CINDY STUART

Clerk of Court & Comptroller
13th Judicial Circuit

An Audit of:

DHSMV INTERNAL CONTROL & DATA SECURITY

COUNTY AUDIT DEPARTMENT

REPORT # 399

September 21, 2021

Integrity, Transparency and Accountability

CINDY STUART

Clerk of Court & Comptroller
13th Judicial Circuit

September 21, 2021

Dear Cindy Stuart, Clerk of Court and Comptroller:

The Audit Team has completed an audit of the security controls required by the Florida Department of Highway Safety & Motor Vehicles (DHSMV) for Driver's License (DL) transcript data (Audit Report # 399, dated September 21, 2021) in relation to the control measures and requirements outlined in the Data Exchange Memorandum of Understanding (MOU) number HSMV-0129-21.

The purpose of this Report is to provide management with an independent, objective analysis, and assessment of the activities pertaining to the personal information data received via transcript exchange from the DHSMV. Furthermore, this report serves to comply with section VI. Compliance and Control Measures Part A of the MOU. This is not an appraisal or rating of management.

The Audit Team exercised due professional care in the performance of this audit, however, this should not be construed to mean that unreported noncompliance or irregularities do not exist. The deterrence of fraud and/or employee abuse is ultimately the responsibility of management. Audit procedures alone, even when carried out with professional care, cannot guarantee that fraud or abuse will be detected.

We greatly appreciate all of the cooperation and professionalism displayed by the Directors and personnel of the Clerk's Information Technology (IT) department during this audit.

As always, if you have questions or concerns, please do not hesitate to contact me directly.

Sincerely,

Together, we will get to YES!

Heidi Pinner, CIA CISA CFE CRMA
Chief Audit Executive, Clerk of Court & Comptroller

CC: MaryLou Whaley, Chief of Staff
Michelle Decker, Chief Information Officer
Doug Bakke, Chief Operating Officer, Courts
Idania Alfonso, Senior IT Director

TABLE OF CONTENTS

EXECUTIVE SUMMARY

BACKGROUND INFORMATION

The Florida Department of Highway Safety & Motor Vehicles (DHSMV), also known as the Providing Agency, maintains a database containing driver's licenses and motor vehicle information. The Clerk's Office (the Clerk), also known as the Requesting Party, obtains this information through driver history transcript downloads from the DHSMV's web services system and provides those transcripts to judges over the Odyssey case management system for the judges to use in court proceedings. In order for the Clerk to be granted access to these records, a Memorandum of Understanding (MOU) is signed with the DHSMV. The conditions included in this MOU require the Clerk to comply with a series of laws and security standards to ensure that records and information received, stored, transmitted, and/or used by the Clerk are maintained in a secure environment. These applicable laws and standards include:

- The Driver's Privacy Protection Act (DPPA) 18 U.S. Code 2721.
- Florida Statute 501.171, Security Breaches.
- Florida Administrative Code Rule 60GG-2, Florida Cybersecurity Standards (FCS).
- The DHSMV External Information Security Policy.

The security standards identified in these laws and in the MOU aligned with the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity. This Framework includes controls designed to identify, protect, detect, respond, recover, and/or minimize security risks to data, computer systems, and other assets. By signing the MOU with the DHSMV, the Clerk agrees to comply with these laws and standards.

OBJECTIVE

The objective of the audit was to determine whether or not the Clerk's information security controls are in compliance with the security requirements stipulated in the DHSMV's MOU.

SCOPE

The audit was conducted in conformance with *the Generally Accepted Government Auditing Standards* and the *International Standards for the Professional Practice of Internal Auditing*. These Standards require that County Audit plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the audit comments and conclusions based on the audit objectives. County Audit believes that the evidence obtained provides this reasonable basis.

The audit scope includes the state of information security controls as of August 2021 for the Hillsborough County Clerk of Court as they pertain to the requirements set forth in the DHSMV MOU.

OVERALL EVALUATION & AUDIT OPINION

The Audit Team reviewed internal controls, standards and applicable laws governing the use and dissemination of driver's licenses and motor vehicle information included in the MOU. The audit assessment completed by the Audit Team evaluated each applicable standard and internal controls established by the Clerk's Office to ensure that driver license records and information received, transmitted, stored and/or used is securely processed and maintained.

Based on the assessment performed, the Audit Team has concluded that information security controls currently established in the Clerk's Office are in compliance with the DHSMV MOU requirements. This includes security policies and procedures that are in place for personnel to follow that are adequate to protect driver license and motor vehicle personal data from unauthorized access, distribution, use, modification or disclosure. All control improvement opportunities were corrected by management during the course of the audit to ensure current security controls comply with the MOU standards and to prevent any potential future recurrence.

The exit conference was held on September 14, 2021.

AUDIT CONDUCTED BY

Heidi Pinner, CIA, CISA, CFE, CRMA, Chief Audit Executive
Ben Everett, CPA, CIA, CFE, Audit Manager
Raul Cardona, CIA, CISA, CSX-A, Senior Internal Auditor

TESTING METHODOLOGY

The latest MOU signed with the DHSMV (HSMV-0129-21) on October 2, 2020 includes three sets of standards with a total of 208 security controls. Each of these controls listed in the table below were reviewed and evaluated by the Audit Team.

Standards	Standard / Requirement Sections	Total Controls
Florida Cybersecurity Standards	**Identify**	
	Asset Management	6
	Business Environment & Governance	9
	Risk Assessment	6
	Risk Management	4
	Supply Chain Risk Management	5
	Protect	**30**
	Access Control	7
	Awareness and Training	6
	Data Security	7
	Information Protection Processes	12
	Maintenance & Protective Technology	7
	Detect	**39**
	Anomalies and Events	5
	Security Continuous Monitoring	8
	Detection Processes	5
	Respond	**18**
	Response Planning & Communications	6
	Analysis & Respond Strategy	4
	Mitigation and Improvements	4
	Recover	**14**
	Recovery Planning & Improvements	3
	Communications	3
		6
External Information Security Policy	*Data Security*	6
	Passwords Policy	16
	Encryption and Access Controls	14
	User Account Management	8
	Security Handling & Monitoring	8
	Network Connections/Firewalls	3
	Malware/Virus Protection	6
		61
MOU Statement of Work	*IV. Statement of Work*	20
	V. Safeguarding Information	15
	VI. Compliance & Control Measures	5
		40
	Totals of Standards / Controls	**208**

CRITERIA

During the course of the audit, the Audit Team obtained, reviewed and examined all data security policies, procedures and supporting documentation related to the Clerk's Office driver's license transcript process and corresponding applicable controls contained in the MOU. The 208 security controls included in the MOU cover a broad, comprehensive set of security measures, such as mitigating cybersecurity risks, backing up data, restricting access, encryption methods, password rules, physical protection of assets, audit logging, risk assessments, incident responses, anti-virus software, and data classification.

Each control was evaluated and tested as applicable by the Audit Team. This testing included interviews with IT management and staff, reviews of policies and procedures, observations of system applications, data examination and analysis, and two onsite visits to server storage facilities to determine whether or not appropriate processes are in place to comply with each individual control.

RESULTS

The Audit Team found that many of the controls required by the MOU duplicate throughout the various frameworks and one process or procedure may satisfy multiple controls concurrently. Clerk IT was able to provide responses, documentation, screenshots, explanations, and data that demonstrated compliance with the detailed, in-depth control requirements and standards outlined in the MOU. The Audit Team concluded that the current Clerk's Office software and hardware systems have the necessary controls in place to comply with MOU requirements. In addition, all security policies and procedures examined were approved by senior members of the Information Security Department (Risk Management IT Security Professionals) and meet the requirements as listed in the MOU.

The Audit Team did identify some control improvement opportunities (listed below). These have been mitigated by management during the course of the audit to ensure current security controls comply with the MOU standards and to prevent any potential future recurrence. In many instances a single corrective action addressed multiple opportunities.

Opportunity	Corrective Action Taken	Date
System limitations were not fully documented for areas related to audit logs, password settings, and outside agency access accounts.	Mitigating controls were implemented and/or system limitations and risks were identified, reviewed, analyzed and properly documented through a formal and established risk management process.	August 2021
Policy updates were needed in order to fully comply with MOU requirements language.	IT Security policies including Risk Management, Data Classification, Incident Response Plan, and the User Confidentiality Form were updated by IT Security personnel to incorporate areas / language included in the MOU requirements.	August 2021