Marion County Human Resources DHSMV Data Exchange Audit

Report No. 2020-11

Presented To:
The Honorable Board of County Commissioners
Mounir Bouyounes, County Administrator

August 31, 2020

Issued By:
David R. Ellspermann, Clerk of the Circuit Court and Comptroller
Sachiko Horikawa, CPA, CIA, CISA, CRMA, CGAP, Internal Audit Director

ENGAGEMENT TEAM

Andrew Gibb, Auditor II
Heather Ewing, CIA, CFE, Internal Audit Manager

REPORT ABBREVIATIONS AND TERMS

Terminology	Abbreviation
Driver Privacy Protection Act	DPPA
Florida Department of Highway and Safety Motor Vehicles	DHSMV
Human Resources Department	HR
Information Technology	IT
Marion County Board of County Commissioners	County
Memorandum of Understanding	MOU

EXECUTIVE SUMMARY

On August 21, 2019, Internal Audit received an inquiry regarding an audit of Marion County Board of County Commissioners (County) Human Resources Department (HR) usage of Data Exchange which is an online database offered by the Florida Department of Highway Safety and Motor Vehicles (DHSMV). Internal Audit received a formal request for an internal control and data security audit on October 23, 2019. The purpose of the engagement was to attest, upon evaluation, that HR had appropriate and adequate internal controls "to ensure that the data is protected from unauthorized access, distribution, use, modification, or disclosure."

A Memorandum of Understanding (MOU) was entered into by HR and the DHSMV. The MOU requires there to be formalized policies and procedures for the use of Data Exchange. We found that HR did not have a thorough understanding of the applicable requirements of the MOU, and as a result, did not have formalized policies and procedures for the use of Data Exchange. We communicated our concerns and findings with the departmental management throughout the audit. HR has implemented our recommendations concerning the use of Data Exchange and are continuing to make improvements.

The MOU requires the Data Exchange user to have adequate general information technology (IT) controls and a security policy which is in alignment with Florida Statutes Section 282.318, Florida Administrative Code Rule 74-2, and the DHSMV security policies. The County IT department had previously created and implemented an IT Security Policy. The IT Security Policy could be enhanced by including a risk assessment and an incident response plan. The County's external auditors, Purvis Gray & Company, had previously made recommendations to address these areas of concern during their FY 19/20 audit. Below were their recommendations:

1) "Consider performing, at a minimum, an annual risk assessment on an acceptable framework, as part of its risk management program."

2) "Management should ensure designated IT staff are prepared to control the threat and trained on the procedural steps to minimize the damage to the systems and data from a cybercrime or other security incident."

Internal Audit agrees with the recommendations of the external auditors. In discussion with County IT department management, they expect to have the first draft of a risk assessment and an incident response plan by the end of quarter one of calendar year 2021. The County IT department's progress towards implementation of these recommendations will be followed-up by Internal Audit.

It is our opinion that the operational improvements and the internal controls implemented by HR during this audit were appropriate and adequate.

Per the requirement of the MOU, the County Administrator and Internal Audit Director certified that any and all deficiencies/issues found during the audit have been corrected and measures enacted to prevent recurrence (Exhibit A).

Table 1 Overview of Opportunities for Improvement			
#	**Summary**	**Recommendation**	**Management Response (Status)**
1	The MOU was signed by an HR employee who did not have the signature authority.	HR obtain the County Administrator's signature on the MOU.	Concur (In process of implementation)
2	HR management needed to have a thorough understanding of the MOU requirements to ensure compliance.	HR establish written procedures and forms to ensure compliance to the MOU and to clearly communicate the requirements and expectations to the authorized users of the DHSMV system and those who have access to personnel folders.	Concur (Implemented)
3	HR should manage Data Exchange user accounts effectively and timely.	HR designate an administrative account holder who will timely manage user accounts in Partner Portal.	Concur (Implemented)
4	HR needs to comply with the Internal Control and Data Security Audit Requirements.	HR management be familiar with contract terms and implement methods to ensure timely completion of required actions.	Concur (Implemented)
5	Driver's license transcripts needed to be labeled as confidential.	HR create procedures to label personnel information as public, sensitive, or confidential. Specifically, driver's license transcripts printed and placed in personnel files should be labeled as confidential.	Concur (Implemented)
6	The two authorized Data Exchange users were sharing a password to log into Partner Portal.	Each authorized individual with access to the Partner Portal have his/her own personal unique passwords that are not shared with others.	Concur (Implemented)
7	There was inconsistency between the Commission Policy 97-2 and the Procurement Code Section 2.240 concerning the signature authority.	The County Administration revise and update Commission Policy 97-2 to align with the Procurement Code Sec. 2.240.	Concur (In process of implementation)

BACKGROUND

On December 11, 2017, a MOU was made and entered into by HR and the DHSMV. The MOU established the conditions and limitations under which DHSMV agrees to provide electronic access to driver's license and motor vehicle information to HR.

The authorized HR employees access the Data Exchange database to obtain driver's license transcripts to ensure employees and volunteers possess and maintain a valid driver's license to operate a County vehicle. A driver's license transcript provides detailed driving history, including various violations, suspensions, restrictions, and other information some of which are protected by the Drivers Privacy Protection Act (DPPA). HR obtains driver's license transcripts for every new hire and volunteer prior to hiring or accepting, then annually for those with CDL licenses, and every three years for firefighters.

HR was required to submit an internal control and data security audit on or before the first anniversary (December 11, 2018) of the execution date of the MOU or within 120 days from the receipt of a request from the DHSMV. HR must also submit to the DHSMV an Annual Certification Statement indicating that HR has evaluated and certifies it has adequate controls in place to protect the personal data from unauthorized access, distribution, use, modification, or disclosure, and is in full compliance with the requirements of the MOU and applicable laws.

OBJECTIVE, SCOPE AND APPROACH

The objective of this audit was to determine if HR had appropriate internal controls to ensure that data are protected from unauthorized access, distribution, use, modification, or disclosure.

The scope included verification of compliance with the applicable requirements of the MOU executed on December 11, 2017.

To determine compliance with the MOU, we performed the following:

- Obtained an understanding of the MOU requirements and relevant laws and regulations referenced in the MOU, specifically Florida Statutes Section 282.318, Florida Administrative Code Rule 74-2, and the DHSMV security policies;
- Observed HR's protocols concerning the use of Data Exchange;
- Interviewed HR staff to inquire of protocols regarding the storage of personnel records;
- Reviewed driver's license transcript searches to determine if they were for a legitimate business purpose;
- Compared the Marion County Technology and Security Policies Handbook to the requirements of Florida Statutes Section 282.318, Florida Administrative Code Rule 74-2, and the DHSMV security policies; and
- Compared the newly created policies and procedures concerning the use of Data Exchange to the requirements of the MOU, the DHSMV security policies, and the DPPA.

OPPORTUNITIES FOR IMPROVEMENT

<u>Observation 1</u> – The MOU was signed by an HR employee who did not have the signature authority.

The MOU was signed by an HR employee who did not have the signature authority.

Per Procurement Code Sec. 2-240 and the County Attorney's Office, the County Administrator has the signature authority for procurement of goods and services. The MOU with the DHSMV falls under procurement of service; therefore, the County Administrator should have signed the MOU.

The HR Director stated that the previous MOU had been signed by the HR Manager, so HR followed the precedent.

Signing a contract without having signature authority can create a liability without the knowledge of the County Administration and/or result in the contract being void.

We recommend that HR obtain the County Administrator's signature on the MOU.

Management Response: We concur. There was limited guidance from DHSMV during the signing of the MOU. Our first DHSMV representative who was assisting with the process, Rahkia Robertson, transferred to another department. She was replaced by Rodney Coring, who left the organization and we were not provided with a replacement. We did not receive confirmation that the MOU was complete/accepted until we tracked down our original representative, Rahkia Robertson, who confirmed on February 8, 2018 that our MOU had been officially executed.

We plan to discontinue future use of Data Exchange. We are currently in consultation with DHSMV to identify which data exchange will best suit our needs.

<u>Observation 2</u> – HR management needed to have a thorough understanding of the MOU requirements to ensure compliance.

There was a lack of understanding of the MOU requirements by HR employees who had access to Data Exchange and HR management.

We observed the following:

- There were no written procedures for the authorized users and management to recognize requirements of the MOU and other related security policies.

- HR management asserted that employees with access to personnel files received Public Records Law training which explained that 1) driver's license numbers are exempt from public disclosure and 2) there could be civil and criminal sanctions if violated. However, the employees' acknowledgement of their understanding was not formally documented.

- At the time of the auditor's on-site visit, HR management was not monitoring employee access to the Data Exchange Service to verify business purpose of its use.

Without internal policies and procedures being communicated to the users and management, personnel may not understand what is expected of them and may violate the requirements without a means to be held accountable. The County may be liable for a breach of personal information.

MOU Section V. Safeguarding Information requires:

- "All personnel with access to the information exchanged under the terms of this MOU will be instructed of, and acknowledge their understanding of, the confidential nature of the information;

- All personnel with access to the information will be instructed of, and acknowledge their understanding of the civil and criminal sanctions specified in state and Federal law for unauthorized use of the data; and,

- All access to the information must be monitored on an ongoing basis by the Requesting Party."

We recommend that HR establish written procedures and forms to ensure compliance to the MOU and to clearly communicate the requirements and expectations to the authorized users of the DHSMV system and those who have access to personnel folders.

(Update: Following discussion, HR management subsequently created departmental procedures specific to DHSMV Data Exchange usage.)

Management Response: We concur. All departmental policies, procedures and forms specific to DHSMV Data Exchange usage were reviewed by the auditor and found to be sufficient.

<u>Observation 3</u> – HR should manage Data Exchange user accounts effectively and timely.

HR employees with access to the Partner Portal were not familiar with the Partner Portal Web Application User Guide and were not knowledgeable of how to manage access properly. As a result, we observed the following:

- A former HR employee was still listed as the administrator of the DHSMV Partner Portal, a web application to manage accounts and banking information.
- A present HR employee was not aware that she had two separate user accounts in Partner Portal.
- There was an unknown service account user who had access to the Data Exchange site.

(Update: The Partner Portal Web Application User Guide was located in HR records and auditor shared it with HR employees during an on-site visit. Auditor observed that the unknown service account was disabled during the on-site visit).

If access is not properly managed, it can lead to unauthorized users accessing DHSMV applications resulting in a breach of personal information.

MOU Section IV.B.10 & 11 states that the Requesting Party agrees to "update user access/permissions upon reassignment of users within five (5) business days," and "immediately inactivate user access/permissions following separation, or negligent, improper, or unauthorized use or dissemination of any information."

We recommend that HR designate an administrative account holder who will timely manage user accounts in Partner Portal.

Management Response: We concur. The point of contact (HR employee) is supposed to have two user accounts, one to pull MVR reports in the Partner Portal and one Service Account. She did not realize that she had created two user accounts in Partner Portal. Once this was discovered the duplicate account was deleted.

Our prior point of contact went to work at one of our constitutional offices May 31, 2019, and continued to provide training to the new point of contact, so her "Service Account" status was not revoked immediately after her departure. It was disabled after the initial audit meeting November 19, 2019.

HR has designated an administrative account holder to timely manage user accounts in Partner Portal.

<u>Observation 4</u> – **HR needs to comply with the Internal Control and Data Security Audit Requirements.**

MOU Section VI.A. Compliance and Control Measures requires an Internal Control and Data Security Audit from a qualified party on or before the first anniversary of the execution date of the MOU. The required audit was due on December 11, 2018.

HR management was not familiar with the MOU requirements concerning the time frame for an audit. Internal Audit received the first inquiry regarding an audit concerning the MOU on August 21, 2019, and a formal audit request on October 23, 2019.

As a result, HR was in technical breach of the MOU and at risk for data access being terminated.

We recommend that HR management be familiar with contract terms and implement methods to ensure timely completion of required actions.

Management Response: We concur. HR received an audit reminder from DHSMV in July 2019. At that point we exchanged numerous emails with our contact from DHSMV, Matthew Strickland, for guidelines of what should be included on the audit, who should conduct it, etc. When he was unable to provide guidelines, we requested a sample of an audit. We were told, “This is a new process. We don’t have one. Just send us a draft and we will tell you if it is correct.” For weeks we emailed Matthew Strickland for guidance on who in our organization was qualified to conduct the audit, ruling out our IT department because they did not have the required certifications. Once they confirmed that our internal auditor should do the audit we reached out to Internal Audit/Sachiko Leon on August 21, 2019 for assistance and were told that the earliest they could conduct an internal audit would be October 2019.

During one telephone conversation with Matthew Strickland, HR mentioned their concern for timeliness of the audit. His response was, “As long as you are making efforts to do the audit and communicating your progress to us, you will not be in breach of contract.”

<u>Observation 5</u> – Driver's license transcripts need to be labeled as confidential.

HR employees were not familiar with the security requirements of the MOU.

DHSMV Vendor IT Security Policy #A-02: Data Security, Section 7.0 Data Classification provides the following: "To ensure the security and integrity of all data, any data asset is Public, Sensitive or Confidential and should be labeled accordingly."

Additionally, information in driver's license transcripts is protected by the DPPA.

As of November 26, 2019, HR did not label personnel records in the personnel files, including driver's license transcripts, as confidential to protect personal information.

Without proper labeling of the confidentiality of personal information such as driver's license transcripts, employees or people who request to review personnel files may allow access to or disclose confidential information.

We recommend that HR create procedures to label personnel information as public, sensitive, or confidential. Specifically, driver's license transcripts printed and placed in personnel files should be labeled as confidential.

Management Response: We concur. Immediately after the first audit meeting, HR began stamping driver's license transcripts as confidential at the recommendation of the auditor. Although they were not physically stamped confidential, staff still protects the personal information by excluding the transcripts when personnel files are requested.

<u>Observation 6</u> – Passwords must not be shared.

Employees were not familiar with the Partner Portal Web Application User Guide and the IT security requirements. As a result, the two authorized Data Exchange users were sharing a password to log into Partner Portal.

DHSMV Vendor IT Security Policy #A-04: Passwords 2.0 Policy and Standards provides the following:

- "Passwords, which are the first line of defense for the protection of the Departments information resources, must be treated as sensitive information and must not be disclosed;
- Passwords must not be divulged to anyone. Passwords must be treated as confidential information and should be safeguarded; and,
- Passwords and usernames should not be shared with anyone to include co-workers or contractors."

Sharing of passwords creates security risk. In the event of inappropriate account activity or breach of personal information, the responsible person will not be easily identified.

We recommend that each authorized individual with access to the Partner Portal have his/her own personal unique passwords that are not shared with others.

*(Update**:** During an on-site visit, auditor observed an HR employee create a separate user account which eliminated the need to share one account and password.)*

Management Response: We concur.

<u>Observation 7</u> – There was inconsistency between the Commission Policy 97-2 and the Procurement Code Section 2.240 concerning the signature authority.

Commission Policy 97-2 states that "all contracts for services … must be submitted to the Marion County Board of County Commissioners for approval and execution." These requirements do not align with the requirements of the Procurement Code.

Procurement Code Sec. 2.240 – Authority of County Administrator or his or her designee states that "the procurement of all goods and services shall be under the supervision and management of the County Administrator or his/her designee."

Through consultation with the County Attorney's office, it was advised that the Procurement Code supersedes the Commission Policy; therefore, it is the recommendation of the County Attorney's Office to repeal Commission Policy 97-2 for consistency.

Conflicting policies do not allow for clarity or provide clear guidelines and is a weakness of internal controls.

We recommend that the County Administration revise and update Commission Policy 97-2 to align with the Procurement Code Sec. 2.240.

Management Response (County Administration): Concur. We are continuing to develop and update our policies and will work with the County Attorney's Office to ensure the Commission Policy is presented to the board for approval to repeal.

Management Response (HR): We concur. We shared the information with the County Attorney's Office and they are working with Administration to present the Commission Policy to the board for approval to repeal.

CLERK OF THE CIRCUIT COURT AND COMPTROLLER
David R. Ellspermann

MEMORANDUM

TO: **Richie Frederick, Chief Bureau of Records**

FROM: **Sachiko Horikawa, Internal Audit Director**

RE: **Audit of Contract Number HSMV-0302-18**

DATE: **August 21, 2020**

As per a requirement of Contract Number HSMV-0302-18, "Memorandum of Understanding For Driver's License and/or Motor Vehicle Record Data Exchange" (MOU), an audit of the MOU has been performed by the Internal Audit Department for the Marion County Board of County Commissioners (County).

I, Sachiko Horikawa, Internal Audit Director, certify the following:

- The internal controls governing the use and dissemination of personal data have been evaluated in light of the requirements of the 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 data security procedures/policies have been approved by the Security Officer and the Director of Information Technology Department (IT), who would be considered "Risk Management IT Security Professional" as specified in the MOU.
- Any and all deficiencies/issues found during the audit have been corrected or measures enacted to prevent recurrence.

The following measures are in the process of implementation to rectify the existing conditions as of the date of this memorandum.

- The MOU was signed by a HR employee who did not have the signature authority. HR is currently in consultation with DHSMV to identify which platform will best suit their needs.
- The IT Security Policy of Marion County Board of County Commissioners needed to be enhanced by including a risk assessment and an incident response plan. The IT management expects to have the first draft of both plans by the end of quarter one of calendar year 2021.
- There are inconsistencies between the County's Procurement Code Sec. 2.240 and the Commission Policy 97-2 whether the Board or the County Administrator has the

---

Marion County Clerk of the Circuit Court and Comptroller
Board of County Commissioners – Internal Audit Division – Sachiko Horikawa, Internal Audit Director
Post Office Box 1030 • Ocala Florida 34478-1030 • Telephone (352) 671-5604 • Facsimile (352) 671-5625 •
www.marioncountyclerk.org

CLERK OF THE CIRCUIT COURT AND COMPTROLLER
David R. Ellspermann

signature Authority for the MOU. The County Attorney's Office determined that the Procurement Code Sec. 2.240 superseded the Commission Policy 97-2; therefore, the County Administrator has the signature authority. The County Administration will revise and update Commission Policy 97-2 to align with the Procurement Code Sec. 2.240 and present the Commission Policy to the board for approval to repeal.

Also reviewed and certified by:

Mounir Bouyounes, County Administrator

Marion County Clerk of the Circuit Court and Comptroller
Board of County Commissioners – Internal Audit Division – Sachiko Horikawa, Internal Audit Director
Post Office Box 1030 • Ocala Florida 34478-1030 • Telephone (352) 671-5604 • Facsimile (352) 671-5625 •
www.marioncountyclerk.org

REPORT DISTRIBUTION LIST

Name	Position Title
The Honorable Kathy Bryant	Chairman of the Board of County Commissioners
The Honorable Jeff Gold	Vice Chair of the Board of County Commissioners
The Honorable David Moore	District 1 Commissioner
The Honorable Carl Zalak	District 4 Commissioner
The Honorable Michelle Stone	District 5 Commissioner
Mounir Bouyounes	County Administrator
Jeannie Rickman	Assistant County Administrator – Public Services
Guy Minter	County Attorney
Dana Olesky	Chief Assistant County Attorney
Amanda Tart	Human Resources and Risk and Benefits Director
Tom Northey	Information Technology Director
Robyne Fraize	Human Resources Manager