CENTRAL
FLORIDA
EXPRESSWAY
AUTHORITY

protiviti®
Face the Future with Confidence

DAVID Data Security Assessment

Central Florida Expressway Authority

February 2019

This document has been prepared for use by CFX Management, Internal Audit and board of directors. This report provides information about the condition of risks and internal controls at one point in time. Future events and changes may impact these risks and controls in ways that this report did not and cannot anticipate.

Table of Contents

This document has been prepared for use by CFX Management, Internal Audit and board of directors. This report provides information about the condition of risks and internal controls at one point in time. Future events and changes may impact these risks and controls in ways that this report did not and cannot anticipate.

Executive Summary

Overview

During the period of January 22, 2019 to February 6, 2019, Internal Audit performed a Data Security Assessment of the Driver and Vehicle Information Database systems ("DAVID") 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 Driver and Vehicle Information Database 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.
- The Requesting Party shall not indemnify and shall not be liable to the Providing Agency for any driver license or motor vehicle information lost, damaged, or destroyed as a result of the electronic exchange of data pursuant to the MOU, except as otherwise provided in Section 768.28, Florida Statutes.
- Any and all DAVID-related information provided to the Requesting Party (CFX) as a result of the MOU, particularly data from the DAVID system, will be stored in a place physically secure from access by unauthorized persons.
- The Requesting Party shall comply with Rule 74-2, Florida Administrative Code, and with Providing Agency's security policies, and employ adequate security measures to protect Providing Agency's information, applications, data, resources, and services. The applicable Providing Agency's security policies shall be made available to Requesting Party.
- When printed information from DAVID is no longer needed, it shall be destroyed by cross-cut shredding or incineration.
- The Requesting Party (CFX) shall maintain a list of all persons authorized within the agency to access DAVID information, which must be provided to the providing agency upon request.
- Access to DAVID-related information, particularly data from the DAVID System, will be protected in such a way that unauthorized persons cannot view, retrieve, or print the information.
- Under the MOU agreement, access to DAVID shall be provided to users who are direct employees of the Requesting Party (CFX) and shall not be provided to any non-employee or contractors of the Requesting Party (CFX).

Scope and Approach

Internal Audit conducted an assessment of the process used for safeguarding DAVID 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 and Vehicle Information Database System Data Exchange* process.

- CFX Management approved the scope of work and believed it to be sufficient to meet the requirements of the MOU. Performed testing of controls related to the following areas:

  - Policies and Procedures
  - Application Access
  - Risk Management
  - Change Control
  - Data Storage
  - Data Transfer
  - Network Firewall
  - Network Architecture
  - System Authentication
  - Access Controls
  - Physical Security

- After testing was completed, analysis was performed to compare the results of testing to the control objectives outlined in the MOU.

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 Driver and Motor Vehicle Database system Data Exchange process.

Appendix A – Controls Tested

	Control Objective	Control Description	Testing Results
1	Document and manage legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations.	**Policies and Procedures:** CFX has identified cybersecurity legal and regulatory requirements and identified individuals responsible for managing requirements.	**Control Effective**
2	Ensure governance and risk management processes address cybersecurity risks.	**Risk Management:** CFX has documented risk management processes in place to address cybersecurity risks.	**Control Effective**
3	Identify and prioritize risk responses, implement risk mitigation plans, and monitor and document plan implementation.	**Risk Management:** CFX has implemented risk management processes in place to mitigate risks identified.	**Control Effective**
4	Determine risk tolerance as necessary, based upon: their analysis of sector specific risks; the agency's industry sector; agency-specific risks (e.g., Health Information Portability Accountability Act of 1996 compliance for agencies that maintain this information); and the agency's role in the state's mission.	**Risk Management:** CFX has implemented risk management processes in place to identify industry specific risks.	**Control Effective**
5	Establish parameters for IT Staff participation in procurement activities.	**Procurement Activities:** CFX has implemented policies and procedures for procurement activities.	**Control Effective**
6	Identify the IT issues IT staff must address during procurement activities (e.g., system hardening, logging, performance, service availability, incident notification, and recovery expectations).	**Procurement Activities:** CFX has implemented policies and procedures to ensure proper requirements are addressed during procurement activities.	**Control Effective**

	Control Objective	Control Description	Testing Results
7	Prior to introducing new IT resources or modifying current IT resources, perform an impact analysis. The purpose of this analysis is to assess the effects of the technology or modifications on the existing environment.	**Change Control:** Changes are classified prior to implementation to identify the effects of changes within the environment. CFX appropriately documents and tests each change.	**Control Effective**
8	Ensure that privileged users understand their roles and responsibilities.	**Privileged Access:** All individuals / users with privileged access are aware of their responsibilities to CFX's data security.	**Control Effective**
9	Maintain adequate capacity to ensure system availability and data integrity.	**System Monitoring:** CFX has implemented automated mechanisms to monitor system capacity and data integrity.	**Control Effective**
10	Integrity checking mechanisms are used to verify hardware integrity.	**Hardware Integrity:** Access to physical devices is restricted to authorized individuals and additional integrity monitoring is in place to detect changes to critical system files associated with hardware devices.	**Control Effective**
11	Ensure backups of information are conducted, maintained, and tested periodically.	**Backup Procedures:** Backups are conducted and tested periodically.	**Control Effective**
12	Establish a policy and procedure review process that facilitates continuous improvement to protection processes.	**Security Improvement:** CFX has implemented a risk assessment process to monitor and facilitate improvement of security controls currently in place.	**Control Effective**
13	Ensure that effectiveness of protection technologies is shared with stakeholders that should or must receive this information.	**Technology Effectiveness:** CFX communicates the effectiveness of implemented technologies related to cybersecurity when deemed necessary.	**Control Effective**
14	Each agency shall perform maintenance and repairs of information systems and components consistent with agency-developed policies and procedures.	**System Maintenance:** Maintenance on in-scope systems is documented and performed by appropriate personnel or approved vendors where maintenance agreements are in place.	**Control Effective**

	Control Objective	Control Description	Testing Results
15	Not engage in new development of custom authenticators. Agencies assess the feasibility of replacing agency-developed authenticators in legacy applications.	**Authentication Mechanisms:** CFX utilizes Active Directory authentication on in-scope systems. For systems not utilizing Active Directory authentication, CFX utilizes .NET authentication frameworks for one in-scope system with plans to implement Active Directory authentication for future system implementation.	**Control Effective**
16	Protect and restrict removable media in accordance with agency-developed information security policy.	**Removable Media:** CFX has implemented controls to prevent removable media where not required for business purposes.	**Control Effective**
17	Protect communications and control networks by establishing perimeter security measures to prevent unauthorized connections to agency IT resources.	**Network Firewall:** CFX has an operational firewall in place to restrict access to the internal network.	**Control Effective**
18	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	**System Availability:** CFX has implemented a redundant data center to provide resiliency in the event of system outages.	**Control Effective**
19	Each agency shall develop policies and procedures that will facilitate detection of anomalous activity in a timely manner and that will allow the agency to understand the potential impact of events. Such policies and procedures shall establish and manage a baseline of network operations and expected data flows for users and systems	**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**
20	Monitoring for unauthorized personnel, connections, devices, and software.	**Access Controls:** CFX has implemented badge access and cameras at facilities, and firewalls, file integrity, and antivirus software on systems to restrict access to the internal network, and unauthorized software.	**Control Effective**

This document has been prepared for use by CFX Management, Internal Audit and board of directors. This report provides information about the condition of risks and internal controls at one point in time. Future events and changes may impact these risks and controls in ways that this report did not and cannot anticipate.

protiviti®

Face the Future with Confidence