CENTRAL FLORIDA EXPRESSWAY AUTHORITY

protiviti®
Risk & Business Consulting.
Internal Audit.

DHSMV Data Security Assessment

Central Florida Expressway Authority

December 2015

Table of Contents

Executive Summary

Overview

During the period of December 7, 2015 to December 18, 2015, Internal Audit performed a Data Security Assessment of the Department of Highway Safety and Motor Vehicles (DHSMV) data within the Central Florida Expressway Authority (CFX) environment. The objectives of the assessment were to review internal controls for gaps in design related to the requirements set forth in *Section V – Safeguarding Information*, of the DHSMV Drivers License or Motor Vehicle Record Data Exchange Memorandum of Understanding (MOU).

The summarized objectives of Section V are:

- Information exchanged 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 purposes, personal use, and the dissemination, sharing, copying or passing of this information to unauthorized persons.

- Information exchanged by electronic means will be stored in a place physically secure from access by unauthorized persons.

- Access to the information will be protected in such a way that unauthorized persons cannot review or retrieve the information.

- All personnel with access to the information exchanged under the terms of the MOU will be instructed of, and acknowledge their understanding of, the confidential nature of the information. These acknowledgements must be maintained in a current status by the Requesting Party (CFX).

- All personnel with access to the information will be instructed of, and acknowledge their understanding of, the criminal sanctions specified in state law for unauthorized use of the data. These acknowledgements must be maintained in a current status by the Requesting Party (CFX).

- All access to the information must be monitored on an on-going basis by the Requesting Party (CFX). In addition, the Requesting Party (CFX) must complete an annual audit to ensure proper and authorized use and dissemination.

Executive Summary

Scope & Approach

Internal Audit conducted an assessment of the process used for safeguarding DHSMV data in the CFX environment. In order to complete this review, the following procedures were performed:

- Reviewed policies and procedures related to the safeguarding of electronic and physical data transfers, data storage, and data access.
- Conducted interviews with key personnel to understand the *Drivers License or Motor Vehicle Record Data Exchange* process.
- CFX Management approved the scope of work and believed it to be sufficient to meet the requirements of the MOU. Conducted testing of controls related to the following areas:
    - Policies and Procedures
    - Application Access
    - Segregation of Duties
    - Change Control
    - Data Storage
    - Data Transfer
    - Network Firewall
    - Network Architecture
    - Active Directory
    - Physical Security
- After testing was completed, analysis was performed to compare the results of testing to the control objectives outlined in the MOU.

Executive Summary

Summary of Results

As a result of this review, Internal Audit identified zero (0) observations that should be addressed in order to enhance CFX's Drivers License or Motor Vehicle Data Exchange process.

Appendix A – Controls Tested

	Control Objective	Control Description	Testing Results
1	Information exchanged will not be used for any purposes not specifically authorized by this agreement. 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.	**Policies and Procedures:** CFX implements company-wide policies and procedures that enforce the safeguarding of company data and other sensitive customer data whether or not it is currently being used or accessed.	**Control Effective**
2	All personnel with access to the information exchanged under the terms of the Drivers License or Motor Vehicle Record Data Exchange MOU will be instructed of, and acknowledge their understanding of, the confidential nature of the information. These acknowledgements must be maintained in a current status by the requesting party.	**Training:** CFX requires in the hiring process that all users sign an acknowledgement after reviewing either the employee or contractor security guidelines handbook which covers the safeguarding of data. These acknowledgments must be maintained for all current/active users.	**Control Effective**
3	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**TRIMS Access:** System access to the TRIMS applications for new users is appropriately administered through the submission of a New User Authorization Form. This form is completed by the new user's Manager and the proper approvals/signatures are obtained. Access to the applications is then administered by IT support.	**Control Effective**
4	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**TRIMS Access - Terminated Users:** System access to the TRIMS application and company network is appropriately revoked in a timely fashion for terminated users. Upon receipt of a termination notification (email, authorization form, phone call, etc.) from HR or a Manager responsible for the terminated user, the user's system account is disabled immediately.	**Control Effective**
5	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Database-level Access:** Database-level access is restricted to the appropriate individuals through the use of unique accounts.	**Control Effective**

Appendix A – Controls Tested

	Control Objective	Control Description	Testing Results
6	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Server-level Access:** Server-level access is restricted to the appropriate individuals through the use of unique accounts.	**Control Effective**
7	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**FTP Gateway Access:** All individuals / user accounts with access to the FTP Gateway are authorized and appropriate.	**Control Effective**
8	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Host (HT250) Access:** All individuals / user accounts with access to the Host (HT250) are authorized and appropriate.	**Control Effective**
9	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Oracle DB Access:** All individuals / user accounts with access to the Oracle DB are authorized and appropriate.	**Control Effective**
10	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**DOCPRD1 Access:** All individuals / user accounts with access to the DOCPRD1 server are authorized and appropriate.	**Control Effective**
11	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Infoview Crystal Reports (RPTPRD4) Server Access:** All individuals / user accounts with access to the Infoview Crystal Reports (RPTPRD4) server are authorized and appropriate.	**Control Effective**
12	Information exchanged will not be used for any purposes not specifically authorized by this agreement. 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.	**DHSMV Data Access:** Management performs a periodic review of user access across each of the in-scope entities to ensure that the assigned access level is commensurate with his/her job function.	**Control Effective**

Appendix A – Controls Tested

	Control Objective	Control Description	Testing Results
13	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Change Control / Patch Management:** Dedicated Test environments exist for the testing of changes and patches, where practical. CFX appropriately documents and tests each change.	**Control Effective**
14	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Change Control / Patch Management:** All changes and patches are authorized, executed, and documented according to stated procedures.	**Control Effective**
15	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Data Encryption:** Driver's license number as it is obtained from the DHSMV is encrypted when stored in the Oracle database. Also test encryption methods at all other transmission points, including at network, application, and database layers (if applicable).	**Control Effective**
16	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Network - Firewall:** CFX has an operational firewall in place to restrict access to the internal network.	**Control Effective**
17	Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information.	**Network - Active Directory:** All individuals with Active Directory credentials are current, active users and all rights granted through Active Directory are commensurate with their current job responsibilities.	**Control Effective**
18	Information exchanged by electronic means will be stored in a place physically secure from access by unauthorized persons.	**Physical Security - Data Center:** Access to the data center(s) is restricted to appropriate personnel and is provided through the use of a physical key, key card, biometric, or other form of physical security.	**Control Effective**

Appendix A – Controls Tested

	Control Objective	Control Description	Testing Results
19	Information exchanged by electronic means will be stored in a place physically secure from access by unauthorized persons.	**Physical Security - Work Areas:** Access to the work areas is restricted to appropriate personnel and is provided through the use of a physical key, key card, biometric, or other form of physical security.	**Control Effective**
20	All access to the information must be monitored on an on-going basis by the Requesting Party. In addition the Requesting Party must complete an annual audit to ensure proper and authorized use and dissemination.	**Logging & Monitoring:** Logging and auditing functions are enabled on all in-scope entities. In addition, all system logs are monitored for unauthorized access and irregular activity.	**Control Effective**
21	All access to the information must be monitored on an on-going basis by the Requesting Party. In addition the Requesting Party must complete an annual audit to ensure proper and authorized use and dissemination.	**Vulnerability Scanning / Penetration Testing:** CFX performs periodic external vulnerability scans and penetration tests.	**Control Effective**