



**Office of
Internal Audit**

FLORIDA INTERNATIONAL UNIVERSITY

**Examination of the Department of
Parking, Sustainability & Transportation's
Compliance With Contract Number
HSMV-0185-22**

**Report No. 22/23-03
October 28, 2022**



Office of Internal Audit

FLORIDA INTERNATIONAL UNIVERSITY

Date: October 28, 2022

To: Thomas Hartley, Assistant Vice President, Department of Parking, Sustainability & Transportation

From: Trevor Williams, Chief Audit Executive

A handwritten signature in blue ink, reading "Trevor Williams", is placed over the name in the "From:" field.

Subject: Examination of the Department of Parking, Sustainability & Transportation's Compliance With Contract Number HSMV-0185-22, Report No. 22/23-03

Pursuant to your request, we have examined the Department of Parking, Sustainability & Transportation's ("Parking") internal controls and data security governing the use of personal data as required by the Florida Department of Highway Safety and Motor Vehicles (DHSMV or "the Department") Memorandum of Understanding (MOU) 0185-22, Contract Number HSMV-0185-22. The objectives of the examination were to determine whether Parking's policies and procedures for protecting personal data are: (1) adequate and effective, (2) being adhered to, and (3) ensure that the confidentiality of the data is maintained and protected. This includes an evaluation of the controls in place to prevent unauthorized access, distribution, use, modification, or disclosure of personal data.

The examination also certified that: (1) the data security policies and procedures have been approved by a Risk Management Information Technology (IT) Security Professional, (2) all deficiencies and/or issues found during the examination have been corrected, and (3) corrective measures have been enacted by Parking to prevent recurrence. Therefore, we are satisfied that the current internal controls adequately protect personal data from unauthorized access, distribution, use, modification, or disclosure.

Attachment

C: FIU Board of Trustees

Kenneth A. Jessell, University President-Designate

Elizabeth M. Bejar, Interim Provost, Executive Vice President, and Chief Operating Officer

Aime Martinez, Interim Chief Financial Officer and Vice President for Finance and Administration

Javier I. Marques, Vice President for Operations & Safety and Chief of Staff, Office of the President

TABLE OF CONTENTS

	<u>Page</u>
INDEPENDENT ACCOUNTANT’S REPORT	1
SCOPE, OBJECTIVES, AND METHODOLOGY	3
MANAGEMENT AND INDEPENDENT ACCOUNTANT’S RESPONSIBILITIES	5
OVERALL ASSESSMENT AND INTERNAL CONTROLS RATING	6
SUMMARY OF DEFICIENCIES OBSERVED AND CORRECTIVE ACTIONS TAKEN	7
MANAGEMENT’S CERTIFICATION	10
BACKGROUND	13
APPENDIX I – OIA CONTACTS AND STAFF ACKNOWLEDGMENT	15

INDEPENDENT ACCOUNTANT'S REPORT

We have examined the assertions made by the management of Parking that internal controls are in place to protect data received from the Department and these controls are adequate to protect data from unauthorized access, distribution, use, modification, or disclosure, and that policies and procedures in place during the attestation engagement period were approved by a Risk Management IT Security Professional and met the requirement as listed in the MOU. The management of Parking further asserts that all deficiencies and/or issues found during the examination have been corrected and corrective measures have been enacted by Parking to prevent recurrence. Parking's management is responsible for its assertions. Our responsibility is to express an opinion whether Parking had internal controls in place to protect data received from the Department and whether these controls were adequate to protect data from unauthorized access, distribution, use, modification, or disclosure, and whether policies and procedures in place during the attestation engagement period were approved by a Risk Management IT Security Professional and met the requirement as listed in the MOU, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform the examination to obtain reasonable assurance about whether the above assertions of Parking's management are presented based on the criteria contained in the MOU, in all material respects. An examination involves performing procedures to obtain evidence about the above assertions of Parking's management. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of the stated management assertions, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

The criteria for this examination as delineated in the MOU are related to IT (Information Technology) security standards established by the Florida Information Technology Security Act, Section 282.318, Florida Statutes (F.S.), Florida Cybersecurity Standards, Florida Administrative Code (F.A.C.) 60GG-2, and the Department's policy. We have provided a detailed description of these standards in the section of this report titled Scope, Objectives, and Methodology (page 3). Additionally, in the section of the report titled Management and Independent Accountant's Responsibilities (page 5), we have provided detailed descriptions of Parking management's responsibility for the subject matter examined and our responsibility under the engagement.

Our examination disclosed deviations in Parking's internal controls subject to this examination, that if not corrected, could diminish the controls' effectiveness in

protecting data from unauthorized access, distribution, use, modification, or disclosure. The deviations were related to the absence of user's documented acknowledgment of their understanding of the confidential nature of the data accessed and the civil and criminal sanctions for disclosing this information, users not completing Cybersecurity Awareness Training, the existence of non-conforming password parameters, and vulnerabilities to certain workstations. We have provided details of the observed deviations along with the corrective actions taken by Parking's management and their date of implementation in the section of this report titled, Summary of Deficiencies Observed and Corrective Actions Taken (page 7). Further, we have applied appropriate examination procedures to verify the implementation and effectiveness of the corrective actions taken by Parking to prevent recurrence.

In our opinion, except for the deviations from the criteria described in the preceding paragraph, the attestation made by the management of Parking that internal controls are in place to protect data received from the Department and are adequate to protect data from unauthorized access, distribution, use, modification, or disclosure, and policies and procedures in place during the attestation engagement period are approved by a Risk Management IT Security Professional and meet the requirement listed in the MOU, is presented in accordance with the criteria listed in the MOU, in all material respects.



Trevor L. Williams, CPA
Office of Internal Audit,
Florida International University
Miami, Florida
October 28, 2022

SCOPE, OBJECTIVES, AND METHODOLOGY

Scope and Objectives

Our examination assessed Parking's internal controls and data security practices governing the use and dissemination of personal data pursuant to the requirements of the Florida Department of Highway Safety and Motor Vehicles (DHSMV) Contract Number HSMV-0185-22 for Record Data Exchange. Pursuant to the MOU, Parking must have developed security requirements and standards consistent with the Florida Information Technology Security Act, Section 282.318, F.S., Florida Cybersecurity Standards, F.A.C. 60GG-2, and the Department's policy. In addition, Parking's data security policies and procedures must be approved by a Risk Management IT Security Professional.

The objectives of the examination were to determine whether Parking has policies and procedures in place to prevent unauthorized access, distribution, use, modification, or disclosure of the personal data that is provided/received pursuant to the Department's MOU and whether those data security policies and procedures have been approved by a Risk Management IT Security Professional.

An overview of the scope of section 282.318, F.S., F.A.C. 60GG-2, and the DHSMV policy are as follows:

Section 282.318, F.S., *Security of data and information technology*, also known as the "Information Technology Security Act," states that the Agency for State Technology is responsible for establishing standards and processes consistent with generally accepted best practices for information technology, including cybersecurity, to ensure availability, confidentiality, and integrity of an agency's data to mitigate risks. The information security framework guidelines established by the act are consistent with the Cybersecurity standards outlined in F.A.C. 60GG-2.

F.A.C. 60GG-2, also known as the Florida Cybersecurity Standards (FCS), establishes standards that State Agencies must comply with in the management and operation of their IT resources. These are minimum standards to be used by state agencies to secure IT resources. The standards consist of five high-level functions: Identify, Protect, Detect, Respond, and Recover. These functions support lifecycle management of IT risks, and their related activities should be evident for securing critical data residing on the FIU NuPark system. (See Background on page 13.)

The DHSMV policy applies to all agents, vendors, contractors, and consultants (External Entities) that use and/or have access to the Department's information resources. External Entities that use and/or have access to the information resources shall adhere to said policy. The authority for the DHSMV policy derives from section 282.318, F.S., and F.A.C. 60GG-2.

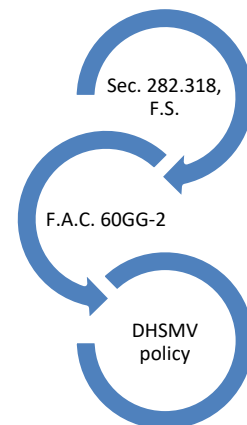


Figure 1: HSMV-0185-22 Requirements

Methodology

The examination methodology was based on the requirements of the MOU, the Department's External Information Security Policy, and F.A.C. 60GG-2. To align with the requirements of the MOU, our examination included an evaluation of internal controls in place during the MOU service year ended September 28, 2022. The examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and in conformance with the *International Standards for the Professional Practice of Internal Auditing* and ISACA *IS Audit and Assurance Standards*. Those standards require that we plan and perform our examination to obtain reasonable assurance to satisfy our engagement objectives. Our examination also included tests of the five high-level functions identified in F.A.C. 60GG-2 and such other examination procedures, as we considered necessary under the circumstances. We performed our examination fieldwork between August and October 2022.

To satisfy our objectives, we:

- Reviewed University policies and procedures, FIU Board of Trustees (BOT) and Florida Board of Governors (BOG) regulations, applicable Florida Statutes and Florida Administrative Code 60GG-2, MOU HSMV-0185-22, and the Department's External Information Security Policy;
- Observed Parking's current processes and practices;
- Interviewed responsible personnel;
- Tested selected systems, processes, and activities;
- Examined the internal controls over the data exchange environment between the FIU NuPark system and the Department (see Figure 2 on page 14); and
- Reviewed the controls over the Microsoft Azure Hosting platform services identified in the recent Service Organization Controls report (SOC 2) performed for that platform. The report covered the AICPA Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy throughout the period April 1, 2021, to March 31, 2022.

Sample size and items selected for testing were determined on a judgmental basis applying a non-statistical sampling methodology.

In performing the examination, we utilized staff members from the University's Division of Information Technology ("DoIT") as subject matter experts for completing certain aspects of the engagement, including collaborating with our Office to ensure adequate controls were in place for the workstations used to access NuPark and completing an analysis of the controls in place within the NuPark organization, based on NuPark's responses to the Higher Education Community Vendor Assessment Toolkit (HECVAT) questionnaire used to assess vendor risk. In addition, a DoIT Risk Management IT Security Specialist, with over 10 years of experience as a Senior IT Security Engineer, and Microsoft System Engineer Global Information Assurance Certification (GIAC) Security Essentials certified, has approved Parking's data security policies and procedures in place during this attestation engagement.

MANAGEMENT AND INDEPENDENT ACCOUNTANT'S RESPONSIBILITIES

Management's Responsibility

Parking is responsible for: (1) designing, implementing, and maintaining a system of internal controls, including data security policies and procedures for its personnel to follow to protect personal data; (2) ensuring that the data security policies and procedures are reviewed and approved by a Risk Management IT Security Professional; and (3) ensuring that deficiencies found during the examination are corrected and measures have been enacted to prevent recurrence. Pursuant to the MOU, the appropriate management personnel must sign the examination report along with the independent auditor. The required management certification is included in the Management's Certification section of this report.

Independent Accountant's Responsibility

Our responsibility is to: (1) evaluate the internal controls, including policies and procedures, governing the use and dissemination of personal data pursuant to the MOU and applicable laws, and to express an opinion on the adequacy of those controls to protect personal data from unauthorized access, distribution, use, modification, or disclosure; (2) verify that a Risk Management IT Security Professional has approved Parking's data security policies and procedures; and (3) verify that deficiencies found during the examination have been corrected and measures enacted to prevent recurrence.

OVERALL ASSESSMENT AND INTERNAL CONTROLS RATING

Our examination identified deviations in Parking's in-scope internal controls related to the absence of user's documented acknowledgment of their understanding of the confidential nature of the data accessed and the civil and criminal sanctions for disclosing this information; users not completing Cybersecurity Awareness Training; non-conforming password parameters; and workstation vulnerabilities. Parking has corrected the deficiencies identified and enacted measures to prevent recurrence. We have applied appropriate examination procedures to verify the implementation and effectiveness of the corrective actions taken by Parking. Our overall evaluation of internal controls is summarized in the table below.

INTERNAL CONTROLS RATING			
CRITERIA	SATISFACTORY	FAIR	INADEQUATE
Process Controls	X		
Policy & Procedures Compliance	X		
Effect	X		
Information Risk	X		
External Risk	X		
INTERNAL CONTROLS LEGEND			
CRITERIA	SATISFACTORY	FAIR	INADEQUATE
Process Controls	Effective	Opportunities exist to improve effectiveness	Do not exist or are not reliable
Policy & Procedures Compliance	Non-compliance issues are minor	Non-compliance Issues may be systemic	Non-compliance issues are pervasive, significant, or have severe consequences
Effect	Not likely to impact operations or program outcomes	Impact on outcomes contained	Negative impact on outcomes
Information Risk	Information systems are reliable	Data systems are mostly accurate but can be improved	Systems produce incomplete or inaccurate data which may cause inappropriate financial and operational decisions
External Risk	None or low	Potential for damage	Severe risk of damage

SUMMARY OF DEFICIENCIES OBSERVED AND CORRECTIVE ACTIONS TAKEN

The following section details our observations and recommendations related to the internal processes in place to protect the data as outlined in the MOU, F.A.C. 60GG-2 standards, and the DHSMV policies. The corrective actions taken by Parking along with their implementation or estimated completion date are also presented.

Deficiency Observed	Has This Deficiency Been Sufficiently Corrected?	Corrective Action Taken	Date of Corrective Action Taken	If Not Corrected, Estimated Date of Completion
Users were not: (a) being instructed of, or acknowledging their understanding of, the confidential nature of the information via the Cybersecurity Awareness Training; or (b) acknowledging their understanding of the civil and criminal sanctions for disclosing data.	Yes	All current NuPark users with direct or indirect access to DMV data within NuPark have executed an acknowledgment form attesting to the confidentiality of the nature of the information and acknowledging their understanding of the civil and criminal sanctions for disclosing such data. The acknowledgment will also be required of new users prior to receiving access to NuPark and/or DMV systems. The acknowledgment will be renewed yearly in October and has been made part of Parking's procedures.	Immediately	Not Applicable
Nine users who were terminated during the examination period had not completed their Cybersecurity Awareness Training.	Yes	FIU Cybersecurity Awareness Training will be completed as part of the employees' onboarding process.	Immediately	Not Applicable
Not all NuPark user accounts abide by the FLHSMV password policy. Although the users with direct access to the DMV module abide by the policy, the remaining authorized user accounts do not. Also, we observed that an FIU Active Directory (AD) account (nuparktest@fiu.edu) owned by the NuPark team needs to have its password policy requirements adjusted to reduce the risk of compromise.	Yes	All user accounts with access to the back-office version of NuPark have been added to an AD organizational unit (OU) configured to inherit the FLHSMV password policy. Parking procedures have been modified such that all users with indirect access to NuPark are added to the OU during onboarding. The <i>nuparktest</i> account has been deactivated within the NuPark application and the FIU AD domain.	Immediately	Not Applicable
We found 18 of 44 workstations with the following issues: four instances of unsupported versions of Windows 10 running; two requiring an approved Drive Encryption Agent to be installed; four requiring updates to the Data Loss Prevention (DLP) endpoint product currently installed; and 15 workstations with local administrative accounts.	Yes	The workstations' operating systems were patched to currently supported versions of Windows 10. The Drive Encryption Agent and DLP Endpoint products were installed and updated, and all local administrative accounts were removed.	Immediately	Not Applicable

Deficiency Observed	Has This Deficiency Been Sufficiently Corrected?	Corrective Action Taken	Date of Corrective Action Taken	If Not Corrected, Estimated Date of Completion
There were two generic accounts listed in the authorized NuPark users report. Upon review, we found that they were not needed or utilized. In addition, one user account was still active 17 days after the employee was terminated.	Yes	The accounts have been deactivated.	Immediately	Not Applicable

MANAGEMENT'S CERTIFICATION



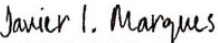
RE: Contract No.: HSMV-0185-22, Memorandum of Understanding - Data Exchange


Pursuant to Section VI., Compliance and Control Measures, Part A, Internal Control and Data Security Audit, of the current Memorandum of Understanding ("MOU") between the Florida Department of Highway Safety and Motor Vehicles ("Department") and Florida International University Board of Trustees on behalf of the Parking and Transportation Department ("Department of Parking, Sustainability & Transportation" or "Parking"), which was executed on September 29, 2021, continued access to personal data is contingent upon the Parking having appropriate internal controls in place at all times to protect data received from the Department from unauthorized access, distribution, use, modification or disclosure.

Thomas Hartley, Assistant Vice President FIU Operations and Safety of Parking has submitted an attestation to be reviewed by the Florida International University Office of Internal Audit ("Office of Internal Audit"). The Office of Internal Audit has examined the Parking attestation for the period of time between July 1, 2021, and September 28, 2022, to determine that Parking has adequate policies, procedures, and controls in place to protect data received from the Department from unauthorized access, distribution, use, modification, or disclosure in accordance with the MOU. The Office of Internal Audit's responsibility is to provide an opinion based on verifying and validating the internal controls based upon attestation standards.

Pursuant to Section VI., Part A of the MOU, the attestation was performed by a currently licensed Certified Public Accountant ("CPA") to evaluate that internal controls are in place to protect data received from the Department and these controls are adequate to protect data from unauthorized access, distribution, use, modification, or disclosure. The examination was conducted in accordance with the attestation standards established by the American Institute of Certified Public Accountants ("AICPA"). These standards require that the Office of Internal Audit plan and perform the examination to obtain reasonable assurance that the attestation made by Parking was fairly stated, in all material aspects. The examination involved performing tests of compliance to obtain evidence about the attestation. The nature, timing, and extent of procedures selected depend on the Office of Internal Audit's judgment, including an assessment of the risks of material misstatement of Parking's attestation, whether due to fraud or error. The Office of Internal Audit believes that the evidence obtained was sufficient to provide a reasonable basis for their opinion.

The internal controls were evaluated, in conjunction with the requirements of the MOU and applicable laws. Additionally, this included a review to ensure that policies and procedures are in place for personnel to follow and data security procedures and policies are in place to protect personal data.

DocuSigned by:

396705DFE0284E4
Javier I. Marqués
Vice President for Operations & Safety
Chief of Staff

DocuSigned by:

BCC27A7A57B040C
Thomas Hartley
Assistant Vice President
Parking, Sustainability & Transportation

BACKGROUND

On September 29, 2021, Florida International University Board of Trustees; on behalf of Parking, entered into the Memorandum of Understanding 0185-22 with the Florida Department of Highway Safety and Motor Vehicles. The MOU is a three-year agreement that allows Parking electronic access to driver license and motor vehicle data to be used to verify vehicle registration and ownership information for the purpose of issuing University parking permits and collecting fines related to citations. The agreement expires September 28, 2024, and its continuance is contingent upon Parking and its third-party hosting environment (NuPark) having appropriate internal controls in place at all times to protect the data that is being provided or received pursuant to the MOU, from unauthorized access, distribution, use, modification, or disclosure.

The University has used NuPark LLC's Parking Software Management platform ("the system") since 2014. In 2018, Passport Labs, Inc., acquired NuPark LLC. Through an Invitation to Negotiate executed on June 24, 2022, the University awarded a three-year agreement with two, one-year renewals to Passport Labs, Inc. In July 2022, Passport Labs, Inc., assigned its right to its agreement with FIU to T2 Systems, Inc., who continues to offer the NuPark product pursuant to the terms of FIU's existing agreement.

The system is a database-encrypted, fully hosted, cloud-based parking management system and has the following features:

- Secured real time license plate recognition (LPR) technology that provides Parking a focused enforcement solution that enables the use of virtual or traditional permits using vehicle based mobile LPR cameras. The LPR provides Parking an effective way to verify parking permits, confirm mobile or meter-payments, issue citations, identify scofflaws, and provide vehicle location information all in real-time. The LPR technology allows for management of the enforcement process from permit verification to citation reconciliation.
- User friendly, secure, e-commerce online permit purchasing portal, and a mobile iOS or Android application, giving customers the ability to purchase permits and manage their account from phones and/or computers. The system facilitates acceptance of multiple payment methods, such as credit, debit, and payroll deductions.
- A back office to facilitate the system management and customer status. Customer profiles may be reflected in the system as a VIP or individual with specific lot/garage/space privileges. This information is communicated in real-time to all aspects of the system allowing the field officers to have the most up-to-date status information and giving them the ability to take appropriate action in the field.
- Citations are issued electronically via email for vehicles identified in the system or printed and mailed for unidentified vehicles. A one-way interface with the DHSMV was created to acquire vehicle owner information for unidentified vehicles. The DHSMV data flow diagram is shown on the following page.

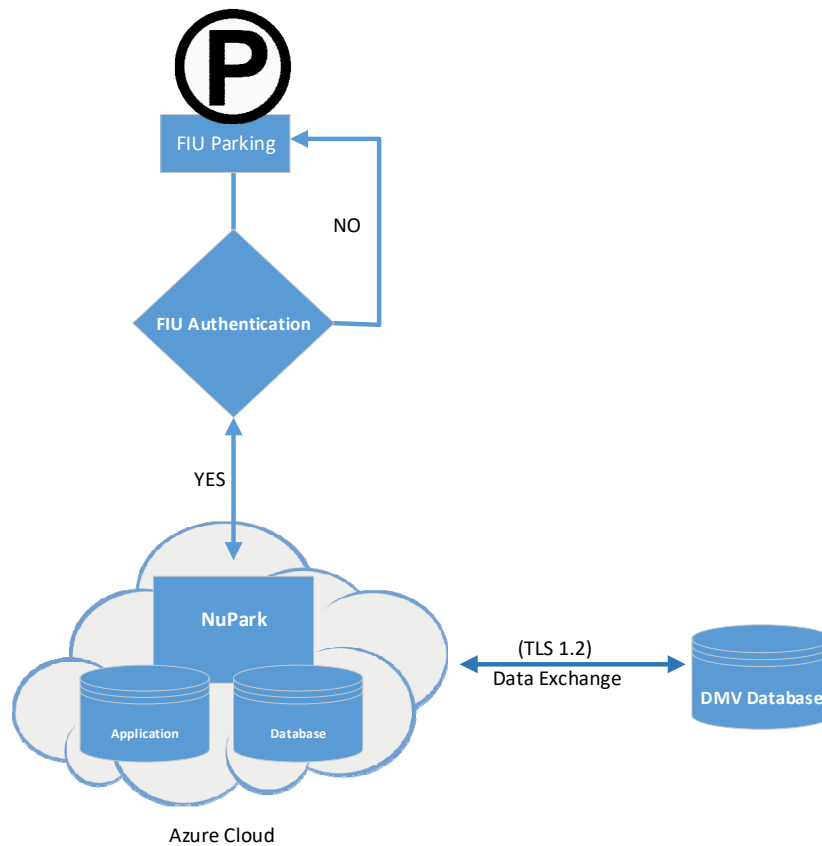


Figure 2: Data Process Flow Overview

Parking’s users authenticate through the FIU Active Directory prior to accessing the NuPark System. Once connected, users are able to access citation information and also request data from the DMV database through a Transport Layered Security Version 1.2 encrypted data exchange connection.

The NuPark system is fully hosted on the Microsoft Azure platform. Microsoft is responsible for maintaining storage, security, operating system upgrades, routine maintenance, and the backup/recovery of the NuPark online system.

APPENDIX I – OIA CONTACTS AND STAFF ACKNOWLEDGMENT:

OIA contact:

Joan Lieuw 305-348-2107 or jlieuw@fiu.edu

Contributors to the report:

In addition to the contact named above, the following staff contributed to this audit in the designated roles:

Henley Louis-Pierre (auditor in-charge);
Manuel Sanchez (supervisor and reviewer);
David Assee (Specialist, Subject Matter Expert, DoIT);
Helvetiella Longoria (Specialist, Subject Matter Expert, DoIT); and
Stephanie Price (independent reviewer).