Office of

Nikki Alvarez-Sowles, Esq.

Pasco County Clerk & Comptroller

CCC Driver and Vehicle Information Database (DAVID) Attestation

Report No. 2025-01

Department of
Inspector General
July 28, 2025

Christine Calianno, CIG, CIGA, CGAP, CFE
Inspector General

Erika Hendricks, CIA, CIGA, CFE
Auditor III

#ServeAndConnect

Office of Pasco County Clerk & Comptroller

INTRAOFFICE MEMORANDUM

DATE: July 28, 2025

TO: Nikki Alvarez-Sowles, Esq., Clerk & Comptroller

FROM: Christine Calianno, Inspector General

DEPARTMENT: Department of Inspector General

SUBJECT: Report No. 2025-01, CCC Driver and Vehicle Information Database (DAVID) Attestation

---

This audit was included as a planned project on the Department of Inspector General's 2025 Annual Audit Plan. The purpose of this audit was to:

- Determine if the Office of Pasco County Clerk & Comptroller was in compliance with the Memorandum of Understanding for governmental entity access to the Driver and Vehicle Information Database (DAVID) system, contract #HSMV-0615-19.

- Evaluate the adequacy of internal controls over personal data obtained from DAVID.

The Department of Inspector General appreciates the cooperation, professional courtesy, and responsiveness received from management during this audit.

Cc: Kimberly Thompson, Chief Operations Officer
Tim Jamison, Information Technology Director
Leonard Mattison, Criminal Courts Director

TABLE OF CONTENTS

EXECUTIVE SUMMARY 2

Background Information 2

Objectives 3

Scope 3

Methodology 4

Criteria 4

OPPORTUNITIES FOR IMPROVEMENT AND RECOMMENDATIONS 5

Compliance 5

Control 8

Observations 11

EXECUTIVE SUMMARY

Contract #HSMV-0615-19, a Memorandum of Understanding (MOU) made between the Office of Pasco County Clerk & Comptroller (the Office) and the Florida Department of Highway Safety and Motor Vehicles (FLHSMV) was executed on May 29, 2019. Compliance requirements are outlined in the MOU.

Based on the results of this audit, the Department of Inspector General (Department) concluded that the Office met the requirements of the MOU. Adequate controls were designed for the required control areas of the MOU; however, certain control areas were not operating effectively, and some process procedures were not formally defined for specific areas. The audit results are summarized below:

Control Area	Result
Safeguarding Information	☑
User Access & Permission Management	☑
User Activity Monitoring	☑

Legend:	☑	Controls are in place & operating effectively.	☑	Controls are partially in place and/or not operating effectively.	☑	Controls are not in place.

Opportunities for improvement and recommendations were discussed with management, and corrective actions were taken by management for all issues identified during the audit.

Background Information

FLHSMV is responsible for maintaining the Driver and Vehicle Information Database (DAVID). This database is a central repository for driver's license, vehicle registration, and other related information. Information stored in DAVID includes personal information[1]. Due to the confidential nature of this information, it is protected against disclosure[2] and exempt from public records under Florida Statute[3].

According to the MOU, the Office is required to submit an Attestation Statement from their Internal Auditor, Inspector General, Risk Management IT Security Professional, or a currently licensed Certified Public Accountant, on or before the third and sixth anniversary of the agreement or within 180 days from receipt of a request for an attestation from FLHSMV. The purpose of the attestation is to affirm that internal controls over personal information were

[1] As described in Chapter 119, Florida Statutes, information found in the motor vehicle record which includes, but is not limited to, the subject's driver identification number, name, address, telephone number, social security number, medical or disability information, and emergency contact information.

[2] 18 USC 2721: Prohibition on release and use of certain personal information from State motor vehicle records.
[3] F.S. Section 119.0712(2): Executive branch agency-specific exemptions from inspection or copying of public records.

evaluated and controls were adequate to protect it from unauthorized access, distribution, use, modification, or disclosure. The Attestation Statement also certifies that any and all deficiencies identified during the audit were corrected and measures were enacted to prevent recurrence.

A total of 18 teammates in three departments had DAVID access (as of February 10, 2025):

- Information Technology - 3 teammates. These teammates were designated as Point-of-Contact (POC) for the Office. The MOU defined this role as a person(s) appointed by the Requesting Party (the Office) as the administrator of the DAVID program in their agency. The POCs ensured appropriate internal controls were implemented and maintained to protect data obtained through DAVID. The POCs had administrative functions and were responsible for reviewing DAVID user status and activity. The POCs also granted DAVID access and assigned user roles and permissions based on job duties.

- Criminal- 13 teammates. These teammates used the DAVID system primarily to access driver license and vehicle information to process impound orders and citations. As an additional internal control over DAVID users, the Office also designated a Department Audit Contact (DAC) within Criminal to review user status and activity.

- Inspector General - 2 teammates. These teammates had access to the DAVID system for audit purposes only. Department auditors verified user activity to determine compliance with the requirements of the MOU.

Objectives

The audit objectives were to:

- Determine if the Office was in compliance with the terms of the MOU (contract #HSMV-0615-19).

- Determine if internal controls over DAVID information were adequate to protect it from unauthorized access, distribution, use, modification, or disclosure.

Scope

The audit period was from January 6, 2024, through January 6, 2025. The scope was limited to the requirements specified in the MOU. The nature and scope of the audit was intended to provide objective and relevant assurance, and to contribute to the effectiveness and efficiency of governance, risk management, and control processes of the area under review.

Although the Department exercised due professional care in the performance of this audit, this does not mean unreported noncompliance and/or irregularities did not exist. The deterrence of fraud, waste, or abuse is the responsibility of management. Audit procedures alone cannot guarantee that fraud, waste, or abuse were detected.

The audit was neither designed nor intended to be a detailed study of every relevant system, procedure, or transaction. It was not an appraisal or rating of management.

Methodology

The audit procedures included, but were not limited to, the following:

- Reviewed the MOU (contract #HSMV-0615-19).
- Reviewed internal policies and procedures related to the use and oversight of DAVID.
- Interviewed key personnel involved in the DAVID oversight process and a random sample of DAVID users.
- Reviewed *DAVID User Activity Reports* to determine if information was used for business-related purposes. The information searched was traced to the associated case in Clericus for validity.
- Observed safeguarding measures over DAVID information to determine if physical and electronic access controls ensured that information was protected from unauthorized access, distribution, use, modification, or disclosure.
- Verified the most recent prior *Annual Certification Statement* and *Attestation Statement* were submitted to FLHSMV, as specified by the MOU.
- Verified quarterly quality control reviews were conducted, as specified by the MOU and internal policies and procedures.
- Verified all active users had a signed *DAVID Access Authorization Request Form* on file.
- Verified user access and permission roles were appropriate for all active users.
- Verified DAVID access was disabled within five working days upon the teammate's termination, separation, or reassignment, as specified by the MOU.

Criteria

To conduct this audit, the Department relied on the following criteria:

- *Memorandum of Understanding for Governmental Entity Access to DAVID* (contract # HSMV-0615-19), dated May 29, 2019
- Amendment No. 1 to the *Memorandum of Understanding for Governmental Entity Access to DAVID* (contract #HSMV-0615-19), dated July 2, 2019
- *DAVID Access Authorization Request Form*, revised September 2014
- *DAVID Quarterly Audit Guideline*, revised January 16, 2025
- *Quarterly DAVID Audit Log*, revised June 12, 2024
- *DAVID Quarterly Quality Control Review Report*, revised June 26, 2014
- *DAVID User Access Guideline*

The Department identified seven opportunities for improvement and one observation:

	Opportunities for Improvement	
	Compliance	**Page**
1.	Safeguarding printed and electronic personal data obtained from the DAVID system.	5
2.	Updating DAVID system user access.	6
3.	Properly documenting searches in the DAVID system.	7
	Control	**Page**
4.	Improving existing procedures for password security.	8
5.	Updating *DAVID Access Authorization Request Forms*.	8
6.	Updating user permissions in the DAVID system.	9
7.	Improving existing DAVID procedures and guidelines to reflect current operations, additional internal controls, and clarification for some processes.	9
	Observations	
A.	Implementing policy management software and consolidating DAVID guidance to create a multi-departmental procedure.	11

OPPORTUNITIES FOR IMPROVEMENT AND RECOMMENDATIONS

Compliance: Compliance is adhering to approved policies and procedures, agreements, contracts, laws, rules, and regulations. Opportunities to improve compliance were identified below.

1. Safeguarding printed and electronic personal data obtained from the DAVID system.

According to MOU Section V, Safeguarding Information:

- Subsection E: When printed information from DAVID is no longer needed, it shall be destroyed by cross-cut shredding or incineration.
- Subsection G: Access to DAVID-related information, particularly data from the DAVID system, will be protected in such a way that unauthorized persons cannot view, retrieve, or print the information.

During testing, the following was noted:

A. Criminal teammates were instructed to place printed DAVID information in OSA (Obsolete, Superseded, or Administrative Value Lost) boxes when the information

was no longer needed. However, OSA boxes were not physically secured from access by unauthorized persons.

B. Some teammates with DAVID access telework. However, computer screens at workstations were not required to be blacked out while accessing the DAVID system remotely.

Recommendation:
R.1: Since compliance with agreements, contracts, laws, rules, regulations, policies, and procedures are required, a recommendation was not provided.

Criminal Management Response:
- *Agree*
- *Agree*

Corrective Action Plan:
- *A new bulletin (CDB 25-10) was sent via email for accessing DAVID remotely. DAVID is required to be accessed through a computer using the Splashtop application when working remotely. Teammates teleworking are required to black out their screens when accessing DAVID and will restore their screens at the conclusion of DAVID use.*

- *Five cross-cut shredders were ordered to be placed in Criminal areas that access DAVID. These shredders were delivered and placed in the supervisor's offices of all areas of Criminal that may potentially print DAVID materials.*

- *Bulletin CDB 25-04 was issued regarding restrictions on printing DAVID material.*

- *Bulletin CDB 25-14 was issued that directs printed DAVID material to be disposed of by use of the crosscut shredders.*

Completion Date:
- *February 2025*
- *March 2025*
- *January 2025*
- *March 2025*

2. Updating DAVID system user access.

According to MOU Section IV, Statement of Work:

- Subsection B.8: The Requesting Party (the Office) must update user access/permissions upon reassignment of users within five (5) business days.

During testing, the following was noted:

A. One user was deactivated 55 working days after reassignment/transfer to a new position that did not require use of the DAVID system. The Department verified the teammate did not access the DAVID system after their reassignment/transfer date.

Recommendation:
R.2: Since compliance with agreements, contracts, laws, rules, regulations, policies, and procedures are required, a recommendation was not provided.

IT Management Response:

- *Agree*

Corrective Action Plan:

- *The importance of security form completion was discussed with the POCs and Information Technology Security team. The DAVID Quarterly Audit Guideline was also updated to clarify the MOU requirements.*

Completion Date:

- *January 2025*

3. Properly documenting searches in the DAVID system.

According to the *DAVID Quarterly Audit Guideline:*

- User Standard Search Procedure (page 11): A reason code must be entered for every search performed.

Of the 67 DAVID searches included in testing, the following was noted:

A. For four searches performed by one user, the user entered the case or citation number, but did not enter a reason code. The Department verified the searches were for a valid business purpose.

Recommendation:
R.3: Since compliance with agreements, contracts, laws, rules, regulations, policies, and procedures are required, a recommendation was not provided.

Criminal Management Response:

- *Agree*

Corrective Action Plan:

- *The specific user was reminded of the requirement to ensure they include a purpose code for all DAVID searches and to follow the DAVID User Access Guideline.*

- *A bulletin was sent to Criminal teammates to remind them of the DAVID User Access Guideline, the DAVID bulletins, and where this information can be found.*

Completion Date:

- *May 2025*
- *March 2025*

Control: The primary purpose of internal controls is to help safeguard an organization and further its objectives. Internal controls function to minimize risks and protect assets, ensure accuracy of records, promote operational efficiency, and encourage adherence to policies, rules, regulations, and laws. Opportunities to improve internal controls were identified below and recommendations were provided.

4. Improving existing procedures for password security.

Some practices did not demonstrate effective password security.

A. Teammates used the web browser's autofill feature to save their username and password for DAVID login and did not lock their workstation when it was unattended.

B. Passwords were kept in an envelope stored in an unlocked desk drawer.

Recommendation:
R.4: Update the *Computer, Internet, and Email Usage Guideline* to include detailed procedures for locking computers and storing passwords.

IT Management Response:
- *Agree*

Corrective Action Plan:
- *The Computer, Internet, and Email Usage Guideline was updated to include language for locking computers when unattended, prohibited password practices, and requirements for storing passwords. The updated guideline was published on OfficeNet.*

Completion Date:
- *March 2025*

5. Updating *DAVID Access Authorization Request Forms*.

One *DAVID Access Authorization Request Form* was not updated to reflect the teammate's correct department.

Recommendation:
R.5: Update the *DAVID Access Authorization Request Form* to reflect the correct department.

IT Management Response:
- *Agree*

Corrective Action Plan:
- *The DAVID Access Authorization Request Form was updated to reflect the correct department.*

Completion Date:
- *March 2025*

6. Updating user permissions in the DAVID system.

DAVID user permissions were not updated for some users.

A. Criminal: Permission settings for users' roles were not consistent. 5 of the 13 users had permission settings to search by vehicle make and model, which was not necessary for Criminal users' roles.

B. Criminal and Inspector General: There were variations of days and hours for DAVID access.

Recommendation:
R.6: Update access for all teammates to reflect the correct user permission roles and access.

IT Management Response:
- *Agree*

Corrective Action Plan:
- *For Criminal and IG users, management determined days and hours of access to the DAVID system will be Monday – Friday 7:00 a.m. – 7:00 p.m. Criminal users required the following permission roles: search/view motor vehicle record, search/view driver license record, and view driver history. The POC will use these as standards for new teammates unless directed otherwise. User permission roles and access were updated in the DAVID system to reflect new standard.*

Completion Date:
- *March 2025*

7. Improving existing DAVID procedures and guidelines to reflect current operations, additional internal controls, and clarification for some processes.

Some process procedures were not documented, complete, or updated to reflect current practices.

Procedures or internal controls not documented:

A. Updating changes to the name of the Requesting Party (the Office), its Agency head, its POC, address, telephone number, and/or e-mail address in the DAVID system within ten calendar days of occurrence.

B. Monitoring access to restricted DAVID network folders on a regular basis to ensure user permissions are appropriate.

C. Assigning and reviewing user permission roles in the DAVID system.

D. Assigning a back-up DAC to perform quarterly quality control review responsibilities when needed.

E. Performing standard searches and properly logging out of the DAVID system by DAVID users.

Procedures not documented in the proper format according to the Office standard:

A. The *DAVID Quarterly Audit Guideline* (revised January 16, 2025) provided the steps used during the quarterly audit to detect potential misuse of the DAVID system and the actions required based on the results. It was not intended to be applied as an office-wide guideline, rather it documented quarterly audit procedures applicable to the IT and Criminal departments.

Procedures not updated or complete:

A. The *DAVID Quarterly Audit Guideline* (revised January 16, 2025), pages 2-10, Dual Control Process & Quarterly Quality Control Review, did not include proper segregation of duties or complete search procedures. In addition, the case and citation number verification process was not updated to reflect current practices.

Recommendation:

R7.1: Implement a formal procedure for updating changes in the requesting party's agency head, its POC, address, telephone number and/or email addressing the DAVID system within 10 calendar days.

R7.2: Change the *DAVID Quarterly Audit Guideline* to a procedure.

R7.3: Update the *DAVID Quarterly Audit Guideline* to reflect the current processes and internal controls described above.

R7.4: Implement a formal procedure for monitoring access to the restricted DAVID folders.

R7.5: Implement a formal procedure for assigning user roles and permissions in the DAVID system.

R7.6: Update the *DAVID User Access Guideline* to include guidance for how to conduct searches in the DAVID system, including how to properly log out of the DAVID system.

Criminal and IT Management Response:

- *Agree to all*

Corrective Action Plan:

- *The DAVID Quarterly Audit Guideline was changed to a procedure (DAVID Quarterly Audit Procedure, IT-OP0035). This procedure was updated to reflect the recommendations above (R7.2 and R7.3). DAVID POC Security Procedure, IT-OP0036 was also created to address recommendations above (R7.1, R7.4, and R7.5).*

- *The DAVID User Access Guideline was updated to reflect the recommendation above (R7.6). This guideline was republished on OfficeNet.*

Completion Date:

- *Completed April 2025*
- *Completed April 2025*

Observations: Observations noted during the audit process that were outside the scope of the audit, but important enough to bring to management's attention were identified below.

A. Implementing policy management software and consolidating DAVID guidance to create a multi-departmental procedure.

During testing, the following was noted:

A. Criminal and Information Technology had independent versions of DAVID audit procedures. Management confirmed that Criminal's *DAVID Audit Process Guideline* (dated October 31, 2022) and *DAVID Audit Procedure*, *CR-000 (*draft), dated May 31, 2022, were obsolete and were replaced with IT's *DAVID Quarterly Audit Guideline (*revised January 16, 2025*)*.

B. Some DAVID users in Criminal were unaware of documented DAVID procedures and guidelines.

C. Updates to DAVID procedures were communicated via email to Criminal teammates through Criminal Department Bulletins (CDBs). Procedures and guidelines were updated as time permitted to reflect information presented in CDBs.

Recommendation:

RA.1: Consider implementing policy management software.

RA.2: Consolidate DAVID guidance to create a multi-departmental procedure.

RA.3: Ensure information presented in Criminal Department Bulletins related to DAVID has been updated in associated procedures or guidelines.

Criminal and IT Management Response:

- *RA.1 – Agree*
- *RA.2 – Agree*
- *RA.3 – Agree*

Corrective Action Plan:

- *RA.1 – The policy management software program Comply that is within NeoGov may be the program to use. Reviewing the program and tools is required to determine how to proceed and determined as an Officewide solution for management of all policies, procedures, and guidelines.*

- *RA.2 – For the security and authenticity of the audit, the procedure documents are contained in three documents. The DAVID POC Security Procedures are for teammates assigned to the POC roles and responsibilities. The DAVID Quarterly*

Audit Procedures are an intra-departmental procedure for teammates assigned to the POC and DAC roles and responsibilities. The DAVID User Access Guideline is for all teammates with access to DAVID. The separation of procedures protects the integrity of the DAVID audit process.

- *RA.3 – The DAVID User Access Guideline is reviewed and updated following the issuance of a bulletin that outlines the change(s) to a procedure.*

Completion Date:

- *RA.1 – To be determined once an Officewide solution is determined and implemented.*
- *RA.2 – Not applicable*
- *RA.3 – On-going*

For additional information contact the Public Records Liaison.
publicrecordsrequest@pascoclerk.com

Public Records Liaison, P.O. Box 338, New Port Richey, FL 34654-0338
www.pascoclerk.com

Follow us on our socials!

@PascoClerk