

**Internal Control and Data Security Audit
of
Data Exchange Memorandum of Understanding
(MOU) Between Florida Department of Highway
Safety and Motor Vehicles and Seminole County
Clerk of the Circuit Court and Comptroller's Office
(MOU No. HSMV-0190-26)**

REPORT NO. 26-002

DISTRIBUTION LIST

The Honorable Grant Maloy	Clerk of the Circuit Court and Comptroller
Tony Landry	Chief Information System Officer
Mahesh Gunda	FLHSMV MS Business Consultant II



DIVISION OF INSPECTOR GENERAL
Grant Maloy, Clerk of the Circuit Court and Comptroller
Seminole County, Florida

October 6, 2026

To: The Honorable Grant Maloy, Clerk of the Circuit Court and Comptroller

At the request of management, the Division of Inspector General conducted an audit of the internal controls over the Seminole County Clerk of the Circuit Court and Comptroller ("Clerk") office's access and usage of the Drivers' License Transcript and/or Motor Vehicle Record Data Exchange (Data Exchange) provided by the Florida Department of Highway Safety and Motor Vehicles (FLHSMV).

The objectives of our review were to determine whether the internal controls and data security for the Data Exchange comply with the terms of the Memorandum of Understanding (MOU), No. HSMV-0190-26, with FLHSMV. The audit period was October 8, 2025 through August 14, 2026.

We conducted the audit in accordance with standards that 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 findings and conclusions on our audit objectives.

We greatly appreciate the cooperation and support received from Tony Landry, Chief Information Officer, IT Department personnel, and Jen Pizarro, Trial Court Technology Officer for the 18th Judicial Circuit Court.

Respectfully submitted,

Randall Nunley, CPA, CGMA, CIA, CGAP, CRMA, CIG
Inspector General



Internal Control and Data Security Audit of Data Exchange
Memorandum of Understanding (MOU) Between Florida Department of
Highway Safety and Motor Vehicles and Seminole County Clerk of the
Circuit Court and Comptroller's Office
(MOU No. HSMV-0190-26)

Audit Team:

Randall Nunley, CPA, CGMA, CIA, CGAP, CRMA, CIG
Inspector General

Amin Zain, CISA
Inspector General Auditor

Table of Contents

Report Summary	1
Overall Conclusion	1
Audit Objectives and Outcomes	2
Scope and Methodology	2
Background	3
Security of Driver License and Motor Vehicle Exchange	6

Report Summary

Overall Conclusion

At the request of management, the Division of Inspector General conducted an audit of the Seminole County Clerk of the Circuit Court and Comptroller's (Clerk's) Memorandum of Understanding (MOU) with the Florida Department of Highway Safety and Motor Vehicles (FLHSMV) for the driver license transcript data exchange. The MOU (No. HSMV-0190-26) was fully executed by FLHSMV on October 8, 2025.

We conducted the audit in accordance with standards that 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 findings and conclusions on our audit objectives.

Based on our independent and objective assessment, the IT department's governance, risk management, and internal control environment were effective for the scope of this audit. Governance, risk management and internal controls were operating effectively and consistently applied to support the achievement of objectives in the area audited. We identified areas of strength where controls were strong and aligned with the IT department's goals.

The internal controls governing the use and dissemination of personal data obtained from the driver license transcript data exchange have been evaluated for compliance with the requirements of the FLHSMV MOU and applicable laws. Based on our review, the controls are adequate to protect the personal data from unauthorized access, distribution, use, modification, and disclosure. This includes documented data security policies and procedures for personnel to follow and data security policies and procedures in place to protect personal data. The data security policies and procedures were reviewed by a Risk Management IT Security Professional and found to be acceptable to protect personal data.

Our review revealed the Clerk's Office used the FLHSMV's driver license transcript data exchange solely for court purposes to make driver license transcripts available during court proceedings. We identified no issues regarding the Clerk's Office adherence to the requirements of the MOU. While no reportable findings were identified, opportunities for process and governance improvements were noted and communicated separately in a Management Letter.

The exit conference was held on October 6, 2026.

Audit Objectives and Outcomes

The objectives of the audit were to:

- Ensure compliance with the data security requirements in the MOU and other applicable data protection statutes, codes, and policies;
- Determine the adequacy of the Clerk's policies and procedures in place to protect personal data provided by the FLHSMV through the driver license transcript process;
- Determine the adequacy of security over access to the Clerk's Office and FLHMVS data; and,
- Confirm there is appropriate security over the distribution, use, modification, and disclosure of FLHSMV data obtained through the driver license transcript process.
- Verify Clerk's Office personnel who handled/accessed the data received via the Transcript Exchange completed the Information and Cyber Security Awareness training provided by FLHSMV.

As a result of the audit, we determined:

- The Clerk's Office was in compliance with the data security requirements in the data exchange MOU and referenced data protection statutes, codes, and policies.
- The IT Department had adequate policies and procedures in place to protect data provided by the FLHSMV through the driver license transcript process.
- The security controls were adequate to restrict access to FLHSMV data obtained through the driver license transcript process.
- Clerk's Office personnel who handled/accessed the data received via the Transcript Exchange completed the Information and Cyber Security Awareness training provided by FLHSMV.

Scope and Methodology

The scope of this audit included the terms and conditions relating to the data exchange MOU between the Clerk and FLHSMV for the purpose of obtaining driver license transcripts.

Section VII. A. of the MOU requires the completion of an internal control and data security audit on or before the first anniversary of the execution date of the MOU.

Based on the applicable data protections laws and requirements referenced within the MOU, the scope of the audit was to assess the internal controls governing the use and dissemination of personal data obtained.

The audit included examining the internal controls at the Clerk's Office to ensure that they were sufficient to protect the personal data from unauthorized access, distribution, use, modification, and disclosure. The audit period was October 8, 2025 through August 14, 2026.

We reviewed the following:

- The MOU and the applicable statutes, codes, and Clerk's IT policies and procedures;
- The IT program diagrams that identify the design and IT security controls;
- Interviewed appropriate IT personnel to determine the path the driver's license transcript data through FLHSMV, Clerk's Office, and the Courts;
- The IT Internal Control objectives and techniques;
- The internal controls that ensure FLHSMV transcript data is safely secured in the Clerk's Office;
- The security access controls; and,
- The physical security controls that restrict access to computer equipment and the device transcript application and FLHSMV.
- Conducted meetings with the CIO, other IT Department personnel and the Court's Trial Court Technology Officer to understand how it distributed, used, modified, and disclosed, as applicable, FLHSMV driver license transcript data.

Background

On October 8, 2025, a Memorandum of Understanding (MOU) was entered into between the Seminole County Clerk of Court and Comptroller (Clerk' Office) and the Florida Department of Highway Safety and Motor Vehicles (FLHSMV). The referenced MOU contract number is HSMV-0190-26.

The FLHSMV collects and maintains personal information that identifies individuals. The purpose of the MOU is to establish the conditions and limitations under which the FLHSMV agrees to provide electronic access to driver's license and motor vehicle information.

The MOU requires the Clerk's Office to maintain the confidential and exempt status of any and all information and also to ensure that any Third-Party End Users comply with the same confidentiality requirements.

The FLHSMV as the custodian of the state's driver and vehicle records, is required to provide access to records permitted to be disclosed by law. More specifically the following provision:

Section I of the MOU states FLHSMV agrees to provide electronic access to Driver License Information, Motor Vehicle Information, Crash Report Information, Crash Insurance Information, and/or Insurance Record Information to the "Requesting Party" [Clerk's Office]. However, based on our review, walkthrough, and inquiry of the CIO and the Court's Trial Court Technology Officer, the only information the Clerk's Office provides the Court is driver license information.

Sections III and IV of the MOU state in part:

Under this MOU, the Requesting Party [Clerk's Office] will be provided, via remote electronic means, certain Driver License Information, Motor Vehicle Information, Crash Report Information, Crash Insurance Information, and Insurance Record Information, including personal information authorized to be released pursuant to Section 119.0712(2), Florida Statutes and DPPA. By executing this MOU, the Requesting Party [Clerk's Office] agrees to maintain the confidential and exempt status of all information provided by the Providing Agency [FLHSMV] pursuant to this MOU and to ensure that any Third-Party End Users accessing or utilizing information obtained shall do so strictly in compliance with Section 119.0712(2), Florida Statutes and DPPA. Highly restricted personal information shall only be released in accordance with DPPA and Florida law...

The Clerk's IT Department has global protection security controls to ensure that all personal and confidential information is protected from misuse. The Clerk's Office has implemented specific internal security control features to safeguard driver's license information relating to the MOU with FLHSMV which includes, but not limited to, specific driver's license information accessed is required to be associated with a Court case in Seminole County.

The Clerk's IT Department has established physical security controls including:

- Camera security to monitor the Clerk's enterprise computer system. Video is stored on two Network Video Recorders (NVRs) and recordings are retained for 30 days. In addition, Seminole County Sheriff's Office monitors the perimeters of the Clerk's office with video and on-site security 24 hours a day, 7 days a week.
- Access to the MIS department, which is secured with a second and more restrictive electronic badge
- The enterprise computer system is locked in a physically secured location within the MIS Data Center. This provides a third layer of physical access control via a physical locked cage.
- The MIS Data Center, servers, network, environmental control, and workstations are protected from power loss with a redundant set of Uninterruptible Power Supply (UPS) devices. This is a redundant system in itself as the building's generator will provide power in the case of a utility supplied power outage.

At the request of the Clerk's Chief Information Officer, the Clerk's Division of Inspector General conducted an audit of the internal data security controls to ensure compliance with the requirements of the MOU.

Section VII (A) of the MOU states the following:

"Internal Control and Data Security Audit – This MOU is contingent upon the Requesting Party [Clerk's Office] having appropriate internal controls in place at all times to ensure that the information provided or received pursuant to this MOU is protected from unauthorized access, distribution, use, modification or disclosure. The Requesting Party [Clerk's Office] must submit to the Providing Agency an Internal Control and Data Security Audit from a currently licensed Certified Public Accountant, on or before the first anniversary of the execution date of this MOU or within one hundred twenty (120) days form receipt of a written request from the Providing Agency [FLHSMV]. Government agencies may submit the Internal Control and Data Security Audit from the Agency's Internal Auditor or Inspector General. The audit report shall indicate whether the internal controls governing the use and dissemination of personal data have been evaluated based on the requirements of this MOU, and applicable laws and include an opinion on whether those internal controls are adequate to protect the personal data from unauthorized access, distribution, use, modification, or disclosure. This includes both policies/procedures in place for personnel to follow and data security procedures/policies in place to protect personal data. This audit shall indicate that the data security procedures/polices have been approved by a Risk Management IT Security Professional. The audit shall also indicate that any and all deficiencies/issues found during the audit have been corrected and measures enacted to prevent recurrence..."

We conducted the audit in accordance with standards that 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.

The scope of this audit included the terms and conditions relating to the data exchange MOU between the Clerk and FLHSMV for the purpose of obtaining driver license transcripts.

Section VII (A) of the MOU requires the completion of an internal control and data security audit on or before the first anniversary of the execution date of the MOU.

Based on the applicable data protections laws and requirements referenced within the MOU, the scope of the audit was to assess the internal controls governing the use and dissemination of personal data obtained.

The audit included examining the internal controls at the Clerk's Office to ensure that they were sufficient to protect the personal data from unauthorized access, distribution, use, modification, and disclosure. The audit period was October 8, 2025 through August 14, 2026.

We reviewed the following:

- The MOU and the applicable statutes, codes, and Clerk's IT policies and procedures;
- The IT program diagrams that identify the design and IT security controls;
- Interviewed appropriate IT personnel to determine the path the driver's license transcript data through FLHSMV, Clerk's Office, and the Courts;
- The IT Internal Control objectives and techniques;
- The internal controls that ensure FLHSMV transcript data is safely secured in the Clerk's Office;
- The security access controls; and,
- The physical security controls that restrict access to computer equipment and the device transcript application and FLHSMV.

Security of Driver License and Motor Vehicle Exchange

The purpose of the Data Exchange MOU was to establish the conditions and limitations under which the FLHSMV agreed to provide electronic access to driver's license information to the Clerk. Therefore, the Clerk's IT Department established a policy to ensure information exchanged will not be used for any purposes not specifically authorized by the MOU with FLHSMV.

This policy is designed to establish a secure and confidential Internal Control Environment that ensures that information exchanged will not be used for any purposes not specifically authorized by the Memorandum of Understanding (MOU). The Clerk's IT Department has developed security requirements and standards consistent with Florida Statutes, Florida Administrative Code and the Florida Department of Highway Safety and Motor Vehicles ("DHSMV").