June 6, 2013 Internal Audit Report IA 13-203 Thomas F. Kirwin

Audit of Internal Controls Over Personal Data Exchanged Under DHSMV Memorandum of Understanding and Audit Follow-up of IA 12-205

EXECUTIVE SUMMARY

Numerous sections (user entities) within the Department of Financial Services (Department) access driver license and motor vehicle information under the terms of a Memorandum of Understanding (MOU) with the Florida Department of Highway Safety and Motor Vehicles (DHSMV). The MOU requires the Department to submit, upon request by DHSMV, an attestation indicating whether the internal controls over the personal data exchanged under the MOU are adequate to protect the personal data from unauthorized access, distribution, use, modification or disclosure. The objectives of this audit were to evaluate the adequacy and effectiveness of internal controls for these areas and included a follow-up on the audit findings included in our prior report IA 12-205 (Internal Audit of the Department's Memorandum of Understanding for Use of the DAVID ad DAVE Databases).

Findings:

Generally, internal controls were adequate to protect the personal data from unauthorized access, distribution, use, modification or disclosure. However, we determined that, in some areas, internal controls need to be strengthened. We found, as follows:

- Access permissions for five DAVID database users were not timely revoked.
- The frequency and performance of Quarterly Quality Control access reviews needs improvement.
- Four user entities retained personal information from DAVE absent written authorization from DHSMV.
- Access authorization and acknowledgement forms were not maintained for all users of the databases.
- Procedures over the performance of the semi-annual misuse audits need improvement.
- Security incident procedures were not sufficient to meet the unique misuse reporting requirements of the MOU.
- Department contracting policies and procedures are not sufficient to ensure a proper evaluation of legal authority for data exchange agreements.
- A security issue involving the DAVID database needs remediation.

Recommendations:

- The Department enhance its DAVE and DAVID Access Control Procedures related to user access criteria and revocations, monitoring activities (e.g., QQC reviews and semi-annual audits), and maintenance of records.
- The Department provide training and/or guidance related to the performance of MOU monitoring activities (e.g., QQC reviews, semi-annual misuse audits).
- The Division of Information Systems (DIS) continue its effort to revise its Computer Security Incident Reporting Team (CSIRT) procedures.
- The Department revise its contracting procedures to ensure a proper review of statutory authority for data exchange agreements.

ACKNOWLEDGEMENTS

The Office of Inspector General would like to thank the management and staff of the various Department user entities, the Division of Administration and Division of Information Systems for their input, cooperation and assistance throughout the performance of this audit. We appreciate the time spent gathering and providing documentation, participating in interviews and responding to our many inquiries. We also appreciate the courtesy extended to us by the Orlando and Tampa field offices during our observations of security practices. We acknowledge the considerable efforts and commitment of the Division of Information Systems in implementing comprehensive procedures related to the DAVE and DAVID databases in a short time frame. Additionally, we commend the Division of Public Assistance Fraud for the excellence of its misuse audit procedures.

INTRODUCTION AND BACKGROUND

On December 1, 2011, the Department renewed its MOU[1] with the DHSMV for access to DHSMV's DAVID and DAVE databases. Per the terms of the MOU, DHSMV will provide the Department electronic access to these databases at no cost for a three-year term.

The DHSMV provides access to the Driver And Vehicle Information Database , or DAVID database, through the Florida Criminal Justice Network (CJNet) maintained by the Florida Department of Law Enforcement (FDLE). The 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. A user entity with access to DAVID must designate a "Digital Certificate Coordinator" (DCC), who is responsible for administering access to the DAVID database on behalf of the user entity.

The Driver And Vehicle Express, or DAVE database, is a web-based version of DAVID which the DHSMV makes available to non-criminal justice agencies. The DHSMV controls access to DAVE through assigned user names and passwords. A user entity with access to DAVE must designate a "Point of Contact" (POC), who is responsible for administering access to the DAVE database on behalf of the user entity.

The databases contain extensive information on Florida drivers, including their driver license number, social security number, home address and telephone number. In addition, the databases provide 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. The DAVID database also provides access to a driver's photograph and signature, which are generally not available to users with access to the DAVE database.

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. 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.

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 February 2013.

[1] HSMV-0380-12.

[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
DFS User Entities as of February 2013

DFS User Entity	Primary Purpose for Database Access	No. DAVID Users (as of Feb. 2013)	No. DAVE Users (as of Feb. 2013)
1. Division of Insurance Fraud	Investigations (Criminal justice agencies)	152	
2. Division of State Fire Marshal, Bureau of Fire and Arson Investigations		81	
3. Division of Accounting and Auditing, Office of Fiscal Integrity		2	
4. Division of Public Assistance Fraud		54	
5.a. Division of Workers' Compensation, Bureau of Compliance	Investigations (Non-criminal justice agencies)		12
5.b. Division of Workers' Compensation, Bureau of Compliance	Regulatory Function		31
6. Division of Accounting and Auditing, Bureau of Unclaimed Property			33
7. Division of Administration, Bureau of Human Resource Management	Check Staff Driver License Status/Moving Violations		5
8. Division of Rehabilitation and Liquidation, Administrative Services Section			3
9. Division of Administration, Bureau of General Services, Facilities and Property Management Office	Parking Enforcement		3(a)
Total		289	87

Source: Data and information compiled by the OIG.
(a) The Division of Administration, Bureau of General Services revoked access for all of its users in March 2013.

FINDINGS AND RECOMMENDATIONS

During the summer of 2012, the Office of Inspector General (OIG) conducted an audit of the Department's Management of the Memorandum of Understanding for Use of the DAVID and DAVE Databases (IA 12-205) and noted various deficiencies. In response to that audit, management of the MOU was centralized and, in December 2012, the Department's Division of Information Systems (DIS) was assigned responsibility for managing the MOU.

In February and March 2013, DIS implemented written policies and procedures specific to the DAVE and DAVID Databases (the DAVE Access Control Procedures and DAVID Access Control Procedures). The policies address security of the databases and information obtained from the databases, access controls, and monitoring of the databases, among other things. In addition, the procedures establish a mechanism through which each of the user entities administration of the databases is monitored to ensure that activities required under the MOU are performed. For example, Quarterly Quality Control access reviews must be submitted to DIS upon completion. In this manner, DIS is able to determine whether the reviews are being performed quarterly and also to ensure that acceptable documentation is maintained to evidence the review. The DIS also developed and provided trainings to the user entity POCs and DCCs related to the new procedures and is in the process of rewriting its CSIRT Procedures, which are expected to be completed in December 2013.

This audit included a follow-up of the findings noted in our prior audit IA 12-205. Except as noted below, corrective action has been taken with respect to the findings noted in IA 12-205.

In general, based on the results of our testing, we determined that internal controls over the personal data exchanged under the MOU are adequate and operating effectively to protect the personal data from unauthorized access, distribution, use, modification or disclosure. We also determined that internal controls over the personal data could be improved to help ensure that the data is protected from unauthorized access, distribution, use, modification or disclosure. We noted the following:

Finding No. 1: Access Permissions Were Not Always Timely Revoked

Section IV.B.9. of the MOU requires the Department to update user access permissions upon termination or reassignment of users within five working days and immediately update user access permissions upon discovery of negligent, improper, or unauthorized use or dissemination of information.

In testing 18 employee separations, we noted that access was not timely revoked for five DAVID users. Access remained active from 26 to 288 days after the employees separated employment. In one instance, although the DCC timely requested that access be revoked, the DAVID user's name was misspelled in the revocation request and, therefore, the digital certificate was not revoked. In another two instances, the DCC had been out due to illness and the user entity did not have a back-up DCC. Failure to timely revoke access could result in an unauthorized use of the DAVID database.

Recommendation: The Department should consider enhancing its procedures to ensure that access is timely revoked and each user entity has a designated back-up for its DCC or POC. Additionally, revocation notices for DAVID users should contain sufficient information to ensure the proper identification of the digital certificate.

Finding No. 2: The Frequency and Performance of Quarterly Quality Control Access Reviews Need Improvement

Section IV.B.9. of the MOU requires the Department to conduct quarterly quality control (QQC) access reviews to ensure all current users are appropriately authorized to access the databases.

In February and March 2013, the Department implemented written procedures, including a form and instructions to assist the DCCs and POCs in completing the QQC reviews. The procedures require the DCCs and POCs to submit their QQC reviews to DIS, thereby creating a means to monitor completion of the reviews.

During the audit period, all of the user entities performed at least one QQC review. However, in the past, the reviews were not always conducted quarterly. With the implementation of the new policies and procedures, the frequency of the QQC reviews should improve.

We reviewed a sample of four of the user entities' QQC reviews, and noted the following:

a. While the QQC reviews were generally adequate, documentation of the reviews needs improvement. For example, for two of the four QQC reviews, the number of new and/or revoked users was not correctly noted on the QQC form. This was due, in part, to the way records were maintained to document the new and revoked users. Additionally, none of the four QQC reviews indicated the time period covered by the review.

b. For all four reviews, the QQC review forms did not reflect the review and approval of an appropriate supervisor. Although supervisory review and approval is not required by the new DAVE and DAVID Access Control Procedures, supervisory review and approval of the QQC reviews is a good control to better ensure that the reviews are being properly and timely completed and management is aware of the results of the review.

Recommendation: DIS should consider updating the DAVE and DAVID Access Control Procedures to require documented supervisory review and approval of the QQC reviews. Additionally, the POCs and DCCs would benefit from additional training and/or guidance related to the performance of the QQC reviews.

Finding No. 3: Four User Entities Retained Personal Information from DAVE Absent Written Authorization from DHSMV

Section IV.B.1. of the MOU provides that information obtained from the databases shall not be retained unless it is for a law enforcement purpose.

As noted in our prior audit, four of the Department's user entities retained personal information obtained from the DAVE database for non-law enforcement purposes. All four retained personal information in hard copy format and one retained the information electronically within the imaging component of its claims management system. Retention of this data is not consistent with the MOU and increases the risk that personal information will be inappropriately accessed and/or disclosed.

Subsequent to the end of the audit period, on April 11, 2013, the Department obtained written authorization from DHSMV to print and store a page from DAVE for business purposes.

Recommendation: In instances where clarification or changes are needed to the MOU, the Department should coordinate with its Division of Legal Services to seek written authorization and/or an amendment to the MOU, as necessary. Additionally, to decrease the risk of unauthorized access or disclosure, user entities should consider implementing alternative procedures to meet their documentation needs related to the personal data.

Finding No. 4: Access Authorization and Acknowledgement Forms Were Not Maintained for All Users

Sections V.D. and E. of the MOU require all personnel with access to the information exchanged under the MOU to be instructed on, 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.

We reviewed the practices of six of the Department's user entities related to access authorization and user acknowledgements. While the form and content of the user acknowledgement forms varied somewhat across the user entities, the forms were adequate to inform staff of the confidential nature of the information and criminal sanctions for misuse. Additionally, each of the user entities reported that users were required to sign the acknowledgement form prior to being granted access to the DAVE and DAVID databases. For some of the user entities, the acknowledgement form also served to document authorization to access the databases.

We reviewed documentation for a sample of 45 users, and noted the following:

a. Access authorization forms (which included the above-described acknowledgements) could not be provided for seven DAVID users. Three of the seven users did not sign access authorization forms at the time they were granted access to the system. For the remaining four users, the forms or other documentation had not been maintained by the DCC. As a result, the user entities were unable to demonstrate that, prior to the user being granted access to the DAVID database, supervisory approval had been obtained and that the user had acknowledged the confidential nature of the data and the criminal sanctions for misuse.

b. While access authorization forms were available for the remaining 38 users, for 27 of these users, sufficient documentation was not maintained to demonstrate that users had signed the authorization forms prior to being granted access to the DAVE/DAVID databases. In some instances, the acknowledgement forms were not dated so it was not possible to determine whether they were signed prior to the user being granted access to the database. In other instances, a historical roster which showed the date access was granted had not been maintained so it was not possible to determine when access was physically granted. User entity staff reported that the authorization forms were signed prior to access being granted to the databases.

Recommendation: The Department should consider enhancing its procedures to ensure that access authorization forms and user acknowledgements are properly maintained. Access and acknowledgement forms should be dated and proper records maintained to reflect all users of the databases and pertinent information such as the date access is granted/revoked, etc.

Finding No. 5: Procedures Over the Performance of Misuse Audits Need Improvement

Sections V.A. and F. of the MOU require the Department to monitor use of the databases on an on-going basis and mandate that database information will not be used for any purposes not

specifically authorized by the MOU. Unauthorized use includes, but is not limited to, queries not related to a legitimate business purpose, personal use, and the dissemination, sharing, copying or passing of this information to unauthorized persons.

Both the DAVE and DAVID databases include an audit tool which allows agency DCCs and POCs to run a report of the searches a user conducted during a specified time frame. During the audit period, all Department user entities conducted a misuse audit using the audit tool in order to determine the propriety of the searches made by the sampled users. Additionally, the Department developed written procedures, including a form and instructions to assist the DCCs and POCs in completing the misuse audits. The procedures require the misuse audits to be submitted to DIS, thereby creating a means to monitor completion of the reviews.

We reviewed a sample of four of the user entities' misuse audits, and noted the following:

a. For two of the four misuse audits, sufficient documentation was not maintained to evidence the proper completion of the misuse audits. For example, neither user entity retained the usage reports for the users audited. One did not document the results of the misuse audit on the prescribed form and, therefore, it was not evident which users had been audited, the time period covered by the audit, or the date the misuse audit was conducted.

b. The sampling methodology used by each of the sampled user entities was generally adequate. However, for three of the misuse audits, not all searches of the sampled users were evaluated to determine the propriety of the searches. This was due, in part, to the volume of searches performed by the sampled users during the audit period, but mainly to the difficulty in reconciling the usage reports to user entity records.[3]

   As noted in our prior audit, when performing a search of the DAVE and DAVID databases, a user must first select from a drop-down list the reason for the search. However, the databases do not permit the user to enter an identifying case or claim number or otherwise provide a means for the user to correlate the search to a specific case or claim. Therefore, the usage reports generated from the DAVE and DAVID databases do not link a user's searches to a specific investigation, claim or other identifier. To determine if a user's search activity was for a legitimate purpose, the DCC or POC must first correlate the information in the usage report with information maintained in an internal document or database. Since most of the user entities do not require their users to maintain a record of their search activity, it is difficult and sometimes not possible to link a search to a claim or case and, therefore, to validate that the search was for an authorized purpose.

c. For two of the four misuse audits, appropriate action was not taken by the user entity to investigate and resolve potential misuse or suspicious activity. For one of the misuse audits, the DCC prepared a list of questionable searches. In reviewing this list, we noted that one of the DAVID users had performed a search of an individual who had the same

[3] Although not included within our sample, three additional user entities reported difficulty verifying the searches performed and two of the three indicated that they did not verify the searches.

last name as the DAVID user. However, the DCC did not attempt to tie the search to a case and no inquiry was made to ascertain the propriety of the search. In the other misuse audit, although unverifiable searches were noted, no follow-up activity was undertaken to determine the propriety of the searches.

d. For three of the four misuse audits, the misuse audit did not reflect the review and approval of an appropriate supervisor. While the misuse audit forms do not require supervisory review and approval, review and approval of the misuse audits is a good control to better ensure that the misuse audits are being properly and timely completed and that management is aware of the results of the audits.

Recommendation: The DIS should consider updating the DAVE and DAVID Access Control Procedures to require documented supervisory review and approval of the misuse audits and clarify the type of supporting documentation to be maintained. Additionally, the DAVE POCs and DCCs would benefit from additional training and/or guidance related to the performance of the misuse audits (e.g., sampling methodology, search verification methods, documentation standards, etc.). The Department should consider exploring practical solutions which may include search logs or similar means to ensure that the POCs and DCCs are able to verify users' searches.

Finding No. 6: Department Security Incident Procedures are Not Sufficient to Meet the MOU's Unique Reporting Requirements

Section VI. B. of 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.

a. **Security Incident and Reporting Procedures Need Improvement.** Through February 2013, limited procedures existed to address the management of misuse incidents related to externally owned databases such as the DAVE and DAVID databases. In February 2013, the Department implemented the DAVE and DAVID Access Control Procedures which include some guidance related to misuse incidents and require that misuse incidents related to the databases follow the Department's established Computer Security Incident Reporting Team (CSIRT) process.

   The CSIRT process and procedures are outlined in the Department's CSIRT Guide (Guide). However, the Guide does not contain adequate provisions to ensure compliance with the unique terms of the MOU. For example, the Guide does not clearly require that corrective action be taken to address misuse incidents nor does it provide guidelines for determining how access to systems with confidential information should be addressed prior to completion of the investigation of the incident. Additionally, the Guide does not clearly outline a process for addressing Class 1 incidents (low severity) or set forth procedures for the notification to external parties. Absent clear written procedures related to misuse incidents involving the databases, there is limited assurance that misuse

incidents involving the databases will be addressed in a manner that is compliant with the MOU.

b. **Misuse Incidents Were Not Timely Reported and Required Parties Were Not Properly Notified.** During the audit period, two security incidents involving the DAVID database were reported to the OIG. The first incident was discovered in September 2012, and involved one employee who accessed the personal information of an immediate family member. As a result of internal miscommunications, the DHSMV was not notified of the misuse until 78 days after the misuse was confirmed.

   The second incident was discovered in February 2012, and involved multiple individuals who accessed emergency contact information (ECI) in the DAVID database. Per Section 119.0712(2)(c), Florida Statutes, ECI contained in a motor vehicle record may only be released to law enforcement agencies for purposes of contacting those listed in the event of an emergency. With respect to this incident, the user entity did not immediately report the misuse to DIS and the OIG verbally or in writing as required by Administrative Policy and Procedure (AP&P) 4-03. Additionally, the DHSMV was not notified of the incident until approximately 70 days after the misuse was confirmed. Failure to provide immediate notification of suspected incidents impinges the Department's ability to respond to, mitigate, and investigate the incident and may corrupt evidence of the misuse.

c. **User Access Permissions Were Not Updated.** The MOU requires the Department to "immediately update user access permissions upon discovery of negligent, improper, or unauthorized use or dissemination of information." However, for the two misuse incidents noted above, access permissions were not updated for any of the users involved in the incidents. Although the DAVID and DAVE Access Control Procedures require, in instances of misuse, that access be revoked "following the appropriate notifications," it is not clear who is responsible for providing the notification to the DCC and POC to revoke access, and no guidance is provided as to how access should be handled during the investigation or upon its conclusion. The lack of specific guidelines which outline responsibilities could result in access not being timely and/or properly revoked.

Recommendation: The Department should continue its efforts to enhance its CSIRT procedures to ensure that the procedures meet the unique requirements of the MOU and other externally owned systems. Clarification is needed to the DAVID and DAVE Access Control Procedures to designate who is responsible, in misuse incidents, for notifying the DCC/POC to revoke access and also when revocation should occur during the misuse incident. Additionally, clarification should be sought from DHSMV regarding the updating of access permissions related to misuse incidents.

Finding No. 7: Department Contracting Policies and Procedures are Not Sufficient to Ensure a Proper Evaluation of Legal Authority for Data Exchange Agreements

Section I. of the MOU requires the Department to affirm that it is authorized to obtain personal information under the Driver's Privacy Protection Act (DPPA), 18 USC Section 2721, et. seq.

Further, per Section IV.B.6., the Department may only use the information obtained under the MOU for the purposes authorized by the MOU.

Although the Department as an agency is authorized under the DPPA to access personal information contained within the driver license and motor vehicle records, an organizational unit within the Department may not be authorized. Accordingly, we reviewed the statutory basis for each user entity's access to the DAVE database.

Of the five user entities which had access to the DAVE database, no statutory authority was apparent for one user entity which used the database for parking enforcement services. In March 2013, the user entity determined that it no longer had a business need to access the database and revoked all of its users' access to the database.

Our prior audit noted that the Department's contracting procedures needed improvement for ensuring that appropriate statutory authority exists prior to executing MOU's for the exchange of data and information with external entities. Although the Department's new DAVID and DAVE Access Control Procedures require DIS to evaluate annually each user entity's "business need" for accessing the respective database, a review of business need is not sufficient to ensure that statutory authority exists to access the databases.

Upon review of DFS contracting procedures, we noted that the Contract and Life Cycle Procurement Guide, which establishes the roles and responsibilities of each party in the contract process, does not require any of the parties involved in the contracting process to evaluate statutory authority. Although the Attorney Reviewer is required to evaluate contracts for legal sufficiency, among other things, the Division of Legal Services indicated that statutory authority is not evaluated during the Attorney Reviewer's review of a contract/MOU. Absent clear responsibility for determining statutory authority, there is limited assurance that these types of agreements will be properly evaluated to ensure that statutory authority exists for each user entity's use of the databases.

Recommendation: DIS should consider amending the DAVID and DAVE procedures to define processes for new user entities to acquire database access. Additionally, General Services should consider amending the Contract Management and Life Cycle and Procurement Guide to identify those individuals who are responsible for determining statutory authority for these types of agreements.

Finding No. 8: Security Issue Involving the DAVID Database Needs Remediation

During our prior audit, we identified a security issue related to DAVID access. The issue was discussed with the Department's Chief Information Officer and Information Security Manager and steps to remediate the issue were undertaken. However, the issue has not been fully remediated.

Recommendation: The Department should continue its efforts to remediate the security issue.

MANAGEMENT'S RESPONSE

Department management concurred with all findings and recommendations. Management's response to the audit is attached hereto as Appendix A. The OIG agrees with the response.

OBJECTIVES, SCOPE AND METHODOLOGY

Objectives & Scope

The overall objective of this audit was to evaluate whether the internal controls over the personal data exchanged under DHSMV MOU HSMV-0380-12 are adequate and operating effectively to protect the personal data from unauthorized access, distribution, use, modification or disclosure. Our audit covered the period September 13, 2012, to March 31, 2013. In addition, our audit included follow-up on the audit findings included in our report IA 12-205 to determine whether corrective action had been taken.

Methodology

This audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* published by the Institute of Internal Auditors. Those 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 our findings and conclusions based on our audit objectives.

To accomplish our objectives, we reviewed the 2011 Memorandum of Understanding established between DFS and DHSMV. We reviewed relevant federal and state laws and rules, internal policies and procedures established by DIS and 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 Digital Certificate Coordinator for DAVID manual and other DHSMV publications, memos and related documents.

We met with responsible Department management to discuss the criteria to be used to evaluate internal controls related to the databases, which followed the October 9, 2012 audit worksheet provided by DHSMV. We interviewed relevant staff within the Florida Department of Highway Safety and Motor Vehicles. Within DFS, we interviewed the Chief of the Bureau of General Services and 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 in Tallahassee, Orlando, and Tampa. 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 obtain information regarding each user entity's administration and use of the DAVID and/or DAVE databases. Among other steps, we

evaluated access controls, monitoring activities, training/education activities related to database use and security awareness, dissemination practices, security practices and incident reporting. Our testing included:

- We sampled 45 users and reviewed access authorization documentation, evidence of security awareness training and required acknowledgements.
- We sampled four QQC reviews and four misuse audits performed by the user entities and evaluated the adequacy and effectiveness of the reviews.
- We reviewed the legal basis for the DAVE user entities to access the database.
- We sampled 18 employee separations and movements to determine the timeliness of database access revocations.
- We observed the security practices of five of the user entities at select locations in Tallahassee, Orlando, and Tampa.
- We evaluated two misuse incidents related to the DAVID database to determine compliance with the MOU's misuse reporting requirements and Department security incident reporting procedures.
- We evaluated limited general security controls over the electronic case/claims management systems of five user entities.

Management's Responsibility for Internal Controls

In accordance with Department Administrative Policy and Procedures 1-02 (Internal Controls Policy), the Department, among its divisions, shall establish and maintain a system of internal controls. The internal controls are management driven and designed to provide reasonable assurance that objectives are achieved. Accordingly, Department management is responsible for establishing and maintaining adequate internal controls for compliance with the MOU. The OIG's responsibility is to evaluate the internal controls and compliance with the MOU.

Inherent Limitations In Any System of Internal Controls

Because of inherent limitations in any system of internal controls, errors or irregularities may nevertheless occur and not be detected. Also, projection of any evaluation of the system to future periods is subject to the risk that procedures may become inadequate because of changes in conditions, or that the degree of compliance with procedures may deteriorate. Accordingly, our audit would not necessarily disclose all weaknesses in Department internal controls over the personal data exchanged under the MOU to protect the personal data from unauthorized access, distribution, use, modification or disclosure.

DISTRIBUTION LIST

Jeff Atwater, Chief Financial Officer
Robert Kneip, Chief of Staff
Jay Etheridge, Deputy Chief Financial Officer
Paul Whitfield, Deputy Chief Financial Officer
P.K. Jameson, General Counsel
Daniel Anderson, Director, Division of Insurance Fraud
Stephanie Iliff, Director, Division of Administration
Terry Kester, Chief Information Officer
Tanner Holloman, Director, Division of Workers' Compensation
Julius Halas, Director, Division of State Fire Marshal
Randy Burkhalter, Director, Division of Public Assistance Fraud
Sha'Ron James, Director, Division of Rehabilitation and Liquidation
Christina Smith, Director, Division of Accounting & Auditing
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 Leah Gardner, C.P.A., Director of Auditing.

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

CHIEF FINANCIAL OFFICER
JEFF ATWATER
STATE OF FLORIDA

APPENDIX A

June 6, 2013

Mr. Tom Kirwin
Inspector General
Department of Financial Services
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 Audit of Internal Controls Over Personal Data Exchanged Under DHSMV Memorandum of Understanding and Audit Follow-up of IA 12-205.

If you have any questions concerning this response, please contact the Department of Financial Services Information Technology Security and Compliance Office at (850) 413-3041.

Sincerely,

Robert Kneip
Chief of Staff

RK:ivj

Enclosure

MANAGEMENT'S RESPONSE TO OIG AUDIT OF INTERNAL CONTROLS OVER PERSONAL DATA EXCHANGED UNDER DHSMV MEMORANDUM OF UNDERSTANDING AND AUDIT FOLLOW-UP OF IA 12-205

Finding No. 1: Access Permissions

Access Permissions were not always timely revoked.

Recommendation: The Department should consider enhancing its procedures to ensure that access is timely revoked and each user entity has a designated back-up for its Digital Certificate Coordinators (DCC) or Point of Contacts (POC). Additionally, revocation notices for DAVID users should contain sufficient information to ensure the proper identification of the digital certificate.

Management's Response: We concur. DIS is currently in the process of reviewing and updating DAVE and DAVID Access Control Procedures and user entities are endeavoring to designate and train backup personnel. The Department will work with FDLE to ensure that digital certificates are properly identified for revocation.

Expected Completion Date for Corrective Action: December 31, 2013

Finding No. 2: Quarterly Quality Control (QQC) Access Reviews

The QQC access reviews were not always conducted quarterly. Documentation of four reviews was not adequate in that some of the reviews contained errors, none denoted the time period covered by the review, and none evidenced supervisory review and approval.

Recommendation: The Division of Information Systems (DIS) should consider updating the DAVE and DAVID Access Control Procedures to require documented supervisory review and approval of the QQC reviews. Additionally, the POCs and DCCs would benefit from additional training and/or guidance related to the performance of the QQC reviews.

Management's Response: We concur. DIS is currently in the process of reviewing and updating DAVE and DAVID Access Control Procedures, including the QQC review form and instructions. The updated procedures and forms will be provided to DCCs and POCs as guidance for the performance of the QQC reviews.

Expected Completion Date for Corrective Action: December 31, 2013

Finding No. 3: Retention of DAVE Information

Four DAVE user entities retained personal data obtained from the DAVE database for non-law enforcement purposes, absent written authorization from the Department of Highway Safety and Motor Vehicles (DHSMV).

Recommendation: In instances where clarification or changes are needed to the Memorandum of Understanding (MOU), the Department should coordinate with its Division of Legal Services to seek written authorization and/or an amendment to the MOU, as necessary. Additionally, to decrease the risk of unauthorized access or disclosure, user entities may want to consider implementing alternative procedures to meet their documentation needs related to the personal data.

Management's Response: We concur. The Department has received written authorization from DHSMV to retain data obtained from the DAVE database. The DHSMV has stated that the MOU will be revised subsequent to the implementation of the new DAVID system. The Department will coordinate with the Department's Division of Legal Services for execution of the revised MOU at that time.

Of the four user entities included in the recommendation above, one user entity has discontinued use of the DAVE system, removed all DAVE system access, and shredded all previously acquired DAVE information as of May 24, 2013; one user entity has implemented procedures, as of May 20, 2013, that have removed the use of information from the DAVE database; and the remaining two user entities will consider alternate procedures.

Expected Completion Date for Corrective Action: December 31, 2013

Finding No. 4: Access Authorization and Acknowledgement Forms

Access authorization and acknowledgement forms were not maintained for all users. Sufficient documentation was not maintained to evidence that users of the DAVID database had signed access authorization forms and user acknowledgements prior to being granted access to the database.

Recommendation: The Department should consider enhancing its procedures to ensure that access authorization forms and user acknowledgements are properly maintained. Access and acknowledgement forms should be dated and proper records maintained to reflect all users of the databases and pertinent information such as the date access is granted/revoked, etc.

Management's Response: We concur. In March 2013, DIS implemented DAVE and DAVID Access Control Procedures that clearly define the responsibility for maintaining the dated access authorization forms and user acknowledgements that are incorporated as attachments to the procedures. DIS is currently in the process of reviewing and updating DAVE and DAVID Access Control Procedures, including requirements for detailed user listings. The updated procedures and form will be provided to DCCs and POCs as guidance.

Expected Completion Date for Corrective Action: December 31, 2013

Finding No. 5: Misuse Audits

Sufficient documentation was not always maintained to evidence the proper completion of the misuse audits and appropriate action was not always taken to investigate and resolve potential misuse or questionable searches. The misuse audits did not evidence proper supervisory review and approval and most user entities did not have an adequate means to verify database search activity.

Recommendation: The DIS should consider updating the DAVE and DAVID Access Control Procedures to require documented supervisory review and approval of the misuse audits and clarify the type of supporting documentation to be maintained. Additionally, the DAVE POCs and DCCs would benefit from additional training and/or guidance related to the performance of the misuse audits (e.g. sampling methodology, search verification methods, documentation standards, etc.). The Department should consider exploring practical solutions which may include search logs or similar means to ensure that the POCs and DCCs are able to verify users' searches.

Management's Response: We concur. DIS is currently in the process of reviewing and updating DAVE and DAVID Access Control Procedures, including the audit forms and instructions. The updated procedures and form will be provided to DCCs and POCs as guidance for the performance of the misuse audits. The DAVE and DAVID systems, including the audit tool, are currently being rewritten and are expected to be fully implemented in the fall of 2013. With the rewrite of DAVE and DAVID, it is our understanding that many enhancements will be addressed which may include the capability for tying searches to individual cases. The Department continues to be in contact with DHSMV and is reviewing options for correlating usage activity to authorized business functions.

Expected Completion Date for Corrective Action: December 31, 2013

Finding No. 6: Security Incident Procedures

Security incident procedures were not sufficient to meet the unique reporting needs of the MOU and access permissions were not updated for users involved in misuse incidents. Misuse incidents were not timely and properly reported to the Division of Information Services, the Office of Inspector General or the Department of Highway Safety and Motor Vehicles.

Recommendation: The Department should continue its efforts to enhance its Computer Security Incident Reporting Team (CSIRT) procedures to ensure that the procedures meet the unique requirements of the MOU and other externally owned systems. Clarification is needed to the DAVID and DAVE Access Control Procedures to designate who is responsible, in misuse incidents, for notifying the DCC/POC to revoke access and also when revocation should occur during the misuse incident. Additionally, clarification should be sought from DHSMV regarding the updating of access permissions related to misuse incidents.

Management's Response: We concur. DIS is currently in the process of reviewing and updating CSIRT procedures and the DAVE and DAVID Access Control Procedures. The updated CSIRT procedures will be implemented after they have been reviewed and approved by the CSIRT team. Additionally, DIS is consulting with relavant parties to determine appropriate timing for updating access permissions related to misuse indicidents.

Expected Completion Date for Corrective Action: December 31, 2013

Finding No. 7: Department Contracting Policies and Procedures

Department contracting policies and procedures are not sufficient to ensure a proper evaluation of legal authority for data exchange agreements.

Recommendation: DIS should consider amending the DAVID and DAVE procedures to define processes for new user entities to acquire database access. Additionally, General Services should amend the Contract Management and Life Cycle and Procurement Guide to identify those individuals who are responsible for determining statutory authority for these types of agreements.

Management's Response: We concur. DIS is currently in the process of reviewing and updating DAVE and DAVID Access Control Procedures. Additionally, General Services has added clarifying language to the Contract Management Life Cycle and Procurement Guide to identify those individuals who are responsible for determining and validating statutory authority.

Expected Completion Date for Corrective Action: December 31, 2013

Finding No. 8: Security Issue – Confidential Finding

A security issue involving the DAVID database needs remediation.

Recommendation: The Department should continue its efforts to remediate the security issue.

Management's Response: We concur. The Department is continuing its efforts to remediate the security issue. The planned solution is approaching the testing phase and is scheduled to be fully implemented by September 30, 2013.

Expected Completion Date for Corrective Action: September 30, 2013