DEPARTMENT OF BUSINESS AND PROFESSIONAL REGULATION

Office of Inspector General

Audit Report A-1617BPR-024

Audit of Internal Controls for Driver and Vehicle Information Database (DAVID)

May 2017
MEMORANDUM

TO: Matilde Miller, Interim Secretary
FROM: Lynne T. Winston, Inspector General
DATE: May 11, 2017

SUBJECT: Audit of Internal Controls for Driver and Vehicle Information Database (Report Number A-1617BPR-024)

The attached report presents the results of our Audit of Internal Controls for Driver and Vehicle Information Database (DAVID). Our audit found that the Division of Alcoholic Beverages and Tobacco's internal controls over the personal data accessed through DAVID are adequate to protect the data from unauthorized access, distribution, use, modification, or disclosure.

In accordance with Section 20.055, Florida Statutes, we provided our preliminary findings and recommendations for management's review and response. Division Director Philpot's response is included in the final report.

We would like to thank the management and staff of the Division of Alcoholic Beverages and Tobacco for their cooperation and assistance during the course of our review. We appreciate the time spent with us in interviews and working conferences, as well as the timely response to our requests for information and supporting documentation.

cc: Jonathan Zachem, Deputy Secretary of Business Regulation
    Thomas R. Philpot, Director, Division of Alcoholic Beverages and Tobacco
    Janet Hartman, Deputy Director, Division of Alcoholic Beverages and Tobacco
    Sherrill F. Norman, Auditor General
    Eric Miller, Chief Inspector General
EXECUTIVE SUMMARY

The Division of Alcoholic Beverages and Tobacco (AB&T, division), Bureau of Law Enforcement (bureau, BLE) accesses driver license and motor vehicle information pursuant to a Memorandum of Understanding (MOU, agreement) with the Department of Highway Safety and Motor Vehicles (DHSMV). The MOU permits authorized department employees to access certain driver license and motor vehicle data and information through the DHSMV’s Driver and Vehicle Information Database (DAVID).

The agreement provides that upon the DHSMV’s request, the Inspector General must provide an attestation indicating that the internal controls over the personal data accessed through the database have been evaluated and are adequate to protect the personal data from unauthorized access, distribution, use, modification, or disclosure. The DHSMV notified our department in a letter dated October 18, 2016, that our department had been randomly selected to submit such an attestation.

Accordingly, the purpose of this audit was to evaluate whether the department’s internal controls over the personal data accessed through DAVID were adequate to protect the data from unauthorized access, distribution, use, modification, or disclosure. In accomplishing the review of internal controls, we also assessed the division’s compliance with certain provisions of the agreement related to database access and use, as well as the safeguarding and use of DAVID data and information.

Our review found the division’s internal controls were adequate to ensure the security and integrity of the data obtained from DAVID. However, we determined that internal controls could be strengthened in ensuring that access permissions for DAVID users are timely revoked. We recommended the Bureau enhance its administrative controls to ensure that DAVID access is removed within 5 working days.

Audits of employee use of the database conducted by the Office of Inspector General in May 2017 and by the bureau through their quarterly reviews identified no instances of improper use of the database. BLE further reported they had identified no instances of improper use within the past twelve months.

We also determined the division has established the policies, procedures, and practices necessary to help ensure compliance with MOU terms and conditions regarding database access and use, the safeguarding of information, and use of DAVID data and information.

INTRODUCTION AND BACKGROUND

On September 16, 2014, the Department of Business and Professional Regulation, Division of Alcoholic Beverages and Tobacco, Bureau of Law Enforcement, entered into an agreement with
the Department of Highway Safety and Motor Vehicles for the electronic exchange of driver license and motor vehicle data. Per the terms of the MOU (contract number HSMV-0362-15), DHSMV will provide DBPR with electronic access to DAVID at no cost for a period of three years.

DAVID affords authorized BLE employees access to extensive information. DAVID contains driver license, motor vehicle, and traffic crash information. DAVID may also provide access to driver history, driver information, vehicle co-owners, driver insurance, crash reports, make/model of vehicles, title information, vehicle lien holders, and information on previous vehicles.

Terms of the agreement obligate the division to protect and maintain the confidentiality and security of information obtained through the electronic data exchange in accordance with MOU provisions and applicable state and federal laws. Information obtained through DAVID can only be used for the purposes for which authorization was granted and can be disclosed to others only as authorized by state law.

Examples of misuse of DAVID might include checking a family member’s driving record; checking out photos of friends and relatives; looking up celebrities or politicians; and posting information in locations where it is exposed to the public. The DHSMV may terminate the agreement without notice for failure to comply with any of the requirements of the MOU and applicable law.

As of April 14, 2017, the Bureau of Law Enforcement had 128 users as follows:

<table>
<thead>
<tr>
<th>Status</th>
<th>Purpose</th>
<th>No. of Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Law enforcement and criminal justice purposes.</td>
<td>100</td>
</tr>
<tr>
<td>Inactive</td>
<td></td>
<td>28</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>128¹</td>
</tr>
</tbody>
</table>

AUDIT RESULTS

In general, we determined the division’s internal controls were adequate to protect the personal data obtained from the DAVID database from unauthorized access, distribution, use, modification, or disclosure. BLE uses the confidential and/or sensitive data and information found within DAVID to carry out their assigned duties and responsibilities. Accordingly, the bureau has established a broad framework of internal controls to help ensure the security and integrity of its information assets.

Our audit evaluated the sufficiency of internal controls over the security and integrity of information obtained through the data exchange and Bureau of Law Enforcement compliance with MOU provisions in the following three general areas:

- Database access and use (Access Controls)

¹ A total of 132 DAVID users existed as of April 14, 2017 with 100 users listed as Active and 32 users listed as Inactive. Four users were listed as both Inactive and Active on this report. Our office determined these users were currently Active, but due to inactivity had become Inactive during the course of the MOU. These users later appropriately accessed the DAVID system after appropriate training and should correctly be categorized as Active DAVID users.
Results of our review are discussed below.

**Access Controls**

The Bureau of Law Enforcement's controls over access to the DAVID system appear to be sufficient and functioning as intended.

The MOU provides that “[a]ccess to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.” BLE access to the DAVID system comes in the form of the self-registration option. Self-registration requires a DAVID user to submit relevant information and to agree to the relevant terms regarding information security. The agency point of contact will then approve the self-registrant, as necessary. DAVID users exist in one of two statuses – Active or Inactive.

Our office determined that as of April 14, 2017, 100 users were listed as “Active” and 28 users were listed as “Inactive.” Our office also determined that all users were appropriately registered by the authorized BLE point of contact.

**Finding 1 – Access Permissions Were Not Always Timely Revoked**

Per the MOU, user access permissions must be updated within five working days upon termination or reassignment of users and immediately upon discovery of negligent, improper, or unauthorized use or dissemination of information. We tested BLE’s compliance with this provision by comparing the DAVID removal date with the PeopleFirst listing of the dates of separation for these 28 inactive employees.

Our audit procedures disclosed users were not removed from DAVID as prescribed by the MOU. Specifically, we evaluated the efficiency of access removal for the 28 inactive employees as of April 24, 2017. We found that 9 of the 28 inactive users had DAVID access removed longer than 5 working days after their dates of separation.

BLE noted that these instances were either oversights or situations where notification of separation from AB&T administrative staff did not occur within the 5-day window. The division has now made modifications to this process and instituted additional administrative controls. BLE staff reported that access removal is now occurring timely and in accordance with the provision of the MOU.

The bureau is also required to conduct quarterly quality control reviews to ensure all current users are appropriately authorized. During the course of our audit, BLE staff provided our office with copies of these quarterly quality control reviews. As part of these reviews, BLE staff examines the listed users to determine whether only authorized users have been granted access. This process began on October 24, 2016, and covered the life of the Memorandum of Understanding. The bureau is therefore compliant with this MOU requirement.

**Recommendation** – We recommend that the Division consider enhancing its administrative controls to ensure that user access is revoked within 5 working days of employee separation.
Safeguarding of Information Controls

The Bureau of Law Enforcement’s controls over the safeguarding of DAVID information appear to be adequate and operating effectively.

The MOU specifies that the parties to the agreement shall access, use, and maintain the confidentiality of all information received under the agreement in accordance with Chapter 119, Florida Statutes, and the federal Driver’s Privacy Protection Act. The agreement requires that information exchanged by electronic means will be stored in a place physically secure from access by unauthorized persons and access will be protected in such a way that unauthorized persons cannot review or retrieve the information.

The division appears to maintain appropriate physical controls over its information assets. DAVID users within BLE generally conduct database searches and maintain DAVID data in computers located in secure facilities. Access to division facilities is controlled through the use of card key entry and visitors must be escorted while on-site.

DAVID users within the division also exercise appropriate safeguarding of the information derived through DAVID. When documentation from DAVID is obtained, it is kept in the physical hard copy of the investigative case file. Hard copies of information derived from DAVID are shredded upon case closure. Criminal intelligence information is not kept in the department's OnBase document management system.

BLE DAVID users are also governed by two specific policies addressing this information. Most directly relevant to the DAVID system is BLE Policy and Procedure Directive, 1.08, Records, approved on January 31, 2011. This policy applies to all BLE employees and outlines specific responsibilities and procedures for managing and retaining BLE records. The policy notes that the DAVID system will be subject to detailed monitoring and periodic audits to protect against improper or unauthorized use.

Authorized users will not retain DAVID records, except as required as part of an official report, nor provide them to any third party; and will store DAVID access certificates only on computers that are secured by password and physically secure from unauthorized users. Users must protect access to the information obtained and will utilize emergency contact information associated with the driver or vehicle record only to notify the contact persons in the event of an emergency.

In accordance with the policy, misuse of the DAVID system may result in disciplinary action up to and including dismissal and/or criminal prosecution. Violations must be reported to the Chief of Law Enforcement via the chain of command.

BLE Policy 5-2, Criminal Intelligence, with effective date of June 8, 2012, also establishes guidelines for the collection, analysis, and distribution of intelligence information. The policy notes that BLE staff may collect and maintain criminal intelligence information only if there is reasonable suspicion that an individual or organization is engaged in criminal conduct or activity and the information is relevant to that criminal conduct or activity. All bureau members assigned to an intelligence function shall receive appropriate training based on their position and experience.

---

2 18 United States Code, Chapter 123, Section 2721 et. seq.
Whenever criminal intelligence information or criminal investigative information is available to the bureau, only on a confidential or similarly restricted basis, BLE may obtain and use such information only in accordance with the conditions imposed by the providing agency.

This policy also discusses security of information contained within the intelligence files. Security is necessary to ensure the integrity of the intelligence process, the confidentiality of the information, and the protection of the individual’s or group’s right to privacy. Restrictions are in place to prevent unauthorized attempts to access, modify, remove, or destroy stored information. All information disseminated shall require that an information dissemination log be maintained. Intelligence files are also required to be appropriately secured.

As set forth in the MOU, all personnel with access to the information exchanged under the terms of the agreement will be instructed of, and acknowledge their understanding of, the confidential nature of the information and the criminal sanctions specified in state law for unauthorized use of the data. Acknowledgements must be maintained in a current status by the department.

Access to DAVID requires a user to acknowledge the Disclaimer on the DAVID Usage Warning Screen. The warning notes that “[a]ll data contained within the DAVID system is sensitive and privileged information and shall be handled accordingly. To maintain the integrity of this information, the records will be accorded proper management and security and will only be accessed and used by authorized personnel in accordance with state and federal law.”

The disclaimer also notes the protections against any unauthorized use and that accessing the system constitutes consent to system monitoring. A user must then check a box noting that “I have read and understand this agreement” and “I accept the above conditions on my use of DAVID.”

In addition, all users must take the mandatory Instructional Training and pass the exam prior to gaining access into the DAVID System. The Instructional Training and exam completion date is captured and stored; the training and exam are required on an annual basis in order for the user to maintain access to DAVID. These acknowledgement are automatically maintained electronically when the DAVID tutorial is completed by each user annually.

Our office performed testing on this information and determined that all active users had completed the Instructional Training and exam prior to use. This Training now serves to document that all personnel with access to the information within DAVID have acknowledged their understanding of the confidential nature of the information and maintained these acknowledgements in a current status.

**Usage Controls**

DHSMV provided a guide for agency Inspectors General to use in preparing the requested attestation. In accordance with this guide, in May 2017 we reviewed the DAVID usage of ten DAVID users, selected at random, for calendar year 2017. This period extended from January 1 through April 24, 2017. Documentation from BLE for each instance of database use showed that all access had been accomplished for a legitimate business purpose. The division also reported to us that they had not identified any instances of improper use within the past twelve months.

The department’s controls over use of DAVID appear to be sufficient and operating effectively. The MOU requires the department to monitor access to DAVID information on an on-going basis. DHSMV has developed an audit tool to assist agencies in complying with this
requirement. During the course of our review, the department established procedures to accomplish the required on-going monitoring.

On October 24, 2016, the bureau completed its first audit of DAVID use. For each quarter through the life of the MOU, the bureau’s Criminal Intelligence Analyst has randomly selected 20 DAVID users for review. BLE’s audit of these users’ transactions showed no instances of improper use of the database. The bureau’s procedures provide for quarterly audit of a random sample of DAVID users for transactions throughout the quarter.

**Other Matters**

MOU provisions require the bureau to use the DAVID information only for the purposes authorized by the agreement. The MOU states the bureau will use the personal information for “law enforcement and criminal justice purposes.” All AB&T usage was found to be permissible under the Driver’s Privacy Protection Act exception that allows for the use of the information by any government agency in carrying out its functions.

Our office also determined that in accordance with the agreement, the division has not assigned, subcontracted, or otherwise transferred its rights, duties, or obligations under the MOU.

**MANAGEMENT’S RESPONSE**

We provided a copy of our audit results for management review, and comments. The response from the Division of Alcoholic Beverages and Tobacco is attached.

**OBJECTIVES, SCOPE, AND METHODOLOGY**

**Objectives**

The overall purpose of this audit was to evaluate the effectiveness of the Division of Alcoholic Beverages and Tobacco’s management of the Memorandum of Understanding with the Department of Highway Safety and Motor Vehicles for use of the Driver and Vehicle Information Database (DAVID) system. Specifically, our office assessed the internal controls over the personal data obtained from the DAVID system and ensured that the internal controls are adequate to protect the personal data from unauthorized access, distribution, use, modification, or disclosure.

**Scope**

The scope of our audit included review of Department and Division of Alcoholic Beverages and Tobacco operations, records, and activities with respect to the DAVID system for the period of September 16, 2014 through May 17, 2017.

**Methodology**

This audit was conducted pursuant to Section 20.055, Florida Statutes, and in accordance with the *Principles and Standards for Offices of Inspector General*, as published by the Association of Inspectors General, and the *International Standards for the Professional Practice of Internal Auditing* published by the Institute of Internal Auditors, Inc. These standards 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 the findings and conclusions presented herein.

Audit procedures and tests for this audit included a review of relevant federal and state laws, including the federal Driver's Privacy Protection Act, and Chapters 119, 319, 320, and 322, Florida Statutes. We also reviewed the DAVID Audit Guide as provided in the DHSMV Audit Attestation Request letter of October 18, 2016 and the internal policies and procedures established by the department, the Division of Alcoholic Beverages and Tobacco, and the Bureau of Law Enforcement for use of the DAVID system.

We interviewed relevant staff within the Division of Alcoholic Beverages and Tobacco concerning policies, procedures, and practices for use of the DAVID system and the safeguarding and use of the personal information obtained through the data exchange.

We also carried out the following steps:

- Determined whether the required access had been granted for all DAVID users.
- Determined Division of Alcoholic Beverages and Tobacco compliance with the requirement that access permissions be updated within five working days upon termination or reassignment of users.
- Verified that the required acknowledgment forms and training completion dates were in current status.
- Assessed the adequacy and effectiveness of internal controls over the safeguarding of information obtained from the DAVID database, including review of physical controls; security controls; and department and Bureau of Law Enforcement information security policies, procedures, and practices.
- Evaluated and verified department compliance with various provisions of the MOU including conduct of quarterly quality control reviews and on-going monitoring of database use.
- Audited the database usage of a random sample of ten DAVID users for calendar year 2017 to determine whether any improper use had occurred.

**ACKNOWLEDGEMENTS**

We would like to thank the management and staff of the Division of Alcoholic Beverages and Tobacco for their cooperation and assistance during the course of this audit. We greatly appreciate the time and effort spent in compiling data and information for our review and analysis.
The mission of the Department of Business and Professional Regulation is to:
License efficiently. Regulate fairly.

The Office of Inspector General is established pursuant to Section 20.055, Florida Statutes, to provide a central point for the coordination of and responsibility for activities that promote accountability, integrity, and efficiency in government. The mission of the Office of Inspector General is to be a valuable partner in conducting independent, objective internal audits, reviews, and investigations of department activities and programs.

This review was conducted by Steven Henry, CIGA, CGAP, Senior Internal Auditor, under the supervision of Karen Barron, Director of Auditing.

This and other reports prepared by the Office of Inspector General of the Department of Business and Professional Regulation can be obtained by telephone (850-414-6700) or by mail (2601 Blair Stone Road, Tallahassee, FL 32399-1018).
TO: Lynne Winston, Inspector General  
Department of Business and Professional Regulation  

FROM: Thomas R. Philpot, Director  
Division of Alcoholic Beverages & Tobacco  

SUBJECT: Division Response to Findings in Report No. A-1617BPR-024  
Audit of Internal Controls for Driver and Vehicle Database (DAVID) Data Exchange  

DATE: May 8, 2017  

The Division of Alcoholic Beverages and Tobacco has received and reviewed Report No. A-1617-BPR-024, relating to the Audit of Internal Controls for the Driver and Vehicle Information Database (DAVID) Data Exchange. Based on the report, the Division understands that the audit determined that the Division's broad framework of internal controls were adequate to protect the personal data obtained from the DAVID database from unauthorized, distribution, use, modification, or disclosure in accordance with the Division's Memorandum of Understanding (MOU) with the Department of Highway Safety and Motor Vehicles (Contract Number HSMV-0362-15).

The report identified one finding and recommendation for enhancing the Division's administrative controls regarding user access to the database information. The Division's response to this finding is set forth below.

Finding 1: Access Permissions Were Not Always Timely Revoked

Recommendation: We recommend that the Division consider enhancing its administrative controls to ensure that user access is revoked within 5 working days of employee separation.

Division Response:

The MOU specifies revocation of user access to DAVID shall occur within five working days of employment separation or other action requiring cessation of access. In response to the finding, the Division has implemented the following specific controls to ensure consistent compliance with this access restriction:

1. Upon notification of the effective separation of a DAVID user from employment with the Division, the Division's human resources liaison will immediately notify the Division's DAVID system administrator.

2. Upon notification from the human resources liaison, the Division's DAVID system administrator will immediately revoke the employee's access to the DAVID system.

3. As a component of the quarterly audit process, the Division's DAVID system administrator will review and verify the system access records to ensure separated employees have been removed and that revocation of access was achieved timely in accordance with the MOU terms.

The Division welcomes the review of these processes to facilitate operational improvements and extends our appreciation for the professional manner in which the audit team completed this compliance assessment.

# # #

LICENSE EFFICIENTLY. REGULATE FAIRLY.  
WWW.MYFLORIDALICENSE.COM