



COUNTY AUDIT

HILLSBOROUGH COUNTY, FLORIDA

**DRIVER AND VEHICLE INFORMATION DATABASE (DAVID) ACCESS
CONTROLS AUDIT**

REPORT # 320

FEBRUARY 20, 2017



February 20, 2017

Dear Pat Frank, Clerk of the Circuit Court and Comptroller:

The Audit Team performed an audit of the Driver And Vehicle Information Database (DAVID) Access Controls (Audit Report # 320, dated February 20, 2017). Responses to the Audit Team's recommendations were received from the Chief Deputy of Courts and have been included in the Report after the audit comment and recommendations.

The purpose of this Report is to furnish management independent, objective analysis, recommendations, counsel, and information concerning the activities reviewed. It is not an appraisal or rating of management.

Although the Audit Team exercised due professional care in the performance of this audit, this should not be construed to mean that unreported noncompliance or irregularities do not exist. The deterrence of fraud and/or employee abuse is the responsibility of management. Audit procedures alone, even when carried out with professional care, do not guarantee that fraud or abuse will be detected.

The Audit Team appreciates the cooperation and professional courtesies extended to the auditors by the Chief Deputy of Courts and Senior Directors during this audit.

Sincerely,

Steve Hooper, CIA, CGAP, CCSA, CFE
Director of County Audit

CC: Doug Bakke, Chief Deputy, Courts
Kathleen Rocamora, Senior Director, Civil Courts
Brandi Williams, Senior Director, Criminal Courts

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1

 BACKGROUND INFORMATION 1

 OBJECTIVE 1

 SCOPE 1

 OVERALL EVALUATION 1

 OPINION 2

 AUDITED BY 2

AUDIT COMMENTS & RECOMMENDATIONS 3

EXECUTIVE SUMMARY

BACKGROUND INFORMATION

The Florida Department of Highway Safety and Motor Vehicles (DHSMV) hosts a system known as the Driver And Vehicle Information Database (DAVID) that is used to provide secure online access to driver and motor vehicle information. DAVID is intended for use only by law enforcement, criminal justice agencies, government departments, and Clerks of the Circuit Court and Comptrollers. The DHSMV requires agencies to sign a Memorandum Of Understanding (MOU) agreement that requires certain internal controls to protect personal data from unauthorized access, distribution, use, modification, or disclosure. The Hillsborough County Clerk of the Circuit Court and Comptroller (Clerk's Office) has an MOU agreement with the DHSMV and grants certain employees access accounts to DAVID with a username and password. Each employee's account is setup with access to only certain role permissions at certain time ranges and days of the week.

OBJECTIVE

The objective of the audit was to assess whether or not the Clerk's Office has appropriate internal controls in place to ensure the protection of personal data maintained in the DAVID database from unauthorized access, distribution, use, modification, or disclosure.

SCOPE

The audit was conducted in conformance with the *Generally Accepted Government Auditing Standards* and the *International Standards for the Professional Practice of Internal Auditing*. These Standards require that County Audit plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the audit comments and conclusions based on the audit objectives. County Audit believes that the evidence obtained provides this reasonable basis.

The DHSMV publishes an Audit Guide document that lists recommended audit procedures to test user access controls. The Audit Team utilized this audit guide and obtained a complete list of all DAVID users, for both active and inactive accounts, as-of October 26, 2016.

OVERALL EVALUATION

The management and employees of the Clerk's Office were responsive to the Audit Team's inquiries and provided the information requested in a timely and courteous manner. The Audit Team encountered knowledgeable and dedicated employees during the course of the audit.

AUDIT COMMENT	CONCLUSION OF OBJECTIVE	PAGE
1	Implementation Of DAVID Access Controls Is Necessary To Comply With The Memorandum Of Understanding (MOU).	3

OPINION

The control environment relative to the user access controls over the DAVID system is at the informal maturity level. Required tasks listed in the MOU are not formally assigned and delegated to ensure they are performed. There is a need for policies and/or procedures to ensure compliance with those control requirements specified in the MOU. In some cases, there is a need for the Clerk's Office to implement these controls for the first time. Addressing the improvement opportunities identified throughout this Report will enhance the overall control structure of DAVID user accounts through increased accountability, consistency, and sustainability.

The exit conference was held on January 26, 2017.

Other minor concerns not included in this Report were communicated to management and/or corrected during fieldwork.

AUDITED BY

Steve Hooper, CIA, CGAP, CCSA, CFE, Director of County Audit
Heidi Pinner, CIA, CFE, CISA, CRMA, General & IT Audit Manager
Ben Everett, CPA, CIA, CFE, Senior Internal Auditor

AUDIT COMMENT & RECOMMENDATIONS

AUDIT COMMENT

Implementation Of DAVID Access Controls Is Necessary To Comply With The Memorandum Of Understanding (MOU).

The Audit Team reviewed pertinent system data and system activity logs for individual DAVID users to determine whether or not:

- Quarterly reviews and annual audits are performed by the Clerk's Office.
- Users completed the online training and exam each year as required by the DAVID system.
- User access role permissions are appropriate.
- User access is terminated upon employee separation or re-assignment.
- User logins and inquiries appeared reasonably appropriate for business purposes.
- The inquiry was not performed on relatives, celebrities, political figures, or other unusual records.
- User access inquiry dates and times were within normal Clerk business hours.

At the beginning of the audit, Clerk's Office management decided to limit DAVID access to supervisors and managers only. At that time, 58 of the 86 users (67%) in the population were deactivated. During audit testing, Clerk's Office management decided that access to DAVID will no longer be needed by the Clerk's Office. All remaining users were deactivated, except for one user with administrator rights who management will deactivate upon completion of this audit. The Audit Team proceeded on to complete audit testing.

Quarterly Reviews and Annual Audits

The MOU requires the Clerk's Office to perform quarterly quality control reviews to ensure all current users are appropriately authorized. An annual audit performed by management to ensure proper and authorized use and information dissemination is also required. The Audit Team determined that the quarterly reviews and annual audits had not been performed. Management indicated they were unaware of these requirements and had not delegated the responsibility to any particular employee or director.

Annual Online Training and Examination

Once per year, the DAVID system automatically requires each user to complete a brief online training session and pass an exam. This training and exam may be used to satisfy an MOU requirement that states users must acknowledge the confidential nature of the information and the criminal sanctions for misuse of that information. The Audit Team obtained a listing of the population of all DAVID users, which consisted of 86 accounts. A sample of 24 users was

judgmentally selected from the population for audit testing. Of those 24 users, a data report from DAVID obtained by the Audit Team showed that 20 of them (83%) had completed the online training. Four (4) of the 24 samples (17%) had not completed the online training within the last year.

Appropriate User Access Roles

Certain DAVID users have administrative rights to create, setup, and edit new DAVID users. The administrator grants access to some or all of the available role permissions by clicking checkboxes for each role in the administrator's setup screen. The setup screen also allows the administrator to specify what time ranges and days of the week that the user's account login allows access to those roles.

The Audit Team reviewed the access setup screens for the 24 users in the audit sample for appropriateness. The Audit Team found inconsistencies in the access given to each user. Fourteen users were given access only from Monday through Friday, 2 users were setup for Monday through Saturday, and 8 users had access all 7 days of the week. Some users had access to certain role permissions checked off while others did not, and vice-versa. It is unclear how these determinations were made when setting up the accounts. There is no written policy or procedure for deciding what roles and access time ranges/days should be given to a user.

Deactivating Access After Employee Separation or Re-Assignment

DAVID administrators have the ability to deactivate a user's account to turn off the user's access. The MOU requires a user's account to be deactivated within 5 working days after the user's employment ends or when the user is re-assigned to a different job position that does not require DAVID access. The Clerk's Office has not had a procedure or control in place to ensure these accounts are deactivated within the 5-working-day requirement. The Audit Team reviewed the population of 86 DAVID accounts and determined that 26 of the users (30%) were no longer employed in the Clerk's Office. Three of the 26 users (12%) had their DAVID access deactivated within 5 working days as required by the MOU. Twenty-three of the users however had their access deactivated after the 5-day requirement, most of them by a significant margin. Fourteen of the 26 users (54%) were not deactivated until over 100 calendar days after their employment ended. However, based on the users' last login dates, the Audit Team was able to determine that none of the users utilized their access after their employment separation date.

Appropriateness of DAVID Use

The Audit Team reviewed the activity log report for each of the 24 users selected in the audit sample. These activity logs were for the 18-month period ending November 29, 2016 and included data indicating what tasks were performed by the user with the date and time. The Audit Team reviewed the logs for appropriateness to determine if any unusual names were searched for or if any access times were on holidays, weekends, or after business hours. None of the users in the sample were found to have accessed DAVID during times that are considered

unusual. Two of the 24 sample users (8%) had instances where they accessed family member records. Based on the wording in the DAVID Audit Guide document, this could be considered inappropriate access.

RECOMMENDATIONS

Clerk's Office management should formalize the decision to discontinue the use of DAVID and work with its legal counsel to update or terminate the MOU agreement. The last remaining DAVID user should then be deactivated. If management were to ever re-establish the use of DAVID in the Clerk's Office, the following corrective actions for improvement should be considered by management:

- Prepare a written policy or procedure that assigns the responsibilities required in the MOU.
- Perform quarterly reviews and annual audits of the DAVID user accounts and activity.
- Implement a process to ensure all users complete the required training and exam annually.
- Develop a rationale or methodology for determining what role permissions and access times are granted to each user based on their job responsibilities.
- Require users with administrative access to review the activity of other users that have administrative access.
- Implement controls to ensure user access is deactivated upon employee separation or re-assignment.
- Inform users about what is considered appropriate use of DAVID for business purposes and include related guidance in the policies and/or procedures.

CLIENT RESPONSE

Concur

CORRECTIVE ACTION PLAN

All Clerk Staff DAVID access has been placed in an 'inactive status' effective 02/14/2017. A meeting will be held on 02/22/2017 with Clerk's Chief Legal Counsel to pursue updating / termination of the MOU Agreement with the Florida Department of Highway Safety and Motor Vehicles.

TARGET COMPLETION DATE

April 1, 2017