Florida Department of Financial Services
Jeff Atwater
Chief Financial Officer

Office of Inspector General

Tom Kirwin
Inspector General

January 17, 2013 Internal Audit Number IA 12-205

Audit of the Department's Management of the Memorandum of Understanding for Use of the DAVID and DAVE Databases

EXECUTIVE SUMMARY

Numerous bureaus, offices, and groups (user entities) within the Department of Financial Services (Department or DFS) access driver license and motor vehicle information (driver information) under the terms of a Memorandum of Understanding (MOU or agreement) with the Florida Department of Highway Safety and Motor Vehicles (DHSMV). The MOU establishes specific requirements regarding the Department's use of, access to, and safeguarding of the driver information. Per the MOU's terms, the agreement is subject to unilateral cancellation without notice should the Department fail to comply with any of its requirements. We therefore undertook an evaluation of the Department's management of the agreement. Specific audit objectives were to:

- Evaluate the Department's compliance with the agreement's terms and provisions.
- Assess the adequacy of the Department's internal controls for safeguarding the driver information.
- Review the contracting procedures used to establish the agreement with DHSMV.

Compliance

The Department needs to improve compliance with certain of the MOU's requirements. For example, user access permissions were not always timely revoked upon the employee's separation from DFS and most user entities within the Department were not conducting the required quarterly quality control reviews or performing on-going monitoring of database use. Due to the number of user entities within the Department, and the complex nature of the agreement, we concluded that centralized management of the MOU would facilitate compliance with MOU provisions. We therefore recommend the Department place responsibility for managing the agreement within the Division of Information Systems.

Internal Controls

The DFS could improve internal controls related to access to, use of, and safeguarding of the data and information obtained under the agreement. For most user entities, we found limited written policies and procedures to guide staff in complying with MOU provisions. We recommend that the MOU's contract manager coordinate with user entities to establish written policies and procedures governing access to, use of, and security of the driver information.

Contracting

One user entity did not have statutory or other regulatory authority to access the driver information. Additionally, although the MOU involves the use of external information technology resources, current procedures do not clearly require and therefore, the Division of Information Systems did not review and approve the MOU to ensure such access would not expose the Department to any information security issues.

To address these contracting matters we recommend the Department improve procedures for establishing MOUs to ensure there is appropriate statutory authority for the data exchange, and further, that the Division of Information Systems review and approve all MOUs involving the exchange of data and information with external entities.[1]

ACKNOWLEDGEMENTS

We are grateful for the cooperation, assistance and input provided to us by the management and staff of the entities that use the DAVID and DAVE databases during the course of their work. We appreciate the time spent with us in interviews and observations, and the timely responses to our many requests for supporting documentation. We also appreciate the assistance and support of management and staff within the Division of Administration and Division of Information Systems.

[1] The MOU refers to DHSMV's provision of driver information as an electronic data exchange.

INTRODUCTION AND BACKGROUND

On December 1, 2011, the Department of Financial Services renewed a Memorandum of Understanding with the Department of Highway Safety and Motor Vehicles for access to DHSMV's DAVID and DAVE databases (Contract No. HSMV-0380-12). Per the terms of the 2011 MOU, DHSMV will provide DFS electronic access to these databases at no cost for a three-year term.

The **D**river **A**nd **V**ehicle **I**dentification **D**atabase, or DAVID, contains extensive information on Florida drivers, including their driver license number and personal identifying information, such as social security number, home address and telephone number. In addition to drivers' photographs and signatures, DAVID provides the current license plate number for each vehicle the driver owns, driver history information (including driving violations), insurance information, data on previously owned vehicles and emergency contact information.

DHSMV provides access to DAVID through the Florida Criminal Justice Network (CJNet) maintained by the Florida Department of Law Enforcement (FDLE). CJNet is a secure, statewide information and data-sharing network established for use by the state's criminal justice agencies. The FDLE controls access to CJNet and the DAVID database through a digital certificate authentication system. Access to DAVID is limited to criminal justice agencies.

The **D**river **A**nd **V**ehicle **E**xpress, or DAVE database is a web-based version of DAVID which the DHSMV makes available to non-criminal justice agencies through two Internet portals, mDAVE and iDAVE. The mDAVE portal is preferred for state agencies as it provides more secure access and permits agency mDAVE administrators to grant and revoke user access for agency staff and to monitor database use. Most DAVE users within DFS have access to driver license and motor vehicle information, only. However, DAVE users within DFS' Bureau of Unclaimed Property also have access to driver photographs and signatures pursuant to statutory authority.

Information obtained through the DAVID and DAVE databases can only be used for the purposes for which authorization was granted in the MOU with DHSMV, and can be disclosed to others only as authorized by state law. Unauthorized use of the databases includes queries not related to a legitimate law enforcement or business purpose, personal use, improper dissemination to non-law enforcement personnel, and sharing, copying or distributing information to unauthorized users. Personal data and information associated with a driver or motor vehicle record are protected under both federal and state law.[2] Unauthorized access, use, or disclosure of DAVID or DAVE data may result in penalties and civil lawsuits, and may be a violation of criminal law.

[2] The MOU states that personal information found in the motor vehicle or driver record includes, but is not limited to, the subject's driver identification number, name, address, telephone number, and medical or disability information. Personal information does not include information related to vehicular crashes, driving violations, and driver's status.

Exhibit 1 identifies each DFS user entity, the entity's primary purpose for using the driver information, and the number of database users within the entity as of July 2012.

Exhibit 1
DFS User Entities as of July 2012

DFS User Entity	Primary Purpose for Database Access	Number of DAVID Users (as of July 2012)	Number of DAVE Users (as of July 2012)
1. Division of Insurance Fraud	Investigations (Criminal justice agencies)	147	
2. Division of State Fire Marshal, Bureau of Fire and Arson Investigations		88	
3. Division of Accounting and Auditing, Office of Fiscal Integrity		2	
4. Division of Public Assistance Fraud		54	
5. Division of Insurance Agents and Agency Services, Bureau of Investigations	Investigations (Non-criminal justice agencies)	Terminated [a]	
6a. Division of Workers' Compensation, Bureau of Compliance			13
6b. Division of Workers' Compensation, Bureau of Compliance	Regulatory Functions Verify exemption application information		30
7. Division of Accounting and Auditing, Bureau of Unclaimed Property, Accounts Payable Section	Verify applicant identity		32
8. Division of Administration, Bureau of Human Resource Management	Check Staff Driver License Status/ Moving Violations		3
9. Division of Rehabilitation and Liquidation, Administrative Services Section			2
10. Division of Administration, Bureau of General Services, Facilities and Property Management Office	Parking Enforcement		3
Total		291	83

Source: Data and information compiled by the Office of Inspector General.
(a) Access for Division of Insurance Agents and Agency Services was terminated effective June 21, 2012.

ISSUES

Issue 1: Centralizing management of the MOU would facilitate a more systematic and coordinated approach for managing the agreement with DHSMV. When DFS renewed its agreement with DHSMV in 2011, some user entities were not included in the contracting process and were therefore unaware of the MOU's provisions. A staff person within the Division of Insurance Fraud (DIF) serves as the Department's contract manager for the agreement with DHSMV. However, the Division Director reported that it is difficult for this person to monitor database use and ensure contract compliance across DFS divisions.

For example, the DIF contract manager did not have a complete list of DFS user entities. We therefore surveyed the Department's divisions to identify all user entities, the purposes for which the entities access the databases and the number of database users within each entity. Survey

results showed that when DFS renewed the MOU in 2011, the directors of three divisions with database access were not included in the contracting process. The Department's internal contracting documents also failed to identify all user entities within each of the divisions named in the documents. We further learned that one of the named divisions had also executed a separate, duplicative agreement with DHSMV for the exchange of driver information.[3]

Good contracting practices and sound internal controls dictate that all department entities responsible for complying with contract provisions participate in the contracting process. All parties to the agreement should review the agreement and sign the Department's internal contracting documents. Many of the staff we interviewed did not have a copy of the MOU and were unaware of various MOU provisions. At their request, we provided copies of the agreement for review by managers within five of the eleven user entities.

Due to the number of DFS user entities with access to DAVID and DAVE, and the extensive MOU provisions regarding database access and data security, we determined the Department should centralize management of the MOU. After discussion with the Chief Information Officer and Division of Information Systems management, we concluded the Department should place responsibility for managing the MOU with the Division of Information System's Criminal Justice Information (CJI) Compliance Coordinator. The CJI Compliance Coordinator is part of the Division of Information System's Information Security Office and as such, has department-wide responsibilities related to access and security of criminal justice information used by Department entities. Division of Information Systems management agreed that managing the MOU is an appropriate Division function. The Director of the Division of Insurance Fraud subsequently recommended placing responsibility for managing the MOU within the Division of Information Systems, as well.

Issue 2: Centralizing management of the MOU would assist the Department in improving compliance with MOU provisions. The MOU is subject to unilateral cancellation without notice for failure to comply with any of its requirements. In signing the MOU, the Department agreed to comply with numerous provisions regarding the appropriate use and safeguarding of DAVID and DAVE driver information. The MOU is also contingent upon the Department having appropriate internal controls over the personal data obtained from the databases. Per the MOU, these internal controls must protect the personal data from unauthorized access, distribution, use, modification, or disclosure. Areas requiring improvement are discussed below.

> **User access permissions were not always timely updated.** The MOU requires DFS to update employees' access permissions within five working days upon termination or reassignment of staff, and immediately upon discovery of

[3] During the course of our fieldwork, Department executive management determined the Division of State Fire Marshal should not renew its separate agreement with DHSMV. The Division of State Fire Marshal was included as a user entity when the Department renewed its MOU with DHSMV in 2011. Maintaining separate MOUs would be overly burdensome as the agreement requires the DFS Inspector General to provide an attestation at DHSMV's request as to the sufficiency and effectiveness of internal controls over the security of data accessed under the MOU's terms.

negligent, improper, or unauthorized use and dissemination. However, the Department's user entities were not always timely revoking access.

We obtained a list of employees with approved access to DAVID and/or DAVE from each of DFS' user entities. We then compared these lists with a list of current DFS employees. We identified 8 employees within 4 different user entities who appeared to have separated from the Department. Upon our inquiry, the responsible entities determined these users had separated from the Department and revoked their access, accordingly. However, access for these users had remained active from 9 to 419 days in excess of the MOU's allowed timeframe.

Timely revocation of user access is essential. The Department's Information Security Officer reported that should a separated employee with DAVE access move to another state agency with Internet service, the employee's DAVE user name and password would provide that person access to the database. Similarly, if a separated employee with DAVID access moved to another entity with DAVID access, that employee's digital certificate would still grant them access to DAVID.

Not all user entities have written policies and procedures regarding appropriate authorization for use or timely revocation of users' access to the DAVID and DAVE databases. Each user entity with DAVID access has a Digital Certificate Coordinator (DCC) responsible for administering DAVID access for new users within that entity. Similarly, each entity with DAVE access has a Point of Contact (POC) for administering user access to DAVE. In accordance with the Department's Administrative Policy and Procedure 4-05, the Department should establish guidelines to ensure that DCC's and POC's receive formal written supervisory approval for new users to access the databases. The guidelines should also ensure that the DCC or POC receives timely notification of the user's separation or reassignment. The procedures should also address MOU requirements regarding immediate revocation in instances where an employee has made inappropriate access or use of database information.

Quarterly quality control reviews were not performed by all entities. The MOU requires the Department to conduct quarterly quality control reviews to ensure all current users are appropriately authorized. As of the start of our fieldwork, only two of the Department's user entities had conducted such reviews. The Office of Fiscal Integrity had also established written procedures for conducting the quarterly quality control review.

We obtained a list of the Department's DAVID users from FDLE to verify the accuracy of the lists provided by Department entities. This comparison showed that 7 employees within 3 user entities had duplicate digital certificates. Upon our inquiry, the responsible DCC's revoked the second digital certificate for these employees. To help verify the accuracy of the listings of DAVE users provided

by Department entities, we requested from the DHSMV, but were not provided, a current listing of DAVE users.

The use of quality control reviews is standard practice for ensuring that current users have appropriate authorization to access a particular database. The Department's Administrative Policy and Procedure No. 4-05 requires business units to conduct application access reviews quarterly to ensure that the access privileges of users are consistent with the roles and responsibilities the user needs to perform assigned duties, and that the access privileges of separated users have been removed within established timeframes.

In July 2012, DHSMV published guidelines for DAVID DCC's to use in conducting quarterly quality control reviews.[4] However, the guidelines do not address quarterly quality control reviews for DAVE users. The Department therefore needs to coordinate with the DAVE POC's to establish written policies and procedures for conducting quarterly quality control reviews of DAVE users.

The Department should improve policies and procedures related to the security of the personal data and information obtained from the databases. The MOU provides that information obtained from the databases shall not be retained unless it is for a law enforcement purpose. The agreement also provides that the data will be stored in a place that is physically secure from access by unauthorized persons, and that access to the information will be protected such that unauthorized persons cannot review or retrieve the information.

We determined the criminal justice agency entities (Division of Insurance Fraud; State Fire Marshal, Bureau of Fire and Arson Investigations; Division of Public Assistance Fraud; and Office of Fiscal Integrity) retained DAVID information for law enforcement purposes. These entities retained information in hard copy format in locked file cabinets and/or locked offices in areas that were physically secured and inaccessible to unauthorized persons. Upon case closure, these entities' reported practice is to shred any information in the case file that was obtained from DAVID. The Office of Fiscal Integrity has written procedures to ensure appropriate security of DAVID information within that office.

Two of the criminal justice agency entities enter data obtained from DAVID into their case management systems. These entities did not have written procedures to ensure that only authorized personnel could view the DAVID data entered into these systems, or procedures regarding its retention. Written Department policies and procedures governing the security of DAVID data retained for law enforcement purposes would help ensure the data remain protected from unauthorized use or disclosure.

[4] During the course of our fieldwork, we identified the guidelines on DHSMV's web site. We then surveyed the Department's DCC's and determined that as of September 12, 2012, DHSMV had not notified the MOU's contract manager or Department DCC's that the guidelines were available for their use.

Excluding the Facilities and Property Management Office, the entities with DAVE access (Bureau of Human Resource Management; Division of Workers' Compensation, Bureau of Compliance; Division of Rehabilitation and Liquidation, Administrative Services Section; and Bureau of Unclaimed Property) also retained personal data and information. With the exception of one user entity, the data were retained in hard copy format in locked file cabinets and/or locked offices in areas that were physically secured and inaccessible to unauthorized persons.

Our observation of operations in one user entity showed that hard copy files containing DAVE information were not appropriately secured until after work with the file was completed. The file was then stored in a secure file room. In the interim, the files were left on employees' desks in an unsecured work area. This entity also scanned the personal data into its management information system. During the course of our review, management required all staff with access to this information system to sign forms acknowledging the confidential nature of the DAVE information and their understanding of the consequences for its misuse. We also determined that another user entity retained DAVE data in electronic case files that were accessible to staff members who did not have a legitimate business need for the driver information. To address such issues, the Department needs to establish written policies and procedures for ensuring the security of DAVID and DAVE data retained in both hard copy and electronic format.

Acknowledgement forms were not maintained in current status. Per the MOU, all personnel with access to the information exchanged under the terms of the agreement must be instructed of and acknowledge their understanding of the confidential nature of the database information. All personnel must also 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." The MOU requires acknowledgements of all personnel with access to DAVID and DAVE information; however, DHSMV representatives informed us that only the employees who actually access the databases need to sign an acknowledgement form.

We determined that 7 of the 10 user entities required users to sign an acknowledgement form, but only once, when the employee initially received database access. Although not stated in the MOU, DHSMV representatives informed us that DAVID and DAVE users should sign acknowledgement forms quarterly. To meet the MOU requirement, one Bureau manager suggested that Department users sign a new acknowledgement form annually, at the time of the employee's performance evaluation. As noted by a number of managers and staff, both DAVID and DAVE have warning screens that users must accept prior to accessing the databases. The screens advise users of the confidential nature of the data contained therein, and of the possibility of criminal sanctions for its misuse. To address the MOU's requirements in this area, the Department needs

to establish written policies and procedures regarding staff instruction, and initial and periodic completion of acknowledgement forms.

All entities did not monitor database use on an on-going basis. The agreement with DHSMV requires the Department to monitor all access to the databases on an on-going basis. However, DHSMV did not enforce compliance with this provision until after it released an audit tool for agencies to use in monitoring user access. DHSMV's audit tool permits agency DCC's and POC's to run a report of the searches a user has conducted during a specified timeframe.[5] In this way, a supervisor can determine if the data accessed was for an authorized business purpose. For example, a supervisor could determine if a user had viewed information on driving violations. While some entities have a legitimate business need for this information, Bureau of Unclaimed Property staff, for example, would not need information on moving violations to verify the identity of a claimant for unclaimed property.

DHSMV released a monitoring or audit tool in October 2011; however, DHSMV did not notify the Department's contract manager or DCC's and POC's of its availability. As of the start of our fieldwork in March 2012, only the Office of Fiscal Integrity was routinely monitoring user access.[6] The Office of Fiscal Integrity had also established written procedures to accomplish the required monitoring. These procedures include a requirement for supervisory review of monitoring results.

By July 2012, an additional four user entities had begun monitoring user access. Many of the DCC's and POC's reported difficulties using DHSMV's audit tool. When users access either DAVID or DAVE, they must select a reason for the search from a drop-down menu (such as criminal investigation, parking enforcement, etc.). However, the databases do not include a field for the user to enter an identifying case or claim number. Therefore, the audit report does not tie database activity to a specific investigation, claim or other identifier. To determine if a user's activity was for a legitimate business purpose, the reviewer must first correlate the information in the audit report with information maintained in an internal document or database.

[5] The audit tool permits DCC's and POC's to run monitoring reports only for those users for whom the DCC or POC has granted database access. Consequently, DCC's/POC's cannot monitor database use of staff employed by other user entities within the Department.

[6] In 2009, DHSMV established mDave, which provides Internet access to DHSMV's driver license and motor vehicle database. Prior to mDAVE, agencies accessed DAVE through a mainframe connection. We determined the Bureau of Human Resource Management was still using the mainframe access to DHSMV's database and had not been informed of the need to obtain mDAVE access. Mainframe access does not permit use of the audit tool. During the course of our review, the Bureau of Human Resource Management received mDAVE access. We further determined the Division of Rehabilitation and Liquidation had iDAVE access rather than mDAVE access. Because the audit tool cannot be used in iDAVE, DHSMV advised that the Division of Rehabilitation and Liquidation should seek mDAVE access.

For example, the Office of Fiscal Integrity maintains a log of each DAVID search, the name of the subject associated with the search and the purpose for the search. When monitoring database use, the reviewer verifies that the DAVID records reviewed were of subjects named in the activity log and that the named subjects were associated with an active investigation. Maintaining a log of search activity may not be realistic for field investigators in other DFS user entities or for entities that perform numerous searches each day. Because other state agencies have encountered similar difficulties using the audit tool, DHSMV is reportedly seeking a technical solution to the problem. In the interim, the Department needs to identify practical solutions for all DFS user entities to use in meeting the requirement for on-going monitoring.

The Department should establish policies and procedures regarding misuse of DAVID or DAVE information. The MOU requires the Department to notify the DHSMV and the affected individual immediately following the determination that personal information has been compromised by any unauthorized access, distribution, use, modification, or disclosure. The statement to DHSMV must contain specific information about the security breach including corrective actions and the date the actions were completed.

While we found no instances of non-compliance with these provisions, Department policies and procedures were not sufficient to ensure that misuse of the databases, or of database information are appropriately reported to DHSMV and that management takes corrective action. The procedures should also provide for reporting such incidents to the Department's Computer Security Incident Response Team (CSIRT) and Office of Inspector General in accordance with the Department's Administrative Policies and Procedures.

The Department should establish protocols for accomplishing the required annual audit and affirmation. The agreement requires the Department to complete an annual audit to ensure proper and authorized use and dissemination of data. The MOU does not define audit requirements. In July 2012, DHSMV provided an audit guide for DCC's and POC's to use in performing the required annual audit.[7] However, the guide addresses agency compliance, not user entity compliance. For example, the audit guide asks whether the agency has conducted quarterly quality control reviews and requires the preparer to audit the use of the databases for ten users, selected at random, for a randomly selected week. The audit serves as the basis for the Department's annual affirmation. Per the MOU, the Department will provide DHSMV with an annual affirmation indicating compliance with the requirements of the agreement no later than 45 days after the anniversary date of the agreement.[8]

[7] During the course of our fieldwork, we identified the audit guide on DHSMV's website. We determined that as of September 12, 2012, DHSMV had not notified the Department's contract manager or the DCC's and POC's that an audit guide was available for use in meeting the MOU's audit requirement.
[8] The current MOU was executed on December 1, 2011.

Centralizing management of the MOU within the Division of Information Systems would facilitate a more systematic and coordinated approach for managing the agreement and ensuring compliance with the MOU's provisions. We reviewed each user entity's internal policies and procedures for database access and use. Our review showed that the Office of Fiscal Integrity had established comprehensive written policies and procedures governing database access and data security. However, most user entities had limited, if any written policies and procedures to help ensure compliance with MOU provisions. Written policies and procedures also document the Department's internal controls for safeguarding the data. To address this issue, the MOU's contract manager could coordinate with DFS' user entities to establish a set of overarching policies, procedures and/or guidelines governing compliance with the MOU.

Issue 3: The Department could improve its procedures for establishing MOUs with external entities for the electronic exchange of data and information. One entity did not have authority to access DAVID. Further, current procedures do not clearly require and therefore, the Division of Information Systems did not review the MOU to ensure that any information technology security issues were appropriately addressed.

Access Issues. Access to DAVID is restricted for use by criminal justice agencies. We therefore reviewed the statutory basis for each entity's DAVID access. State law does not specifically designate the Division of Public Assistance Fraud (PAF) as a criminal justice agency. However, section 943.045(10)(e), Florida Statutes, provides that "'Criminal justice agency' means: Any other governmental agency or subunit thereof which performs the administration of criminal justice pursuant to a statute or rule of court and which allocates a substantial part of its annual budget to the administration of criminal justice." PAF requested and satisfied the Federal Bureau of Investigation's requirements for designation as a criminal justice agency and consequently received such designation from FDLE. Upon receipt of designation as a criminal justice agency, PAF was then authorized to access DAVID.

Pursuant to state law, the Division of Insurance Agents and Agency Services is not a designated criminal justice agency. After we discussed the Division's legal status with the FDLE Criminal Justice Information Security Manager, FDLE revoked the Division's access to DAVID as of June 21, 2012. We then provided the Division with information about applying for criminal justice agency status, and as of this writing, the Division is pursuing such designation. We concluded the Department could improve its contracting procedures for ensuring that appropriate statutory authority exists prior to executing MOUs for the exchange of data and information with external sources.

Contract Review Procedures. Department policies and procedures do not clearly require the Division of Information Systems to review and approve MOUs for the exchange of electronic data. Including the Division of Information Systems in the process for establishing such MOUs would assist the Division of Information Systems in maintaining an accurate and up-to-date inventory of the Department's data and information. Such review would also help identify the existence of any potential information technology security risks associated with the data

exchange prior to executing the agreement.[9] During the course of our review, we identified a security issue related to DAVID access. We discussed this issue with the Department's Chief Information Officer and Information Security Manager and steps to remediate the issue were undertaken.

RECOMMENDATIONS

We recommend that:

1. The Department designate the Division of Information System's CJI Compliance Coordinator as the contract manager for the MOU.

2. The MOU's contract manager coordinate with the Department's user entities to develop a set of overarching written policies and procedures to help ensure compliance with MOU provisions and strengthen internal controls regarding:

    a. User access approval and revocation.
    b. Performance of quarterly quality control reviews.
    c. The security of DAVID and DAVE data retained in both hard copy and electronic format.
    d. Maintenance of acknowledgement forms in current status.
    e. On-going monitoring of database use.
    f. Misuse of database information.
    g. Completion of the required annual audits and Department affirmation.

3. The Department improve its procedures for establishing MOUs for the electronic exchange of data and information to:

    a. Ensure entities have a statutory basis for such exchange of data and information with external sources.

    b. Require the Division of Information Systems to review and approve MOUs involving the exchange of data and information with external entities.

[9] Section 282.318, Florida Statutes, requires each agency to have a security program for its data and information technology resources and appropriate cost-effective safeguards to address identified risks to the data, information, and information technology resources of the agency.

MANAGEMENT'S RESPONSE

Department management concurred with all recommendations and management's response to the audit is attached hereto as Appendix A. The Office of Inspector General agrees with the response.

OBJECTIVES, SCOPE AND METHODOLOGY

Objectives

The overall objective of this audit was to evaluate the effectiveness of the Department's management of the Memorandum of Understanding with the Department of Highway Safety and Motor Vehicles for use of the DAVID and DAVE databases. Our specific objectives were to determine whether the Department and its user entities were in compliance with MOU terms and provisions, and to assess the adequacy of the Department's internal controls for safeguarding the security of the driver information. We also reviewed the contracting procedures used to establish the agreement with DHSMV.

Scope

We evaluated the operations of DFS entities with access to the DAVID and DAVE databases during the period from March 9, 2012 to September 12, 2012. We also evaluated documentation from earlier periods, as necessary. Although the Office of Inspector General was a user entity for a portion of the audit period, in accordance with internal auditing standards, we did not include the Office of Inspector General within the scope of this review. We also limited our fieldwork interviews and observations to user entity locations within the Tallahassee area. Because compliance issues were apparent within the Department's central offices, we did not extend our review to include on-site fieldwork within user entities' field offices. During the period of our review, the Division of Information Systems established the Criminal Justice Information Services Compliance Work Group. The purpose of this Work Group is to evaluate the Department's compliance with Federal Bureau of Investigations and Florida Department of Law Enforcement requirements regarding access to, use of, and security of criminal justice information. To avoid duplication of effort, we did not evaluate issues under review by the Work Group.

Methodology

To accomplish our objectives, we reviewed the 2008 and 2011 Memorandums of Understanding established between DFS and DHSMV, and the 2009 Memorandum of Understanding established between the Division of State Fire Marshal, Bureau of Fire and Arson Investigation and DHSMV. We reviewed relevant state laws and rules; internal policies and procedures established by user entities for use of the DAVID and DAVE databases; DFS Administrative

Policies and Procedures; and Department contracting documents and guidelines. We also reviewed the Criminal Justice Information Services (CJIS) Security Policy, Version 5.1 published by the Federal Bureau of Investigation; FDLE's Criminal Justice Information Services (CJIS) Certification Training Manual and Digital Certificate Coordinator for DAVID manual; and other related documents.

We interviewed relevant staff within the DHSMV and the FDLE. Within DFS, we interviewed the Chief of the Bureau of General Services and the DFS Purchasing Director. We also interviewed management and staff within the Division of Information Services. We conducted interviews with management within the DFS entities that access the DAVID and/or DAVE databases and observed operations within selected user entities. We also interviewed, and obtained supporting documentation from each of the Department's DAVID Digital Certificate Coordinators and DAVE Points of Contact.

We conducted a department-wide survey to identify entities within the Department with access to the DAVID and/or DAVE databases. Among other steps, we evaluated users' employment status with the Department, their completion of required acknowledgement forms, the status of users' digital certificates, and we observed and assessed the security of data obtained through the electronic data exchange.

DISTRIBUTION LIST

Jeff Atwater, Chief Financial Officer
Robert C. Kneip, Chief of Staff
Terry Kester, Director, Division of Information Systems
David W. Martin, Auditor General

To promote accountability, integrity, and efficiency in state government, the Office of Inspector General completes audits and reviews of Department of Financial Services programs, activities, and functions.

Pursuant to section 20.055, Florida Statutes, this audit was conducted in accordance with applicable standards contained in the *International Standards for the Professional Practice of Internal Auditing*, published by the Institute of Internal Auditors, Inc., and *Principles and Standards for Offices of Inspectors General* published by the Association of Inspectors General. This audit was conducted by Tonya Pryor, Certified Internal Auditor, under the supervision of Sandra Lipner, Director of Auditing.

Please address inquiries regarding this report to the DFS Office of Inspector General at 850-413-3112.

APPENDIX A

CHIEF FINANCIAL OFFICER
JEFF ATWATER
STATE OF FLORIDA

January 15, 2013

Mr. Tom Kirwin
Interim Inspector General
200 E. Gaines Street
Tallahassee, Florida 32399

Dear Mr. Kirwin:

Pursuant to Section 20.55(5)(d), Florida Statutes, the enclosed response is provided for the preliminary and tentative audit findings included in the Inspector General's operational audit of the *Department's Management of the Memorandum of Understanding for Use of the DAVID and DAVE Databases.*

If you have any questions concerning this response, please contact Terry Kester, Chief Information Officer, at (850) 413-1505.

Sincerely,

Robert Kneip
Chief of Staff

RK:aln

Enclosure

FLORIDA DEPARTMENT OF FINANCIAL SERVICES
Robert Kneip, Chief of Staff
200 East Gaines Street • Tallahassee, Florida 32399 • Tel. 850-413-4900 • Fax 850-413-2985
Robert.Kneip@myfloridacfo.com
AFFIRMATIVE ACTION • EQUAL OPPORTUNITY EMPLOYER

Department of Financial Services
Audit of the Department's Management of the Memorandum of Understanding for Use of the DAVID and DAVE Databases
Office of Inspector General Audit

Issue	Section	Issue Description	OIG's Recommendation	Management's Response
1	All	**Centralizing management of the MOU would facilitate a more systematic and coordinated approach for managing the agreement with DHSMV.**	The Department should centralize management of the MOU. The Department should designate the Division of Information System's CJI Compliance Coordinator as the contract manager for the MOU.	The Division of Information System's CJI Compliance Officer has been designated to manage the MOU.
2	All	**Centralizing management of the MOU would assist the Department in improving compliance with MOU provisions.**	The MOU's contract manager could coordinate with DFS' user entities to establish a set of overarching policies, procedures and/or guidelines governing compliance with the MOU.	The Division of Information System's CJI Compliance Officer will coordinate with the Department user entities to establish documented guidelines and train applicable staff on related responsibilities to ensure compliance with the requirements defined in the MOU.
	1	User Access permissions were not always timely updated.	The Department should establish guidelines to ensure that DCC's and POC's receive formal written supervisory approval for new users to access the databases. The guidelines should also ensure that the DCC or POC receives timely notification of the user's separation or reassignment. The procedures should also address MOU requirements regarding immediate revocation in instances where an employee has made inappropriate access or use of database information.	
	2	Quarterly quality control reviews were not performed by all entities.	The Department therefore needs to coordinate with the DAVE POC's to establish written policies and procedures for conducting quarterly quality control reviews of DAVE users.	
	3	The Department should improve policies and procedures related to the security of the personal data and information obtained from the databases.	The Department needs to establish written policies and procedures for ensuring the security of DAVID and DAVE data retained in both hard copy and electronic format.	
	4	Acknowledgement forms were not maintained in current status.	The Department needs to establish written policies and procedures regarding staff instruction, and initial and periodic completion of acknowledgement forms.	
	5	All entities did not monitor database use on an on-going basis.	The Department needs to identify practical solutions for all DFS user entities to use in meeting the requirement for on-going monitoring.	
	6	The Department should establish policies and procedures regarding misuse of DAVID or DAVE information.	The Department should establish policies and procedures regarding misuse of DAVID or DAVE information. The procedures should also provide for reporting such incidents to the Department's Computer Security Incident Response Team (CSIRT) and Office of Inspector General in accordance with the Department's Administrative Policies and Procedures.	
	7	The Department should establish protocols for accomplishing the required annual audit and affirmation.	The Department should establish protocols for accomplishing the required annual audit and affirmation within 45 days after the anniversary date of the agreement.	

3	All	**The Department could improve its procedures for establishing MOUs with external entities for the electronic exchange of data and information.**	The Department could improve its procedures for establishing MOUs with external entities for the electronic exchange of data and information.	The Department MOU process was revised to include Division of Information System review and approval of related MOUs. Additionally, the Division of Information Systems will ensure that this review includes evaluation of statutory basis for the entity establishing an exchange of data and information with the external source.
	1	One entity did not have authority to access DAVID.	The Department could improve its contracting procedures for ensuring that appropriate statutory authority exists prior to executing MOUs for the exchange of data and information with external sources.	
	2	Current procedures do not clearly require and therefore, the Division of Information Systems did not review the MOU to ensure that any information technology security issues were appropriately addressed.	The Department should require the Division of Information Systems to review and approve MOUs involving the exchange of data and information with external entities.	