

Motorist Services DAVID Audit Review

Consulting Engagement 201213-35

October 21, 2013

Executive Summary

The Bureau Chief of Records requested the Office of Inspector General conduct a review of the Department's Driver and Vehicle Information Database (DAVID) Audit process. Beginning early 2013, Motorists Services staff began conducting audits based on the Memorandum of Understanding (MOU) each agency (law enforcement and non-law enforcement) signs to obtain access to Department systems.

The Department's DAVID system has over 60,000 users in law enforcement, criminal justice, and other state and local agencies. DAVID was originally developed within the Department strictly for law enforcement use; however, in the last five years, the use of DAVID has grown significantly, from 3 million queries per month to 6.4 million queries per month. DAVID is a tool users depend on to perform their job duties, which range from law enforcement purposes ensuring highway safety, to the administration of child support, the Help America Vote Act, and child and adult protective services.

Government agencies must have an MOU with the Department to gain access to the information contained in DAVID. The MOU establishes the purposes for and conditions of electronic access to the DAVID database.

Our review provided four considerations for the Division of Motorist Services:

- Maintain a spreadsheet containing MOU anniversary dates, due dates, and acquisition dates of Requesting Parties' attestations and affirmations;
- Develop a detailed audit process requiring documentation of quality control reviews, confidential and criminal acknowledgements, agency provided training, and the process for reporting misuse when questions are answered in the affirmative;
- Implement a complete audit schedule, to include anticipated and actual audit dates, corrective action plan due dates, follow-up audit dates, and results of each audit to reference for future audits; and
- Implement a more frequent follow-up process for corrective action plans.

Background and Introduction

The Bureau Chief of Records requested the Office of Inspector General conduct a review of the Department's DAVID Audit process. In the beginning of 2013, Motorists Services staff began conducting audits based on the MOU each agency (law enforcement and non-law enforcement) signs to obtain access to Department systems.

The Department's DAVID system has over 60,000 users in law enforcement, criminal justice, and other state and local agencies. DAVID was originally developed within the Department strictly for law enforcement use; however, in the last five years, the use of DAVID has grown significantly, from 3 million queries per month to 6.4 million queries per month. DAVID is a tool users depend on to perform their job duties, which range from law enforcement purposes ensuring highway safety, to the administration of child support, the Help America Vote Act, and child and adult protective services.

The Department plans to audit each law enforcement agency (police departments, sheriff offices, and State Attorney Offices) every two years (approximately 400). Each non-law enforcement agency (property appraisers, clerk of courts, third party vendors, etc.) will be audited every three years (approximately 400). The Department has seven liaisons conducting DAVID audits.

DAVID audits are currently conducted as follows:

- The law enforcement agency is sent a 30 day notification that the Department will be conducting a DAVID audit. The Department provides the audit questions and quarterly quality control review documentation the agency is required to complete.
- The Liaison conducts an on-site audit. The Department has a standard set of 14 audit questions (See Exhibit 1) which are asked of the agency contact.
 - If the agency has no initial findings, the attestation is left with the agency to have the appropriate personnel sign.
 - If the agency has findings, the agency is provided 30 days to respond to the Department with a corrective action plan.
- Each liaison has 30 days to provide an agency summary to the DAVID Audit Supervisor for review and approval. Once the summary is approved by the DAVID Audit Supervisor, the Department's summary is forwarded to the audited agency.

- The Department follows up on the corrective action plan during the next two year audit.

Agencies must have an MOU with the Department to gain access to the information contained in DAVID. The MOU establishes the purposes for and conditions of electronic access to the Department's DAVID system.

Results of Review

We reviewed the Department's MOU and found the following key elements which we recommend be included in more detail in the Department's DAVID Audits to further enhance the Department's DAVID Audit process:

- Section IV, Part B, Subsection 9, of the MOU, titled Statement of Work, states, "The Requesting Party agrees to: Update user access permissions upon termination or reassignment of users within 5 working days and immediately update user access permissions upon discovery of negligent, improper, or unauthorized use or dissemination of information. Conduct quarterly quality control reviews to ensure all current users are appropriately authorized."
- Section V of the MOU, titled Safeguarding Information, states, "The Parties shall access, use, and maintain the confidentiality of all information received under this agreement in accordance with Chapter 119, Florida Statutes, and the Driver's Privacy Protection Act (DPPA). Information obtained under this agreement shall only be disclosed to persons to whom disclosure is authorized under Florida law and federal law. Any person who willfully and knowingly violates any of the provisions of this section is guilty of a misdemeanor of the first degree punishable as provided in sections 119.10 and 775.083, Florida Statutes. In addition, any person who knowingly discloses any information in violation of DPPA may be subject to criminal sanctions and civil liability." Specifically, the MOU states the Parties mutually agree to the following:
 - Information exchanged by electronic means will be stored in a place physically secure from access by unauthorized persons;
 - All personnel with access to the information exchanged under the terms of this agreement will be instructed of, and acknowledge their understanding of, the confidential nature of this information. These acknowledgement must be maintained in a current status by the Requesting Party;
 - All personnel with access to the information will be instructed of, and acknowledge their understanding of, the criminal sanctions specified in state law for unauthorized use of the data. These acknowledgements must be maintained in a current status by the Requesting Party; and

- All access to the information must be monitored on an on-going basis by the Requesting Party. In addition, the requesting party must complete an annual audit to ensure proper and authorized use and dissemination.
- Section VI, Part A, of the MOU, titled Internal Control Attestation, states, “This MOU is contingent upon the Requesting Party having appropriate internal controls over personal data sold or used by the Requesting Party to protect the personal data from unauthorized access, distribution, use, modification, or disclosure. Upon request from the Providing Agency, the Requesting Party must submit an attestation from a currently licensed Certified Public Accountant performed in accordance with American Institute of Certified Public Accountants (AICPA) ‘Statements on Standards for Attestation Engagement’. In lieu of submitting the attestation from a currently licensed Certified Public Accountant, Requesting Party may submit an alternate certification with pre-approval from the Department. In the event the Requesting Party is a governmental entity, the attestation may be provided by the entity’s internal auditor or inspector general. The attestation must indicate the internal controls over personal data have been evaluated and are adequate to protect personal data from unauthorized access, distribution, use, modification, or disclosure. The attestation must be received by the Providing Agency within 180 days of the written request. The Providing Agency may extend the time to submit the attestation upon written request and for good cause shown by the Requesting Agency.”
- Section VI, Part B, of the MOU, titled Internal Control Attestation, states, “Misuse of Personal Information – The Requesting Party must immediately notify the Providing Agency and the affected individual following the determination that personal information has been compromised by any unauthorized access, distribution, use, modification, or disclosure. The statement to the Providing Agency must provide the date and the number of records affected by any unauthorized access, distribution, use, modification, or disclosure of personal information. Further, as provided in Section 817.5681, Florida Statutes, the document must provide a statement advising if individuals whose personal information has been compromised have been notified and, if not, when they will be notified. The statement must include the corrective actions and the date these actions are completed by the requesting Party.”
- Section VI, Part C, of the MOU, titled Internal Control Attestation, states, “The Providing Agency shall receive an annual affirmation from the Requesting Party indicating compliance with the requirements of this agreement no later than 45 days after the anniversary date of this agreement.”

Upon review of the Department's current DAVID Audit process and the Department MOU, we provide the following considerations to the Division of Motorist Services:

- Currently, the Department maintains the signed affirmations and attestations but not a historical spreadsheet encompassing all information. We recommend maintaining a historical spreadsheet containing MOU anniversary dates, due dates, and acquisition dates of Requesting Parties' attestations and affirmations, to ensure that affirmations and attestations are received by all required agencies and are submitted timely;
- According to the DAVID Audit Supervisor, documentation of affirmative responses is not collected at the time of the audit. We recommend the Department develop a detailed audit process requiring documentation of quality control reviews, confidential and criminal acknowledgements, and agency provided training, to ensure audits are consistently performed and law enforcement agencies can support their responses. We also recommend the audit process include reviewing agency procedures to report misuse to determine if the procedures ensure compliance with the requirements of the MOU;
- Although the DAVID Audit Supervisor stated they are developing a list of agencies to audit, we recommend implementing a complete audit schedule to provide management the information necessary to properly supervise the audit process. The audit schedule should include anticipated and actual audit dates, corrective action plan due dates, follow-up audit dates, and results/findings of each audit to reference for future audits. Each liaison should have a listing of agencies which will be audited, anticipated and actual dates of audit to determine timeframes for future scheduling, corrective action plan due dates if there are findings, and the results of the audits to determine if penalties need to be assessed; and
- Currently, the Department does not conduct a follow-up review and waits until the biennial review to verify corrective actions have been implemented. We recommend the Department implement a more frequent follow-up process for corrective action plans to ensure corrective actions are implemented timely.

Purpose, Scope, and Methodology

The Bureau Chief of Records requested the Office of Inspector General conduct a review of the process used to audit external agencies' DAVID use.

The purpose of this engagement was to determine if the process used to audit external agencies' DAVID use is adequate to meet the requirements of the Memorandum of Understanding.

The scope of this engagement was limited to reviewing the process used to audit external agencies' DAVID use.

The methodology included:

- Reviewing applicable Florida Statutes (F.S.);
 - Chapter 119, F.S.
 - Chapter 319, F.S.
 - Chapter 320, F.S.
 - Chapter 321, F.S.
 - Chapter 322, F.S.
 - Chapter 713, F.S.
 - Chapter 775, F.S.
- Reviewing 18 United States Code section 2721 et seq. - Driver's Privacy Protection Act of 1994 (DPPA)
- Reviewing the Memorandum of Understanding - Drivers License and/or Motor Vehicle Record Data Exchange; and
- Interviewing Motorist Services staff.



Distribution, Statement of Accordance, and Project Team

Distribution

Julie L. Jones, Executive Director
Boyd Walden, Director of Motorist Services

Copies distributed to:

Diana Vaughn, Deputy Executive Director
Terry Rhodes, Chief of Staff
Steven Fielder, Deputy Director of Motorist Services
Maureen Johnson, Bureau Chief of Records

Statement of Accordance

Section 20.055, Florida Statutes, requires the Florida Department of Highway Safety and Motor Vehicles' Inspector General to review, evaluate, and report on policies, plans, procedures, accounting, financial, and other operations of the Department and to recommend improvements. This consulting engagement was conducted in accordance with applicable *The International Standards for the Professional Practice of Internal Auditing* published by the Institute of Internal Auditors and Principles and Standards for Inspectors General published by the Association of Inspectors General.

Project Team

Engagement conducted by:
Doane Rohr, Auditor

Under the supervision of:
David Ulewicz, Audit Director

Approved by:


Julie M. Leftheris, Inspector General

Exhibit 1: Department DAVID/DAVE/IRIS Audit Questionnaire



Julie L. Jones
Executive Director

2900 Apalachee Parkway
Tallahassee, Florida 32399-0500
www.flhsmv.gov

DAVID/DAVE/IRIS Audit

Below is a guide to be used to conduct your agency's audit and prepare the attestation requested in the attached letter. The questions are taken directly from Section IV B and Section V of the MOU between your agency and the Department of Highway Safety & Motor Vehicles (DHSMV). When completed, please have the attestation prepared pursuant to Section VI A of the MOU and mail the original signed copy to the address on the attached letter.

1. Has your agency conducted quarterly quality control reviews to ensure all current users are appropriately authorized?
2. Have all personnel with access to the information been instructed on their understanding of the confidential nature of the information?
3. Are confidential acknowledgements being maintained in a current status?
4. Have all personnel with access to the information been instructed on their understanding of the criminal sanctions that are specified in state law for unauthorized use of the data?
5. Are criminal acknowledgements being maintained in a current status?
6. Has your agency assigned, sub-contracted, or transferred any rights, duties, or obligations under the MOU without the consent and approval of DHSMV?
7. Has any information exchanged as a result of the MOU been used for any purpose not specifically authorized?
8. Is the information exchanged by electronic means stored in a physically secure location?
9. Is access to the information exchanged protected in such a way that unauthorized persons cannot review or retrieve the information?
10. Is your agency updating user access permissions upon termination or reassignment within five working days?
11. Is your agency immediately updating user access permissions upon discovery of negligent use, improper use, unauthorized use or unauthorized dissemination?
12. Has your agency had any misuse in the last twelve months?

• Service • Integrity • Courtesy • Professionalism • Innovation • Excellence •
An Equal Opportunity Employer

13. If agency has had misuse in the last twelve months, has it been reported to DHSMV?
14. Randomly select ten users (if you have less than 10 users, select all users) and run an audit report for a randomly selected week. Look for any misuse, including, but not limited to reason codes, running siblings, spouses, ex-spouses, celebrities, and political figures. Look at the times of day the data was accessed. Was it before or after the person's regular shift? Look for repeated runs of the same individual, and look for unexplained access to the Emergency Contact Information.

List the names of the ten users below that you ran an audit on.

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____