in anticipation of the migration to a web service, this audit's scope is the SFTP service since it was in use for the majority of the MOU term to date.

The audit period was February 20, 2020, through January 31, 2021. However, we did not limit the review of transactions and processes by the audit period and scope.

During the audit period, we performed the following:

- Reviewed the data exchange MOU and referenced data protection statutes, codes, and policies.
- Reviewed Business Technology Services (BTS), Office of Technology and Innovation (OTI), and Risk Management policies and procedures governing the protection of personal data.
- Reviewed flow diagrams, reviewed the program design, and conducted meetings with BTS, OTI, and Risk Management staff to identify the path of DHSMV DL transcript data through County systems and all associated entry, exit, and storage points.
- Reviewed the controls in place to secure the machines and servers housing and executing the DL Transcript Retrieval application.
- Reviewed the controls in place to secure the DL transcript data transmissions between the DHSMV and the County.
- Reviewed the controls in place to secure DHSMV DL transcript data stored by BTS, OTI, and Risk Management, as applicable.
- Reviewed the process for the DHSMV to access the FTP service to download and upload DL transcript data and ensured it was adequately controlled.

- Reviewed the physical security controls at BTS and OTI to restrict access to computing equipment that housed the DL Transcript Retrieval application and DHSMV data.
- Conducted meetings with Risk Management staff to understand how the agency distributed, used, modified, and disclosed, if applicable, DHSMV DL transcript data.

# OBJECTIVES AND OUTCOMES

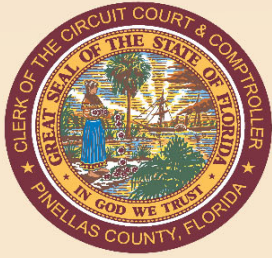
The objectives of the audit were to:

1. Ensure the compliance of Risk Management with the data security requirements in the data exchange MOU and applicable data protection statutes, codes, and policies.
2. Ensure adequate policies and procedures were in place to protect personal data provided to Risk Management by the DHSMV through the DL transcript process.
3. Ensure adequate security over the access of Risk Management, BTS, and OTI to DHSMV data through the batch DL transcript process.
4. Ensure adequate security over the distribution, use, modification, and disclosure of DHSMV data obtained through the batch DL transcript process.

As a result of the audit, we determined:

1. Risk Management was in compliance with the data security requirements in the data exchange MOU and referenced data protection statutes, codes, and policies.
2. Risk Management, BTS, and OTI had adequate policies and procedures in place to protect personal data provided by the DHSMV through the batch DL transcript process.
3. The security controls were adequate to restrict access to the DHSMV data obtained through the batch DL transcript process.
4. There were adequate security controls in place over the distribution, use, modification, and disclosure of DHSMV data obtained through the batch DL transcript process. Access to DHSMV data was controlled, and the data was used solely for Risk Management's business needs.

Our audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* and the *Principles and Standards for Offices of Inspector General*, and accordingly, included such tests of records and other auditing procedures, as we considered necessary in the circumstances.



# DIVISION OF INSPECTOR GENERAL

KEN BURKE, CPA  
CLERK OF THE CIRCUIT COURT  
AND COMPTROLLER  
PINELLAS COUNTY, FLORIDA

## SERVICES PROVIDED

AUDIT SERVICES  
INVESTIGATIONS  
GUARDIANSHIP SERVICES  
CONSULTING  
TRAINING  
COUNTY FRAUD HOTLINE  
GUARDIANSHIP FRAUD HOTLINE  
PCSO PREA HOTLINE



An Accredited Office of  
Inspector General

**Call:** (727) 464-8371

**Fax:** (727) 464-8386

**Fraud:** (727) 45FRAUD  
(727) 453-7283



**Internet:** [www.mypinellasclerk.org](http://www.mypinellasclerk.org)

 [www.twitter.com/pinellasig](https://www.twitter.com/pinellasig)

 [www.facebook.com/igpinellas](https://www.facebook.com/igpinellas)



**Write:**

Division of Inspector General  
510 Bay Avenue  
Clearwater, FL 33756