Office of the City Auditor

City of Gainesville, Florida

Florida Highway Safety and Motor Vehicles Data Exchange Compliance Audit

June 1, 2022

Ginger Bigbie, CPA, CFE, City Auditor
200 E University Avenue, Room 211 Gainesville, FL 32601
352.334.5020

GAINESVILLE CITY COMMISSION

Lauren Poe, Mayor
David Arreola
Cynthia Chestnut
Desmon Duncan-Walker
Adrian Hayes-Santos
Reina Saco, Mayor-Commissioner Pro Tem
Harvey Ward

AUDIT COMMITTEE MEMBERS

Lauren Poe, Mayor
Reina Saco, Mayor-Commissioner Pro Tem
Harold Monk, CPA, CFE (Appointed)

TABLE OF CONTENTS

Florida Highway Safety and Motor Vehicles
Data Exchange Compliance Audit

Executive Summary

What We Did

The objective of this engagement was to assess the design and operating effectiveness of controls related to the Florida Highway Safety and Motor Vehicles data exchange processes from February 6, 2020 through April 30, 2022. We performed the audit through inquiry, observation, and substantive testing for processes in scope. Specifically, we:

Legal and Regulatory Policies and Procedures

- Reviewed the adequacy and completeness of policies and procedures in compliance with the Memorandum of Understanding for Driver's License and/or Motor Vehicle Record Data Exchange, between the Florida Highway Safety and Motor vehicles and the City of Gainesville.
- Assessed the adequacy of management oversight and monitoring related to changes in policies and procedures.

IT and Application Policies, Procedures, and Controls

- Reviewed internal controls and processes for user access control, vulnerability management, data classification and security, and periodic monitoring.
- Obtained and analyzed data for all controls in scope.
- Selected controls to test for compliance with policies, procedures, and the data exchange process.

What We Found

Based on the results of this engagement, the City of Gainesville complies with all of the Florida Highway Safety and Motor Vehicles Data Exchange compliance requirements as stated in the Memorandum of Understanding (MOU) between the State of Florida and the City. There are no areas of non-compliance or audit issues identified.

Auditor's Note: During this engagement, we noted the Risk Management office has not been able to successfully run the HSMV Data Exchange application and perform related procedures since the City implemented the new ERP system in July 2021. While this does not impair compliance with the FLHSMV data exchange MOU, it does increase the risk that the City's data exchange program objectives will not be met or issues with the data exchange process will not be identified and resolved timely.

We have discussed the risk with the responsible party and Risk Management Professional, David Jarvis (Workers' Compensation & Loss Control Manager). Internal Audit will continue to track the risk in ongoing enterprise risk assessment activities.

We would like to thank, Risk Management and IT personnel for their cooperation and professionalism throughout this audit.

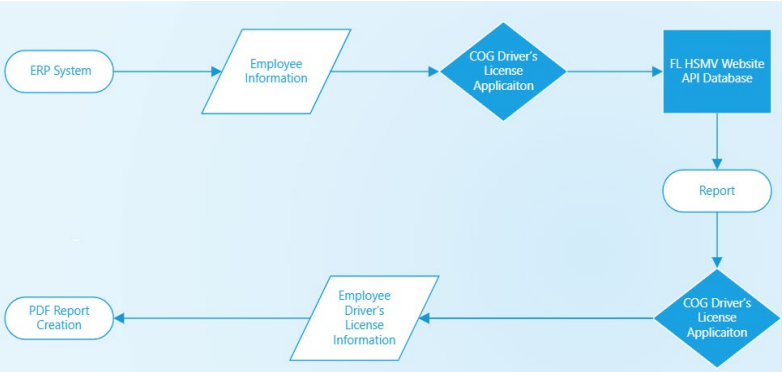
INTRODUCTION

The Florida Department of Highway Safety and Motor Vehicles (FLHSMV) requires the City to submit an Internal Control and Data Security Audit on or before the first anniversary of the Memorandum of Understanding No. 0126-22 (MOU). The MOU between FLHSMV and the City was executed on 08/31/2021.

BACKGROUND

To comply with the insurance policy for City owned motor vehicles, and Federal Transit Administration and Department of Transportation regulations, employee drivers' licenses are reviewed annually and Commercial Driver's License holders every 6 months to ensure they do not have suspended or revoked licenses. The process would take a considerable amount of resources to run each employee's driving history separately. Instead, a batch process is run between the City and the FLHSMV information systems (see Figure 1 – Data Exchange Process Overview)

Figure 1. Data Exchange Process Overview



Legend: Shaded boxes highlight the Driver's License Application and the FLHSMV Database

To review driver's license information, the Worker's Compensation and Loss Control Manager creates a confidential spreadsheet of employee driver's licenses from the City's ERP application. This Manager is the only staff authorized to upload the spreadsheet into the data extract application. The Driver's License Application submits a request directly to the FLHSMV system and the results are stored in an internal database.

Once the data exchange process is completed, the five years driver's license history data extracted from the State's system is available for Risk Management review following City procedure and using the driver's license extract application.

SCOPE AND METHODOLOGY

The scope of this review included an assessment of the design and operating effectiveness of controls related to the data exchange processes from February 6, 2020 through April 30, 2022. We performed the audit through inquiry, observation, and substantive testing for processes in scope. Specifically, we:

Legal and Regulatory Policies and Procedures

- Reviewed the adequacy and completeness of policies and procedures in compliance with the MOU.
- Assessed the adequacy of management oversight and monitoring related to changes in policies and procedures.

IT and Application Policies, Procedures, and Controls

- Reviewed internal controls and processes for User Access Control, Vulnerability Management, Data Classification and Security, and Periodic Monitoring.
- Obtained and analyzed data for all controls in scope.
- Selected controls to test for compliance with policies, procedures, and the data exchange process.

The fieldwork categories in scope were reviewed based on all compliance requirements provided in the MOU that consisted of the Statement of Work agreements and Section V, Safeguarding Information. To ensure that the audit covered the MOU requirements, control requirements were tested from each section where applicable. The Auditor identified 18 primary compliance topics required in the MOU.

Specifically, we tested:

1. Security policies and procedures.
2. Security incident communication policy.
3. Documentation of Confidentiality nature of information training.
4. Policies and procedures for notifying the State of Florida within 5 business days of any violations with the MOU.
5. Physical Security: facility monitoring (surveillance systems, camera, guards, exterior lighting), alarm systems (fire, burglary, water humidity, power), secure storage of back-up data drives.
6. Logical Security: antivirus / malware protection, firewalls, intrusion detection systems.
7. Business Continuity and Disaster Recovery Plans.
8. In scope asset vulnerability patch status.
9. Remote access to the Driver's License Application.
10. Connection to data extract application encryption .
11. Data encryption during transit using TLS 1.2 or later.
12. Documentation for preventative maintenance schedule and quarterly maintenance schedule
13. The data extract application, databases, and driver license folder accessibility from outside the network.
14. Least privilege user access.
15. Monitoring mechanisms to identify unauthorized access, distribution, use, modification, or disclosure to the application, databases, and Driver's License Folder.
16. Log review.
17. Periodic monitoring / review frequency.
18. In scope asset device inventory

RESULTS

Testing results for the 18 required compliance topics are summarized below.

1. **Security policies and procedures –** Section V, letter D of the MOU states that the City shall develop and employ adequate security measures to protect information. The City has a current Cyber Security Incident Response plan (IRP) to provide guidance when addressing cybersecurity

incidents, which may impact the organization's operational, financial, or reputational standing, or the ability to comply with regulatory and legal requirements. The IRP satisfies compliance requirements.

2. **Security Incident Communication Policy –** Section V, letter D of the MOU states that the City shall develop and employ adequate security measures to protect information. The City maintains a Cyber Security Incident response plan, which provides a framework for how incidents are communicated to stakeholders throughout the City and the various situations, which might trigger a communication effort. The IRP meets communication policy compliance requirements.

3. **Documentation of Confidentiality nature of information training -** Staff are informed about the confidential nature of the Driver's License Application and information therein, through mandatory staff online training prior to gaining access. The auditor validated that users with access to the application had completed the training. The application and data access limitations are on a City share site accessible through the following link: http://confluence/display/APPDEV/COG-Drivers+License+Report#COG-DriversLicenseReport-ApplicationandDataAccessLimitations. No exceptions were noted.

4. **Policies and procedures for notifying the State of Florida within 5 business days of any violations with the MOU. –** Section V of the MOU states that the FLHSMV must be notified within five business days of a violation of the MOU. Risk Management does have a policy in place to notify the State of Florida within five business days of any violations with the MOU. The risk management office does have a policy and procedure in place to notify the state within five days of a violation. There were no past violations to test this procedure. No exceptions were noted.

5. **Physical Security: Facility monitoring (surveillance systems, camera, guards, exterior lighting), Alarm systems (fire, burglary, water humidity, power), Secure storage of back-up data drives. -** The MOU's Section V, Safeguarding Information, bullet C states that data exchange information is to be stored in a location that is physically and logically secure from access by unauthorized persons.

   The EOC facility has a manned guard shack. Entry to the facility is controlled through automated gates. The data center at the EOC is in a self-contained building with 24-hour staffing and multiple security checkpoints.. Access requires sign in logs to verify each person and purpose. The Auditor toured the facility and obtained images provided by management showing other physical security controls. These controls sufficiently meet the MOU's requirement that data exchange information is secure from unauthorized persons. No exceptions were noted.

6. **Logical Security: Antivirus / Malware protection, Firewalls, Intrusion detection systems. Badge access is appropriately restricted.**
   The MOU's Section V, Safeguarding Information, bullet C states that data exchange information is to be stored in a location that is physically and logically secure from access by unauthorized persons.

   The driver's license application is stored at the Gainesville Regional Utilities Data Center. Adequate logical security controls included antivirus software, firewall from the production

application to the FLHSMV database, surveillance video cameras, and a locked safe to store backups. There is also an Intrusion Detection system. This can be viewed with both a Business perspective and an IT perspective.

From the Business Perspective, the IDS appliances provide network security alerts for both traditional and advanced network threats, helping organizations identify malicious activity.

From the IT Perspective, the IDS systems provide network security alerts for the identification and reporting of malicious events..

The logical security controls were provided by management due to needing privileged access to sensitive cyber security assets. After review, the layering of all of the logical security controls are adequately designed to minimize risk of unauthorized access. These controls sufficiently meet the MOU's requirement. No exceptions were noted.

7. **Business Continuity and Disaster Recovery Plans -** Section V, letter D of the MOU states that the City shall develop and employ adequate security measures to protect information. This includes the establishment of Business Continuity and Disaster Recover Plans. The current state of the Disaster Recovery Plan does comply with the MOU. Management is in the process of strengthening the Disaster Recovery Plan which will be reviewed in the 2022 cybersecurity internal audit. These controls sufficiently meet the MOU's requirement. No exceptions were noted.

8. **In Scope Asset vulnerability patch status -** Section V, letter D of the MOU states that the City shall develop and employ adequate security measures to protect information. All in-scope assets were assessed showing that they were up to date with no known vulnerabilities currently outstanding. The auditor requested that an administrator run a command in Windows PowerShell to show what patches had been applied to each in-scope server. The auditor then compared results to the latest release of Microsoft Patches to verify there were not any outstanding known vulnerabilities. These controls sufficiently meet the MOU's requirement. No exceptions were noted.

9. **Remote access to the Driver's License Application –** Section V, letter E of the MOU states that unauthorized persons cannot view, retrieve, or print information. The application was tested to ensure that remote users would be unable to access, view, retrieve or print information. The Driver's License Application is not accessible remotely. These controls sufficiently meet the MOU's requirement. No exceptions were noted.

10. **Connection to data extract application encryption -** Section V, letter I of the MOU states that Transport Layer Security (TLS) version 1.2 or higher must be used. The connection the Driver's license application makes is secured over HTTPS using TLS 1.2 or above as required by the FLHSMV service. These controls sufficiently meet the MOU's requirement. No exceptions were noted.

11. **Data encryption during transit using TLS 1.2 or later -** Section V, letter I of the MOU states that Transport Layer Security (TLS) version 1.2 or higher must be used. The internal Web Application requires an HTTPS connection and is secured using at least TLS 1.2. These controls sufficiently meet the MOU's requirement. No exceptions were noted.

12. **Documentation for Preventative Maintenance Schedule and Quarterly Maintenance Schedule** – Section V, letter H states that All access to the information must be monitored on an ongoing basis by the Requesting Party. In addition, the Requesting Party must complete an Annual Certification Statement to ensure proper and authorized use and dissemination of information and provide it to the Providing Agency. To comply, the City has preventative maintenance schedules, quarterly activity audits, annual MOU reviews, and maintains a Cyber Security Incident response plan. These controls sufficiently meet the MOU's requirement. No exceptions were noted.

13. **The data extract application, databases, and driver license folder accessibility from outside the network –** Section V, letter E of the MOU states that unauthorized persons cannot view, retrieve, or print information. Access from outside of the network was tested. Accounts with permissions and without permissions were not able to access the application from outside of the City of Gainesville's corporate network. These controls sufficiently meet the MOU's requirement. No exceptions were noted.

14. **Least Privilege -** The FLHSMV MOU section V Safeguarding Information, item E specifies that Access to the information received from the Providing Agency will be protected in such a way that unauthorized persons cannot view, retrieve, or print the information.

    For Internal Access: The auditor worked with a domain administrator to ensure the practice of least privilege is implemented on the in-scope servers and databases. There are currently two risk management professionals that have rights to view, retrieve, or print the information on the application itself.

    For External Access: The DMZ is a specially controlled network located between the external network (Internet) and the internal network. It represents a buffer zone that separates the networks by strict communication rules and firewalls.

    The Drivers License Report Application is not hosted in the corporate DMZ and is not publicly available. The different web application tiers for the driver's license application are available at the following locations on the corporate network.

Figure 2. DL Application Websites

FUNCTION	URL
Production Web Site	https://ggwebservices.gruadmin.gru.com
QA Web Site	https://ggwebservices-qa.gruadmin.gru.com
Development Web Site	https://ggwebservices-dv.gruadmin.gru.com

The driver's license application is not available to any direct VPN or remote access. The driver's license application is available on the corporate network to authorized staff who successfully negotiate a VPN connection to their workstation or laptop as if they were physically present. These controls sufficiently meet the MOU's requirement. No exceptions were noted.

15. **Monitoring mechanisms to identify unauthorized access, distribution, use, modification, or disclosure to the application, databases, and Driver's License Folder** – Section V, letter H states All access to the information must be monitored on an ongoing basis by the Requesting Party. There are quarterly activity audits performed and stored here: Quarterly Activity Audits - IT Application Development - Confluence. These controls sufficiently meet the MOU's requirement. No exceptions were noted.

16. **Log review -** Section V, letter H states All access to the information must be monitored on an ongoing basis by the Requesting Party. Activity Logs are reviewed by management on a quarterly basis. The auditor reviewed the logs to ensure authorized and unauthorized access attempts are tracked, as well as successful and unsuccessful authentication. Logs that were reviewed to show compliance with the MOU are below:

    - AuthenticationSuccess
    - AuthenticationFailure
    - Authorized
    - Unauthorized
    - AddSession
    - ViewLicenseSummaries
    - ViewLicenseDetails
    - ViewLicensePdf
    - SubmitLicenseBatchUpload
    - GetLicenseUpdate
    - GetLicenseReprint

17. **Periodic Monitoring / Review Frequency -** Section V, letter H states All access to the information must be monitored on an ongoing basis by the Requesting Party. In addition, the Requesting Party must complete an Annual Certification Statement to ensure proper and authorized use and dissemination of information and provide it to the Providing Agency. The City complies with this

requirement by performing quarterly audits and through submission of the annual certification statement. These controls sufficiently meet the MOU's requirement. No exceptions were noted.

18. **In Scope Asset device inventory -** The I.T. department manages I.T. asset inventory differently, depending on the type of asset. There are two broad classifications for the I.T. assets physical vs. virtual and networking vs. servers. The in-scope assets for the Data Exchange application are on virtual servers. There are no physical servers in-scope. Inventory of virtual I.T. assets in scope are held within VMWare. The networking assets are physical assets that are tracked through the SolarWinds Application. Upon review of all in-scope assets it was determined that the in-scope devices were in compliance with the data classification attributes as expected. The handling, identification, and classification is addressed for all in-scope assets. These controls sufficiently meet the MOU's requirement. No exceptions were noted.

CONCLUSION

Based on the results of this engagement, the City of Gainesville complies with the Florida Highway Safety and Motor Vehicles MOU. No exceptions were noted.

Auditor's Note During this engagement we noted the Risk Management office has not been able to successfully run the HSMV Data Exchange application and perform related procedures since the implementation of the new ERP system in July 2021. While this does not impair compliance with the FLHSMV data exchange MOU, it does increase the City's risk that the City's data exchange program objectives will not be met or issues with the data exchange process will not be identified and resolved timely.

We have discussed the risk with the responsible party and Risk Management Professional, David Jarvis (Workers' Compensation & Loss Control Manager) who was aware of this. Internal Audit will continue to track the risk in ongoing enterprise risk assessment activities.

GOVERNMENT AUDITING STANDARDS COMPLIANCE

We conducted this audit engagement in accordance with *Generally Accepted Government Auditing Standards* and the *International Standards for the Professional Practice of Internal Auditing*. Those standards require that we plan and perform the engagement 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 observations and conclusions based on our audit objectives.

INTERNAL AUDIT TEAM

Ginger Bigbie, CPA, CFE, City Auditor
Brecka Anderson, CIA, CFE, CGAP, Assistant City Auditor
Ryan Timmons, CISSP, MCSE, IT Audit Manager (Lead Auditor for this engagement)
Diana Ferguson-Satterthwaite, FCCA, CIA, Senior Internal Auditor