LEGISTAR #190923

FINAL AUDIT REPORT

Audit of Internal Controls and Data Security for the use of Driver's License and Motor Vehicle Record Data Exchange

February 6, 2020

FINAL AUDIT REPORT

A Report to the City Commission

City of Gainesville
Office of the
City Auditor

Interim City Auditor
Leonard F. Loria, CPA

Audit of the Internal Controls and Data Security for the use of Driver's License and Motor Vehicle Record Data Exchange

EXECUTIVE SUMMARY
February 6, 2020

Why We Did This Audit

The Department of Highway Safety and Motor Vehicles required the City submit an Internal Control and Data Security Audit on or before the first anniversary of the Memorandum of Understanding No. 0124-19.

What We Recommend

Key actions City Management should take:

- Security Incident Handling Policy should include reportable FLHSMV events and when to report.
- Ensure systems are adequately patched.
- Classify and categorize information systems.
- Mitigate known vulnerabilities.
- Test in-scope systems at least annually.
- Disable generically named user accounts where appropriate.
- Review and formally approve user access.
- Monitor user activities.
- Encrypt data in transit.

BACKGROUND

The Memorandum of Understanding HSMV-0124-19 (MOU) between the Department of Highway Safety and Motor Vehicles (HSMV) and the City of Gainesville (City), was fully executed on September 28, 2018. The City and Gainesville Regional Utilities utilize a modified self-insured program for protecting itself against losses. The City is self-insured for both automobile and general liability losses.

To comply with insurance and Federal Transit Administration and Department of Transportation regulations, employees' driver's licenses are reviewed twice a year to ensure they do not have suspended or revoked licenses.

OBJECTIVES

The objectives of the audit were the following:

- Certify that the data security policies and procedures have been approved by a Risk Management IT Professional.
- Any and all deficiencies/issues found during the audit have been corrected and measures enacted to prevent reoccurrence.

WHAT WE FOUND

The City requests driver's license information from the FLHSMV data exchange only for purposes authorized in the MOU. This is the first year that the City has been audited for use of the data exchange and the security controls surrounding driver's license data. We identified data security controls that did not align with the MOU requirements, including:

- Strengthening the Security Incident Handling Policy.
- Not all server update patches were installed for in-scope systems.
- IT assets were not classified in accordance with the External Information Systems Security Policy.
- Identified information systems' vulnerabilities need to be examined and controls implemented.
- The Business Continuity Plan did not include the in-scope systems.
- The use of generically named user accounts.
- Access to driver's license information obtained without appropriate approval.
- User activities were not recorded or reviewed.
- Information transmitted to and from the data extract application was not secure.

SCOPE AND METHODOLOGY

This engagement concentrated on the City's compliance with the MOU's requirements during the period September 28, 2018 to September 27, 2019. During the engagement, we attended meetings, interviewed key personnel, observed and mapped processes, performed a process risk assessment questionnaire, and examined documents provided by General Government's Risk Management and the Gainesville Regional Utility IT Departments (GRU IT).

The audit methodology was based on the requirements provided in Section V, *Safeguarding Information*, of the MOU. To ensure that the audit covered the MOU requirements, we cross-walked the data security controls included in the MOU and the External Information Security Policy, where applicable.

RELATED FACTS AND FIGURES

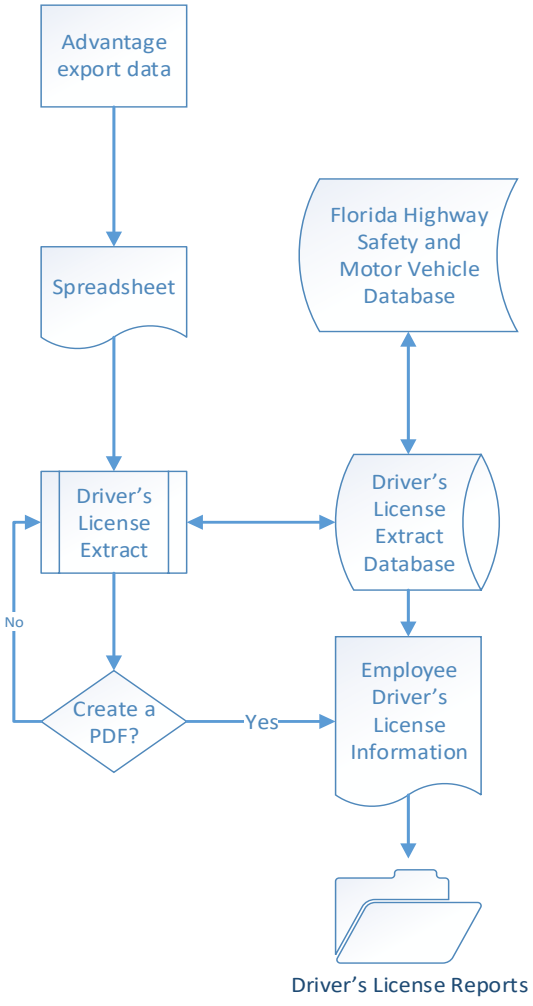

Figure 1 – Data Exchange Process Overview

The City's Risk Management Department reviews employee licenses twice a year, once for CDL drivers and once for all employees to ensure that the City's drivers 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).

To review driver's license information, the Worker's Compensation and Loss Control Manager creates a spreadsheet of employee driver's licenses from the City's Advantage application. This Manager is the only staff authorized to upload the spreadsheet into the data extract application. A request is made directly to the HSMV 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 is available for review using the driver's license extract application.

The data extract application allows users to view each employee's driver's license history information on their screen. An additional feature is the ability to create a PDF of individual employee's driver's license information. PDF copies of City employees who have suspended, revoked, or point totals that may lead to suspension, are stored in the Driver's License Reports folder.

OBJECTIVES AND CONCLUSIONS

1. **Is information exchanged only used as authorized by the MOU?**
   Yes. In the MOU, there are 14 exemptions that allow the use of driver's license information. The City is qualified for two Driver's Privacy Protection Act exemptions as a local government and self-insured entity. The data is used by the City to comply with insurance and FTA/DOT regulations to ensure that employees driving City vehicles do not have suspended or revoked licenses.

   We examined activity log files between October 2018 and June 2019, and polled users on their use of the information. We determined that driver's license data exchange was used in accordance with the exemptions listed in the MOU.

2. **Is information securely stored (physically and logically)?**
   Yes. 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. We sent a process self-assessment questionnaire to 12 employees with access to the data exchange information and asked them to list the location(s) where they stored motor vehicle personal data. None of the recipients responded that they stored physical copies. However, we did identify a shared network folder used to store electronic copies of employee driver's license information (see Objective No. 4 – Least Privilege | Segregation of Duties section for details).

   The driver's license information 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 backup.

3. **Does the City's data security controls and standards align with the MOU?**
   Generally Yes. The MOU's Section V*, Safeguarding Information*, bullet D states the City shall develop security requirements and standards consistent with Section 282.318, Florida Statutes, Florida Administrative Code Rule 74-2[1], and the FLHSMV *External Information Security Policy* to ensure the protection of FLHSMV information, applications, data, resources and services. We compared policies and procedures, security patches, asset inventory lists, vulnerability assessments, and the business continuity plan to the MOU's requirements.

   Our results are as follows:

   Data Security Policies and Procedures:
   We examined policies and procedures related to access controls, network security, personnel security, asset management, asset disposal, acceptable use, data privacy, data center security, business continuity, and security incident handling. Many of the provided policies and procedures met the required security requirements. For example, the password parameters required to access the data are in alignment with the FLHSMV External Information Security Policies #A-04: Passwords Parameters.

[1] Effective on February 5, 2019, Florida Administrative Code Rule Chapter 74-2 was transferred to Rule Chapter 60GG-2 Information Technology Security and is known as the Florida Cybersecurity Standards.

However, in our examination of the provided security incident handling policy, we noted the policy did not include a list of reportable incidents or when to report such events. Reportable events include:

- Physical loss, theft, or destruction of FLHSMV data.
- Unauthorized disclosure, access, sharing user credentials, unauthorized activity, or transmission of data using FLHSMV information resources.
- Data that has been altered or destroyed or access that is denied outside of normal business hours.
- Lost identification badges.
- Violation of any portion of the External Information Security Policy.

Strengthening the security incident handling policies increases management's ability to ensure that events involving the in-scope information systems, whether suspected or proven, which pose a threat to the confidentiality, integrity and availability of the driver's license information, are properly handled. The MOU also requires the City to report such events within five business days of discovery (see Observation A).

Security Patch Updates:
Patching is a process of applying updates to improve the security of the software that runs the information systems. Prior to the IT Quarterly Maintenance, we examined the status of the in-scope server's operating system security updates and identified that 39 patches were available for implementation. During the IT Quarterly Maintenance, performed on December 8, 2019, we noted that 29 of the 39 patches (74%) were implemented on the in-scope systems. Upon our inquiry, an additional four patches were applied to the development database server. The Gainesville Regional Utilities IT Department should review the remaining patches and determine whether they are critical to the data security of the in-scope systems. Operating with outdated patches, information systems are at an increased risk of compromise from known vulnerabilities (see Observation B).

IT Asset Management:
The Florida Highway Safety and Motor Vehicles External Information Security Policy #A-02: Data Security *7.0, Data Classification*, requires that the City abide by the data classification in accordance with Federal Information Processing Standards (FIPS) Publication 199. During the audit period, we noted that IT assets were stored on spreadsheets and were also available for review on an internal portal. The lists are updated approximately every six months and included the item name, description, model number, serial number, location, cost and end of support date.

We identified that the in-scope systems were not classified as either Public, Sensitive, or Confidential as required in the policy. Without the categorization, information systems' management may not allocate the resources necessary to protect the data as well as determine the potential loss or damage from the corruption, loss, or disclosure of driver's license data (see Observation C).

Risk Assessments:
A risk assessment is a systematic process of evaluating the potential risks that may occur. Presently, the City does not perform risk assessments on their information systems. Instead, vulnerability scans are performed by the Gainesville Regional Utilities IT Department. Previously however, they did not include the in-scope systems. Upon our notification, vulnerability scans were performed and

identified 10 critical and 53 high vulnerabilities to the in-scope systems. The 63 vulnerabilities need to be examined and actions taken to reduce the data risk and enact measures to prevent recurrence (see Observation D).

Business Continuity Plan:
For the in-scope systems, GRU IT performs weekly incremental backups and full backups on a monthly basis. Copies of the backups are replicated to an off-site location. However, the provided Disaster Recovery Plan needs strengthening to align with the MOU's requirement that security is consistent with Florida Cybersecurity Standards to protect FLHSMV data and resources.

Specifically, 60GG-2.003 *Protect Information, Protection Processes and Procedures Number 9* and 60GG-2.006 *Recover, Recovery Planning Improvements Number 1* states the City establish, manage, and incorporate lessons learned in recovery plans. Strengthening the Disaster Recovery Plan will help management identify potential scenarios that are likely to give rise to a significant disruption and the business and technical options available to recover operations. According to the Gainesville Regional Utilities Governance and Compliance IT Manager, the IT Disaster Recovery Plan is being updated in 2020 (See Observation E).

4. <u>Are unauthorized users able to view, retrieve, or print information exchange data?</u>
Yes. The MOU's Section V, *Safeguarding Information,* bullet E states that access to the information received from the HSMV will be protected in such a way that unauthorized persons cannot view, retrieve, or print the information. We examined user accounts to (1) determine if they were uniquely identifiable, (2) align with least privilege and segregation of duties controls, and (3) if users were adequately on-boarded and off-boarded. Our results are as follows:

Uniquely Identifiable:
Assigning a unique identification (ID) to each person with access ensures that an individual is uniquely accountable for their actions. During our testing, we found a spreadsheet containing 166 individual driver's license information that was accessible through the internal network via anonymous access. Upon our notification, the spreadsheet was immediately removed from the network.

We also identified generically named user accounts. Generically named accounts reduce the information systems' ability to track individual high-risk user actions. Additionally, the user accounts, specifically with administrator access, could be used to bypass existing identity access management controls (see Observation F).

Least Privilege | Segregation of Duties:
Least privileged user access should only allow minimal access that is necessary for users to accomplish assigned tasks in accordance with their job duties. There were 10 user accounts with access to the data extract application. In our testing, we identified two employees who did not directly log-on to the application, three developers that were not responsible for the maintenance of the application, and one employee who had retired 261 days earlier. Additionally, through the use of the data extract application's PDF feature, we identified 16 GRU trainers who were not approved by the Worker's Compensation and Loss Manager that had access to 135 driver's license reports in a shared folder.

The segregation of duties for individual user accounts is necessary to prevent malevolent activity of driver's license data without collusion. During our access testing we identified that the Gainesville Regional Utilities IT Application Development Manager had administrator access to the data extract application and the production database, but was no longer responsible for the development of the application or related database.

On-boarding | Off-boarding:
Typically, user access activation and deactivation requests are entered into the WISDOM ticketing system where the supervisor approves or disapproves the access request. The Worker's Compensation and Loss Control Manager, a General Government employee, is responsible for approving access to the driver's license information. However, we learned that access was granted to the Utility Safety and Training Facilitator from Gainesville Regional Utilities to assist with verifying driver's licenses. Subsequently, the Worker's Compensation and Loss Control Manager was unaware that a folder was created to store driver's license information (see Related Facts and Figures section) and an additional 17 users had access to the stored reports.

Access to the driver's license information was granted without appropriate approval to various GRU departments. User access should be reviewed and formally approved by the Worker's Compensation and Loss Control Manager to ensure that access provided is the minimum necessary to perform job duties and prevent malevolent activity of driver's license data (see Observation G).

5. **Are all users with access to the information exchanged instructed about the confidential nature of the data and told about the civil and criminal sanctions for unauthorized use of the data?**
Generally no. The MOU's Section V, *Safeguarding Information,* bullet F states all personnel with access to the information exchanged be instructed of and acknowledge their understanding of the confidential nature of the information. Bullet G of this section states all personnel with access to the information will be instructed about and acknowledge their understanding of the civil and criminal sanctions specified in state and federal law for unauthorized use of the data.

We polled 12 employees involved in the data exchange process and asked them if they had been instructed on the confidential nature and the civil and criminal sanctions for the unauthorized use of driver's license information. Of the five respondents, two said that they were instructed about the confidential nature and one was instructed about the criminal sanctions. There were no records showing that the employees were instructed on these requirements.

Upon our notification, the Gainesville Regional Utilities IT Department built an online training presentation which instructs users on the confidentiality and civil and criminal sanctions regarding unauthorized use of driver's license information. Information including the employee's name, ID number, email address, and the date are recorded as proof of training.

6. **Is access to the information exchanged monitored on an ongoing basis?**
No. The MOU's Section V, *Safeguarding Information,* bullet H states that all access to the information must be monitored on an ongoing basis. In addition, an Annual Certification Statement must be completed to ensure proper and authorized use and dissemination of information; however, user activities are not recorded when using the data extract application to access the data exchange information.

While the application did not monitor user activities, Gainesville Regional Utilities employed a Senior IT Infrastructure Designer and Administrator to manually monitor the network for potential malevolent activity. However, the in-scope information systems were not included in this monitoring. According to staff, an automated intrusion detection system is planned for 2020. The lack of log file reviews and monitoring of the in-scope system's activities reduces management's ability to identify unauthorized use as required in the Annual Certification Statement (see Observation H).

7. <u>Is the information exchanged data received and transmitted using TLS version 1.2?</u>

Generally yes. The MOU's Section V, *Safeguarding Information,* bullet I states all data received from the FLHSMV shall be encrypted during transmission to Third Party End Users[2] using Transport Layer Security (TLS) version 1.2 or higher encryption protocols. The FLHSMV data exchange site connection was secured using TLS v1.2. However, based on the data extract's address, information transmitted to the application is not encrypted (see Observation I).

[2] Any individual, association, organization, or corporate entity who receives driver license and/or motor vehicle data from the City of Gainesville in accordance with DPPA and Section 119.0712(2), Florida Statutes.

AUDIT OBSERVATIONS

Internal control helps entities achieve important objectives and sustain and improve performance. The Committee of Sponsoring Organizations of the Treadway Commission (COSO)*, Internal Control – Integrated Framework (2013 Framework),* enables organizations to effectively and efficiently develop systems of internal control that adapt to changing business and operating environments, mitigate risks to acceptable levels, and support sound decision making and governance of the organization. The audit observations listed are offered to help management fulfill their internal control responsibilities.

Observation A: The Security Incident Handling Policy needs strengthening to ensure compliance with the MOU.

Condition:

The Security Incident Handling Policy did not include driver's license data related incidents or when to report potential incidents.

Cause:

There is no incident reporting form specifically related to the data exchange information process.

Criteria:

Florida Highway Safety and Motor Vehicles External Information Security Policy *#B-10: Incident Handling (Security Incidents).*

Effect:

Employees may be unaware or unable to report a data exchange information related security incident.

Risk:

- Not in compliance with MOU-0124-19.
- Security incidents may go unreported.

Recommendation:

The Security Incident Handling Policy should include language that describes reportable FLHSMV security events. Whenever a security incident is confirmed or has the potential to impact the data exchange information, the FLHSMV must be notified in writing within five business days of the discovery.

Observation B: Not all server update patches were installed.

Condition:

A total of 39 in-scope servers' operating system patches were available for implementation. After the IT Quarterly Maintenance performed on December 8, 2019, ten patches were still not applied. Upon our inquiry, an additional four patches were applied to the development database server, which reduced the number of open patches to six.

Cause:

According to the GRU IT Infrastructure Designer and Administrator Lead, a patch failed during installation that contributed to the unapplied patches.

Criteria:

The National Institute of Standards and Technology Special Publications 800-53 Rev. 5 Draft System Integrity (SI) No. 2 *Flaw Remediation* control (C) guidelines require GRU IT to install security-relevant software and firmware updates within the quarterly maintenance period from the release of the updates.

Effect:

Information systems that have not applied critical patches are more susceptible to becoming compromised through known vulnerabilities.

Risk:

Unauthorized access, use or dissemination of driver's license related information.

Recommendation:

Work with the Gainesville Regional Utilities IT Department to implement the remaining operating system patches or document that they are not critical to the data security of the in-scope servers.

Observation C: IT assets are not classified in accordance with the FLHSMV External Information Systems Security Policy's #A-02: Data Security Section 7.0 Data Classification requirements.

Condition:

Information systems are not risk rated or categorized by the data contained within the system.

Cause:

The IT asset inventory list does not contain a column to specify each system's risk rating or to classify the data contained within each system.

Criteria:

The Florida Highway Safety and Motor Vehicles External Information Security Policy #A-02: Data Security 7.0 Data Classification requires that data be classified in one of three categories: Public, Sensitive or Confidential.

Effect:

The Gainesville Regional Utilities IT Department may not allocate the proper resources to ensure the security and integrity of driver's license data.

Risk:

Potential loss or damage from the corruption, loss, or disclosure of sensitive driver's license data.

Recommendation:

Work with the Gainesville Regional Utilities IT Department to properly classify the in-scope systems in accordance with Federal Information Processing Standards (FIPS) Publication 199 and the FLHSMV External Information Systems Security Policy's *7.0 Data Classification* categories.

Observation D: Identified vulnerabilities need to be examined and controls implemented.

Condition:

The vulnerability scans identified 10 critical and 53 high-risk vulnerabilities.

Cause:

Vulnerability scans were not performed previously.

Criteria:

Florida Cybersecurity Standards Rule 60GG-2.002 Identify (ID) *Risk Assessment* (RA) No. 1 *Identify and document asset vulnerabilities*.

Effect:

Critical and high-risk vulnerabilities reduce the effectiveness of data security controls implemented on the in-scope systems.

Risk:

- Unauthorized access.
- Compromised information systems on the internal network.

Recommendation:

Work with the Gainesville Regional Utilities IT Department to examine the 63 vulnerabilities and implement adequate controls to reduce the data risk to an acceptable risk tolerance level.

Observation E: Business Continuity Plan does not include the in-scope systems.

Condition:

The Business Continuity Plan documentation provided by the GRU IT department does not include the in-scope systems. In addition, the plan should be tested at least annually and document the plan's procedures that were successful and specify any modifications required to improve the plan.

Cause:

The Gainesville Regional Utilities IT Disaster Recovery Plan is being updated and completion is expected in 2020.

Criteria:

- Florida Cybersecurity Standards Rule 60GG-2.003 Protect (PR) *Information Protection Processes and Procedures* (IP) No. 9 Establish and manage business continuity and disaster recovery plans.
- Florida Cybersecurity Standards Rule 60GG-2.003 Protect (PR) *Information Protection Processes and Procedures* (IP) No. 10 Test response and recovery plans.

Effect:

The Gainesville Regional Utilities IT Department may be unable to adequately respond to disruptions or continue FLHSMV data exchange operations in a timely manner.

Risk:

Increased time and resources needed to comply with insurance and FTA/DOT regulations to ensure that the City's drivers do not have suspended or revoked licenses.

Recommendation:

The in-scope systems should be included in the business continuity plan and be tested at least once a year. Management should document what was successful and any changes needed as part of the lessons learned.

Observation F: Generically named user accounts.

Condition:

There are three generically named user accounts in the data extract application database and one with administrator privileges to the driver's license reports folder.

Cause:

Generically named user accounts may be used to communicate between applications, operate as a service account, or troubleshoot programming errors.

Criteria:

- The FLHSMV External Information Security Policy #B-02: Access Control *2.0 Policy* states each user accessing a FLHSMV information resource shall be assigned a unique personal identifier.
- The FLHSMV External Information Security Policy #A-02: Data Security *3.0 Data Usage* states that only uniquely identified, authenticated, and authorized users are allowed access to the FLHSMV data.

Effect:

- Users may access more data than they may have been originally granted.
- Inability to track individual user activities.

Risk:

Unauthorized use or dissemination of driver's license information.

Recommendation:

Work with the Gainesville Regional Utilities IT Department to review and disable generically named user accounts, where applicable.

Observation G: User access to driver's license information obtained without appropriate approval.

Condition:

The Worker's Compensation and Loss Control Manager was unaware that 17 users have access to a folder containing driver's license information.

Cause:

Access approval process did not include the Worker's Compensation and Loss Control Manager.

Criteria:

The Florida Highway Safety and Motor Vehicles External Information Security Policy's #B-03: *Account Management for User Accounts* No. 1 states all accounts created must have an associated request and approval that is appropriate for the Department of Highway Safety and Motor Vehicles information resource or service.

Effect:

- Unauthorized access to driver's license information through the use of the data extract's PDF feature.
- User access may not adhere to the least privilege principle that is necessary to perform their job duties.
- User access may not adhere to the segregation of duties principle to prevent malevolent activity without collusion.
- Users may obtain access without attending the appropriate FLHSMV-related training.

Risk:

Unauthorized use or dissemination of driver's license information.

Recommendation:

Work with the Risk Management's Worker's Compensation and Loss Control Manager to review and formally approve user access to the in-scope systems.

Observation H: User activities are not recorded or reviewed.

Condition:

When users access the data exchange information their activities are not recorded or reviewed.

Cause:

Log capabilities have not been built into the data exchange process.

Criteria:

The MOU's *Safeguarding Information* section requires that all access to the data must be monitored on an ongoing basis.

Effect:

- Data exchange information may be accessed or disseminated in an unauthorized manner.
- Misuse of data may go undetected.
- Transferred or terminated employees may still have an active user account.

Risks:

Not in compliance with MOU-0124-19.

Recommendation:

Build monitoring capabilities into the data exchange process and evaluate user activities on a quarterly basis to identify any unauthorized access, distribution, use, modification, or disclosure of data exchanged information. Unauthorized user actions may include:

- Accessing information after transfer or termination.
- Accessing data during non-business hours, weekends, and in between biannual license checks.
- Non-business related purposes

Observation I: Information transmitted to and from the data extract application is not secure.

Condition:

Information sent to the data extract application is not encrypted.

Cause:

The URL is not set to a secure HTTPS connection.

Criteria:

The Florida Highway Safety and Motor Vehicles External Information Security Policy's #A-02: Data Security *4.0 Data Storage and Transmission* states that transmitted data must be secured via a FLHSMV-approved encryption technology.

Effect:

Employee driver's license data may be accessed or disseminated in an unauthorized manner.

Risks:

Not in compliance with MOU-0124-19.

Recommendation:

Ensure that information transmitted to and from the data extract application is encrypted using TLS v1.2 or higher protocols. The City Manager must obtain written approval from the FLHSMV if using an alternate protocol.

GOVERNMENT AUDITING STANDARDS COMPLIANCE

We conducted this performance audit in accordance with generally accepted government auditing standards and ISACA[3] IS Audit and Assurance 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 observations and conclusions based on our audit objectives.

AUDIT TEAM

Leonard F. Loria, CPA, Interim City Auditor
Vincent Iovino, CISA, CRISC, Information Technology Auditor
Eileen Marzak, CPA, CFE, Quality Assurance Auditor

[3] Previously known as the Information Systems Audit and Control Association, ISACA is an independent, nonprofit, global association that engages in the development, adoption, and use of globally accepted industry-leading knowledge and practices for information systems.

City of Gainesville

Office of the City Auditor

January 30, 2020

Chief, Bureau of Records
2900 Apalachee Parkway
Tallahassee, Florida 32399

To Whom It May Concern:

Pursuant to the requirements of the Florida Department of Highway Safety and Motor Vehicles Contract number HSMV-0124-19, we certify that:

1. **The data security policies and procedures reviewed adequately protect the personal data from unauthorized access, distribution, use, modification, or disclosure.**
2. **The data security policies and procedures were reviewed and approved by a Risk Management IT Security Professional.**
3. **Seven of the nine identified deficiencies have been corrected and measures enacted to prevent recurrence. The Gainesville Regional Utilities IT Department is in the process of implementing a solution to address the operating system patches and the one remaining critical vulnerability within the next four months.**

Sincerely,

Leonard F. Loria, CPA
Interim City Auditor

Lee R. Feldman
City Manager

GRU
More than Energy

INTEROFFICE COMMUNICATION

General Manager

APPENDIX A – GAINESVILLE REGIONAL UTILITIES RESPONSE AND CORRECTIVE ACTION PLAN

DATE: January 30, 2019

TO: Len Loria, Interim City Auditor

FROM: Edward J. Bielarski, Jr., General Manager for Utilities

SUBJECT: Management Response to Audit of Internal Controls and Data Security for the use of Driver's License and Motor Vehicle Record Data Exchange

---

GRU IT staff has reviewed the recommendations of your office and find that they are reasonable and applicable.

The attached response was compiled by IT staff and submitted to me by Chief Information Officer Walter Banks. Mr. Banks and his staff is available to answer questions or provide additional information as needed.

APPENDIX A – MANAGEMENT RESPONSE AND CORRECTIVE ACTION PLAN

We believe that management is in a unique position to best understand their operations and may be able to identify more innovative and effective approaches, and we encourage them to do so when providing responses to our recommendations.

Recommendation	Concurrence and Corrective Action Plan	Proposed Completion Date
Recommendations for City Management:		
A. The Security Incident Handling Policy should include language that describes reportable FLHSMV security events. Whenever a security incident is confirmed or has the potential to impact the data exchange information, the FLHSMV must be notified in writing within five business days of the discovery.	GRU IT staff updated policies and procedures for the in-scope systems to include: *Incidents related to systems, or components, involving the data exchange with FLHSMV's Driver and Vehicle Information Database (DAVID) should notify FLHSMV immediately. In addition, the FLHSMV should be notified, in writing, within five (5) business days of a security incident discovery. Reportable events include:* • *Physical loss, theft, or destruction of the FLHSMV data* • *Unauthorized disclosure, access, including sharing user credentials, unauthorized activity or transmission of data using FLHSMV information resources.* • *Data that has been altered or destroyed or access that is denied outside of normal business hours.* • *Lost identification badges.* • *Violation of any portion of the External Information Security Policy.*	Completed
B. Work with the Gainesville Regional Utilities IT Department to implement the remaining operating system patches or document that they are not critical to the data security of the in-scope servers.	GRU IT performs a Quarterly Preventative Maintenance (QPM) event 3–4 times annually. QPM the multi-phased process to apply patches to our development, quality assurance (QA), and production systems. Development and QA patches are performed in the first phase and then validated through internal testing. The production phase occurs 2 weeks afterwards. Initial in-scope development system and component patches were accelerated and applied out-of-band with normal QPM phases after the initial vulnerability assessment was performed. Additional production patches will be applied during the next QPM event scheduled for February 29-March 1.	March1, 2020 (QPM) for Applicable Patches. June 6-7 for the "Migrate" Project.

APPENDIX A – MANAGEMENT RESPONSE AND CORRECTIVE ACTION PLAN

Recommendation	Concurrence and Corrective Action Plan	Proposed Completion Date
	One critical patch was identified and cannot be applied to the current production host to due incompatibilities. To overcome this incompatibility, a new host will be provisioned and the system migrated as detailed in the corrective actions related to Recommendation D (below).	
C. Work with the Gainesville Regional Utilities IT Department to properly classify the in-scope systems in accordance with Federal Information Processing Standards (FIPS) Publication 199 and the FLHSMV External Information Security Policy's 7.0 Data Classification categories.	GRU IT staff updated policies and procedures for the in-scope systems to include: *This application processes and handles information considered to be CONFIDENTIAL.* *When configuring and/or using this application or any of its components please work to ensure its data is treated carefully (Not leaked, etc.).*	Completed
D. Work with the Gainesville Regional Utilities IT Department to examine the 63 vulnerabilities and implement adequate controls to reduce the data risk to an acceptable risk tolerance level.	A vulnerability scan for the in-scope components was performed on 12/9/2019. This established a "baseline" for comparison. An overview of findings are provided in document, "D.2-2-VulnerabilityScan.12-09-2019.Development.and.Production.Baseline.html". To determine potential improvement on these systems, GRU IT applied patches to the in-scope development components ahead of the next scheduled QPM. An overview of findings with this out-of-band upgrade is included in the document, "D.2-2-VulnerabilityScan.01-12-2020.Development.Patched.HTML". Overall improvements are immediately visible by comparing the development systems in the "Patched" document to the "Baseline". The development environment patches, and subsequent improvement, are now scheduled for execution for the in-scope production components during the next QPM event scheduled February 29–March 1, 2020.	March1, 2020 (QPM) for Applicable Patches. June 6-7 for the "Migrate" Project.

APPENDIX A – MANAGEMENT RESPONSE AND CORRECTIVE ACTION PLAN

Recommendation	Concurrence and Corrective Action Plan	Proposed Completion Date
	Some of the alerts, including one critical alert, cannot be addressed via patching. To address these alerts, we've created a project to migrate the application and its database to newer servers and operating systems. We are tentatively aiming to have this complete by 6/7/2020.	
E. The in-scope systems should be included in the business continuity plan and be tested at least once a year. Management should document what was successful and any changes needed as part of the lessons learned.	In-scope systems added to "City of Gainesville-Disaster Recovery Plan" under the new section, 14 APPENDIX A – EXAMPLE DR PROCEDURE: GG DRIVER LICENSE REPORT (CONFIDENTIAL DATA). Disaster Plan testing and results with lessons learned covered in the document, "DR Plan for Inscope Systems and Lesson's Learned.docx".	Completed
F. Work with the Gainesville Regional Utilities IT Department to review and disable generically named user accounts, where applicable.	The following groups were successfully removed. • app_FLHSMVWebUser (database) • FLHSMVDriversLicenseAccessUser (database) • DG_DL_Validation_HomeDept_680_HomeUnit_All (AD security group) • DG_DL_Validation_HomeDept_010_HomeUnit_All (AD security group) • DG_DL_Validation_HomeDept_All_HomeUnit_All (AD security group) Additional generic accounts were removed by eliminating storage of PDF documents on corporate file shares.	Completed
G. Work with the Risk Management's Worker's Compensation and Loss Control Manager to review and formally approve user access to the in-scope systems.	Non-IT staff access is reduced to two staff members in Risk Management. Acceptance and formal approval from Risk Management POC, David Jarvis, received Friday, January 24, 2020, at 11:52 AM. IT staff access for support function is limited to two controlled groups: domain administrators and application management. The Worker Compensation and Loss Control Manager has reviewed and approved the list of users.	Completed

APPENDIX A – MANAGEMENT RESPONSE AND CORRECTIVE ACTION PLAN

Recommendation	Concurrence and Corrective Action Plan	Proposed Completion Date
H. Build monitoring capabilities into the data exchange process and evaluate user activities on a quarterly basis to identify any unauthorized access, distribution, use, modification, or disclosure of data exchanged information. Unauthorized user actions may include: • Accessing information after transfer or termination. • Accessing data during non-business hours, weekends and in between biannual license checks. • Non-business related purposes	Additional monitoring capabilities were built and incorporated into the in-scope systems to audit the following scenarios: • Access to data after termination. • Access to data after transfer. • At abnormal (outlier) dates and times, including non-business hours, weekends, and in between June and December data requests. • Not part of their job duties • Non-business related purposes The initial execution of enhanced monitoring was conducted on January 22-24, 2020 and results shared with City Auditor staff. The next quarterly review is scheduled for April 30, 2020.	Completed
I. Ensure that information transmitted to and from the data extract application is encrypted using TLS v1.2 or higher protocols. The City Manager must obtain written approval from the FLHSMV if using an alternate protocol.	Application secured under HTTPS protocol and backed by valid certificate using TLS 1.2, ECDHE_RSA with P-256, and AES_256_CBC with HMAC-SHA1.	Completed