AGENDA
AUDIT COMMITTEE MEETING
January 27, 2021
10:00 a.m.

Meeting location: Central Florida Expressway Authority
4974 ORL Tower Road
Orlando, FL 32807
Boardroom

A. CALL TO ORDER

B. PUBLIC COMMENT

Pursuant to Section 286.0114, Florida Statutes and CFX Rule 1-1.011, the Audit Committee provides for an opportunity for public comment at the beginning of each regular meeting. The Public may address the Committee on any matter of public interest under the Committee's authority and jurisdiction, regardless of whether the matter is on the Committee's agenda but excluding pending procurement issues. Each speaker shall be limited to 3 minutes.The Public may also submit written comments in advance of the meeting to be read into the record except that if the comments exceed 3 minutes in length, when read, they will only be attached as part of the minutes.

C. APPROVAL OF OCTOBER 27, 2020 BOARD MEETING MINUTES (action Item)

D. AGENDA ITEMS

1. **STATUS UPDATE: FISCAL 2021 INTERNAL AUDIT PLAN** – *Jeff Tecau, Managing Director, Protiviti* (info item)

2. **PROJECT UPDATES**

   a) ERP Requirements Support – *Emily Picard, Senior Manager, Protiviti* (info item)
   b) Toll Revenue Audit Planning – *Alex Conrad, Senior Manager, Protiviti* (info item)

3. **REVIEW AND ACCEPTANCE OF COMPLETED INTERNAL AUDIT REPORTS** (action item)

   a) DHSMV Data Security Assessment – *Chris Porter, Associate Director, Protiviti* (action item)
   b) DAVID Data Security Assessment – *Chris Porter, Associate Director, Protiviti* (action item)
   c) PCI Assessment with Report on Compliance – *David Taylor, Managing Director, Protiviti* (action item)
   d) Ethics Policy Compliance Audit – *Emily Picard, Senior Manager, Protiviti* (action item)

4. **INTERNAL AUDIT BUDGET FOR FISCAL YEAR 2022** – *Lisa Lumbard, Chief Financial Officer* (action item)

(CONTINUED ON PAGE 2)

E. OTHER BUSINESS

F. ADJOURNMENT

This meeting is open to the public.

Section 286.0105, Florida Statutes states that if a person decides to appeal any decision made by a board, agency, or commission with respect to any matter considered at a meeting or hearing, they will need a record of the proceedings, and that, for such purpose, they may need to ensure that a verbatim record of the proceedings is made, which record includes the testimony and evidence upon which the appeal is to be based.

Persons who require translation services, which are provided at no cost, should contact CFX at (407) 690-5000 x5316 or by email at Iranetta.Dennis@cfxway.com at least three (3) business days prior to the event.

In accordance with the Americans with Disabilities Act (ADA), if any person with a disability as defined by the ADA needs special accommodations to participate in this proceeding, then they should contact the Central Florida Expressway Authority at (407) 690-5000 no later than two (2) business days prior to the proceeding.

Please note that participants attending meetings held at the CFX Headquarters Building are subject to certain limitations and restrictions in order to adhere to the CDC guidelines and to ensure the safety and welfare of the public.

C.
Approval Of Minutes

DRAFT MINUTES
CENTRAL FLORIDA EXPRESSWAY AUTHORITY
AUDIT COMMITTEE MEETING
October 27, 2020

Location: Virtual Meeting
Call (321) 430-0870
Conference ID: 924 164 74#

Committee Members Appearing Virtually:
Michelle McCrimmon, City of Orlando Representative, Chairman
Kaye Dover, Osceola County Representative
Kathy Wall, Brevard County Representative
Ray Walls, Orange County Representative

Committee Members Not Present:
Lorie Bailey Brown, Seminole County Representative
Kristy Mullane, Lake County Representative

Others Appearing Virtually:
Laura Kelley, Executive Director
Lisa Lumbard, Chief Financial Officer
Jim Greer, Chief Technology Officer
Woody Rodriguez, General Counsel
Rita Moore, Recording Secretary/Executive Assistant
Daniel O'Keefe, MSL, P.A.
Joel Knopp, MSL, P.A.
Jeff Tecau, Protiviti
Martin Nash, Protiviti
Emily Picard, Protiviti
Chris Porter, Protiviti
David Taylor, Protiviti

A. CALL TO ORDER

The meeting was called to order at approximately 09:59 a.m. by Chairman McCrimmon. Recording Secretary Rita Moore called the roll and announced there was a quorum with four (4) Committee Members present.

B. PUBLIC COMMENT

There was no public comment.

C. APPROVAL OF THE JUNE 17, 2020 MINUTES

A motion was made by Ms. Dover and seconded by Chairman McCrimmon to approve the June 17, 2020 minutes as presented. The motion carried unanimously with four (4) members voting AYE by voice vote. Two (2) members, Ms. Bailey Brown and Ms. Mullane were not present.

D. EXTERNAL AUDIT MATTERS – MSL, P.A.

1. Review and Acceptance of Audit of Fiscal 2020 Financial Statements and Required Communications

Mr. Joel Knopp of MSL, P.A. presented the Review and Acceptance of Audit of Fiscal 2020 Financial Statements and Required Communications.

Committee members asked questions which were answered by Mr. Knopp.

A motion was made by Ms. Dover and seconded by Mr. Walls to accept the Audit of Fiscal 2020 Financial Statements and Required Communications as presented. The motion carried unanimously with four (4) members voting AYE by voice vote. Two (2) members, Ms. Bailey Brown and Ms. Mullane were not present.

E. INTERNAL AUDIT MATTERS – Protiviti

1. Status Update: Fiscal 2021 Internal Audit Plan

Mr. Jeff Tecau of Protiviti presented the Fiscal 2021 Internal Audit Plan to the committee.

(This item was presented for information only. No formal committee action was taken.)

The following item was taken out of order.

3. Other Internal Audit Items:

    a. Public Records Review Maturity Model

Mr. Jeff Tecau of Protiviti presented the Public Records Review Maturity Model to the committee.

Committee members asked questions which were answered by Mr. Tecau.

(This item was presented for information only. No formal committee action was taken.)

2. Review and Acceptance of Completed Internal Audit Reports

b. Public Records Review (Fiscal 2020)

Ms. Emily Picard of Protiviti presented the Public Records Review (Fiscal 2020) to the committee for acceptance.

Committee members asked questions which were answered by Ms. Picard.

A motion was made by Mr. Walls and seconded by Ms. Dover to accept the Public Records Review as presented. The motion carried unanimously with four (4) members voting AYE by voice vote. Two (2) members, Ms. Bailey Brown and Ms. Mullane were not present.

c. Prior Audit Recommendations: Semi-Annual Follow-Up (Fiscal 2021)

Ms. Emily Picard of Protiviti presented the Prior Audit Recommendations: Semi Annual Follow- Up (Fiscal 2021) to the committee for acceptance.

Committee members asked questions which were answered by Ms. Picard and Ms. Lumbard.

A motion was made by Ms. Dover and seconded by Ms. Wall to accept the Prior Audit Recommendations: Semi-Annual Follow-Up as presented. The motion carried unanimously with four (4) members voting AYE by voice vote. Two (2) members, Ms. Bailey Brown and Ms. Mullane were not present.

d. Procurement and Contract Billing Audits (Fiscal 2021)

Ms. Emily Picard of Protiviti presented the Procurement and Contract Billing Audits (Fiscal 2021) to the committee for acceptance.

A motion was made by Ms. Wall and seconded by Ms. Dover to accept the Procurement and Contract Billing Audits as presented. The motion carried unanimously with four (4) members voting AYE by voice vote. Two (2) members, Ms. Bailey Brown and Ms. Mullane were not present.

3. Other Internal Audit Items:

    b. ERP Requirements Support Update and Supplemental Agreement

Ms. Emily Picard and Mr. Martin Nash of Protiviti presented the ERP Requirements Support Update and Supplemental Agreement to the committee for acceptance.

Committee members asked questions which were answered by Ms. Picard and Mr. Nash.

A motion was made by Mr. Walls and seconded by Ms. Dover to accept the ERP Requirements Support Update and Supplemental Agreement as presented. The motion carried unanimously with four (4) members voting AYE by voice vote. Two (2) members, Ms. Bailey Brown and Ms. Mullane were not present.

F. OTHER BUSINESS

No other business was reported.

Mr. Rodriguez, General Counsel explained to the meeting attendees that this portion of the meeting is confidential. He then allowed time for any participants outside of the Committee members, presenters (Protiviti), and CFX Support staff to exit the meeting.

Confidential Recording started at approximately 11:18 a.m.

G. CONFIDENTIAL SECURITY AUDIT

1. NIST Cybersecurity Framework Review (Fiscal 2020)

Ms. Chris Porter of Protiviti presented the NIST Cybersecurity Framework Review (Fiscal 2020) to the committee for acceptance.

A motion was made by Ms. Dover and seconded by Mr. Walls to accept the NIST Cybersecurity Framework Review as presented. The motion carried unanimously with four (4) members voting AYE by voice vote. Two (2) members, Ms. Bailey Brown and Ms. Mullane were not present.

H. ADJOURNMENT

Chairman McCrimmon adjourned the meeting at approximately 11:35 a.m.

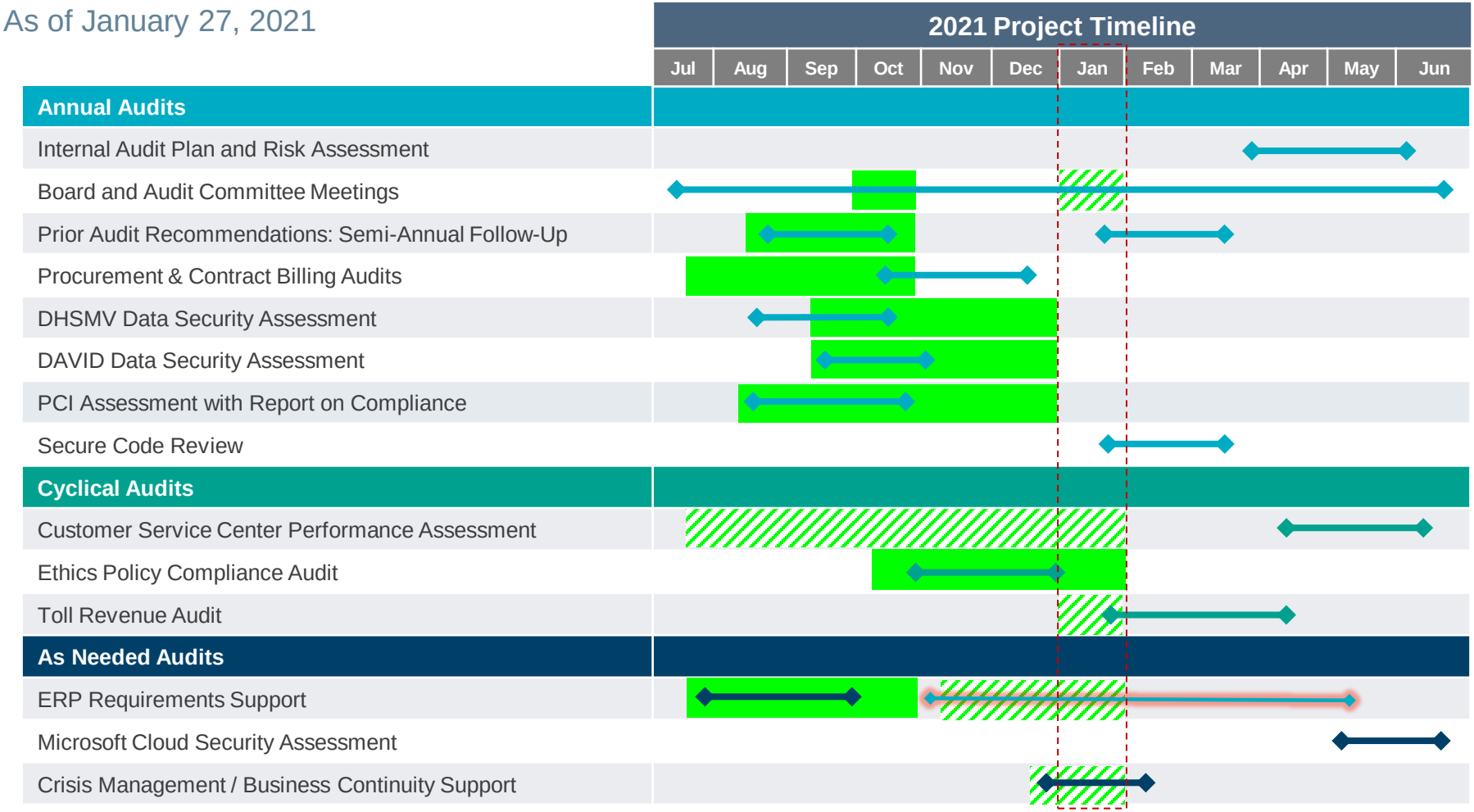
Minutes approved on ____, 2021.

Pursuant to the Florida Public Records Law and CFX Records Management Policy, audio tapes of all Board and applicable Committee meetings are maintained and available upon request to the Records Management Liaison Officer at publicrecords@CFXway.com or 4974 ORL Tower Road, Orlando, FL 32807.

D.1
Status Update: Fiscal 2021 Internal Audit Plan

INTERNAL AUDIT STATUS

As of January 27, 2021



CENTRAL FLORIDA EXPRESSWAY AUTHORITY protiviti

D.2a
ERP
Requirements
Support

NO BACKUP MATERIALS PROVIDED FOR THIS ITEM

D.2b
Toll Revenue Audit Planning

NO BACKUP MATERIALS PROVIDED FOR THIS ITEM

D.3a
DHSMV Data Security Assessment

CENTRAL FLORIDA EXPRESSWAY AUTHORITY

protiviti®
Face the Future with Confidence

DHSMV Data Security Assessment

Central Florida Expressway Authority

December 2020

Table of Contents

Executive Summary

Overview

During the period of November 17th, 2020 to December 17th, 2020, 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.

Scope and 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.

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**

	Control Objective	Control Description	Testing Results
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**
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.	**DOCPRD2 Access:** All individuals / user accounts with access to the DOCPRD2 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**

	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.	**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 or key card.	**Control Effective**
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 or key card.	**Control Effective**

	Control Objective	Control Description	Testing Results
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**

D.3b
DAVID Data Security Assessment

CENTRAL FLORIDA EXPRESSWAY AUTHORITY

protiviti®
Face the Future with Confidence

DAVID Data Security Assessment

Central Florida Expressway Authority

November 2020

Table of Contents

Executive Summary

Overview

During the period of November 2nd, 2020 to November 20th, 2020, 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**

D.3c
PCI Assessment with Report on Compliance

Face the Future with Confidence

Central Florida Expressway Authority

Payment Card Industry (PCI) Assessment

Summary Meeting

January 2021

protiviti®

Face the Future with Confidence

PCI Data Security Standard

The assessment focused on over 400 controls within the following twelve domains of the PCI Data Security Standard

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

protiviti®

Summary of the Assessment

- Protiviti team performed onsite and remote fieldwork between July 11, 2020 through December 15, 2020.
- Fieldwork was conducted through a variety of methods including documentation review, interviews, technical analysis, and physical investigation.
- Issue identified in which vendor responsible for logging practices did not retain logs for the required year, and did not include all appropriate systems. Issue has been remediated.
- All CFX individuals involved were extremely helpful and well attuned to the importance of the assessment.

Face the Future with Confidence

D.3d
Ethics Policy Compliance Report

CENTRAL FLORIDA EXPRESSWAY AUTHORITY

protiviti®
Face the Future with Confidence

CENTRAL FLORIDA EXPRESSWAY AUTHORITY

Ethics Policy Compliance Review

January 2021

Internal Audit, Risk, Business & Technology Consulting

TABLE OF CONTENTS

protiviti

EXECUTIVE SUMMARY

Overview

The Central Florida Expressway Authority ("CFX") operates for the benefit of the public. As such, CFX strives to conduct business in accordance with the highest standard of ethics. The CFX Code of Ethics governs board members, committee members, employees, and consultants in the performance of their duties and obligations to CFX and serves as the standard for official conduct.

As part of a three-year audit cycle outlined in the 2021 Internal Audit Plan, Internal Audit has completed a review of CFX's compliance with the Code of Ethics. Internal Audit last reviewed the compliance with the Code of Ethics in January 2018.

After the January 2018 review, the Code of Ethics was modified in April 2018 to prohibit consultants from holding conflicting employment or contractual relationships.

Objectives, Scope, and Approach

The objectives of this audit were to (1) review CFX's ethics compliance process and related monitoring controls for design and operating effectiveness, and (2) assess CFX board and committee member, employee, and consultant compliance with the Code of Ethics.

The Ethics Policy Compliance Review was performed using the following approach:

1. Conducted interviews with CFX management regarding policy, applicable Florida Statutes, procedures, key personnel, and compliance reporting;
2. Reviewed the Code of Ethics and the following Florida Statutes to identify compliance requirements:
    a. Chapter 112, Part III
    b. Chapter 348.753
    c. Section 104.31;

EXECUTIVE SUMMARY

Objectives, Scope, and Approach

3. Evaluated CFX's processes for monitoring compliance with the Code of Ethics and related internal controls for design effectiveness. Processes evaluated included the following areas:
    a. Communication and Awareness
    b. Training and Reinforcement
    c. Change Management
    d. Conflicts of Interest and Financial Disclosure Monitoring
    e. Violation Monitoring
    f. Penalties and Enforcement;

4. Performed operating effectiveness testing for identified key internal controls for the period February 1, 2018 through July 31, 2020;

5. Reviewed CFX board and committee member, employee, and consultant compliance with the Code of Ethics for the period February 1, 2018 through July 31, 2020; and

6. Identified opportunities and developed recommendations for improving the Authority's ethics compliance management process and internal controls.

EXECUTIVE SUMMARY

Summary of Procedures Performed and Results

Internal Audit evaluated CFX's ethics compliance management processes, internal controls, and the related design and operating effectiveness of the controls based on the requirements of the Code of Ethics and the applicable Florida Statutes. Based on audit results, one opportunity was identified that, if implemented, will strengthen CFX's overall ethics compliance management and internal control environment. The table below provides an overview of the areas reviewed and the opportunity identified.

Area	Procedures Performed	# of Controls Tested	Observation #
Communication and Awareness	✓ Reviewed ownership and responsibility for oversight of the CFX Code of Ethics **– *No Audit Findings*** ✓ Evaluated the effectiveness of communication to internal and external parties regarding ethics requirements **– *No Audit Findings*** ✓ Evaluated controls to obtain internal and external party acknowledgement of the CFX Code of Ethics **– *No Audit Findings***	7	-
Training and Reinforcement	✓ Evaluated Board, Committee, employee and consultant compliance with training **– *No Audit Findings*** ✓ Evaluated controls to encourage employee communication with management regarding ethical matters and ethical compliance **– *Observation #1***	3	1
Change Management	✓ Evaluated controls to review and update the CFX Code of Ethics **– *No Audit Findings*** ✓ Evaluated the process to communicate Code updates and changes **– *No Audit Findings***	2	-
Potential Conflict and Financial Disclosure Monitoring Violation Monitoring	✓ Evaluated Board, Committee, employee, and consultant compliance with conflict of interest and financial disclosure requirements **– *No Audit Findings*** ✓ Evaluated Board and Committee member compliance with voting conflict forms and requirements **– *No Audit Findings*** ✓ Reviewed the process for reporting and monitoring ethics concerns and alleged violations **– *No Audit Findings*** ✓ Evaluated controls to encourage and facilitate employee communication of violations **– *No Audit Findings***	4	-
Penalties and Enforcement	✓ Evaluated penalty and enforcement procedures for noncompliance **– *No Audit Findings***	3	-

DETAILED OBSERVATIONS

DETAILED OBSERVATIONS

Observation 1 – Ethics Hotline Number in Employee Handbook

Risk Rating: Low

Observation

Employees are encouraged to express concerns about their work environment to their supervisor. To further promote a safe, secure and successful professional environment at the Central Florida Expressway Authority, a “Make a Difference” hotline is available to CFX employees and vendors to anonymously report suspected unethical, illegal, or unsafe acts without fear of retaliation. The number for the hotline is listed in the Employee Handbook available to all CFX employees.

Based on review of the Employee Handbook and hotline testing, the first reference to the "Make a Difference" hotline phone number in the Employee Handbook was identified as an invalid number (page 7, “800-226-6043”). Two additional references to the hotline within the Employee Handbook represented the accurate phone number for employees to reach the hotline (pages 11 and 14, “888-226-6043”). An invalid whistleblower hotline listed in Employee Handbook may cause confusion and may result in failure to report suspected unethical, illegal or unsafe acts without fear of retaliation.

Recommendation

Annually, CFX should review and update the Employee Handbook to ensure all information is consistent and accurate, including accuracy of the hotline phone number in all locations referenced.

Management Response

Management concurs.

Management Action Plan

Management will coordinate with Human Resources to make necessary updates to the Employee Handbook to correct the identified reference to the "Make a Difference" hotline phone number. Management will also review other sources of the phone number for accuracy.

Action Plan Owner / Due Date

Woody Rodriguez, General Counsel / Complete

Face the Future with Confidence

protiviti®

D.4
INTERNAL AUDIT BUDGET FOR FISCAL YEAR 2022

Account Number	2020 Actuals	2021 Budget	2021 YTD Actuals	2021 Annualized Amt	2021 Yr. End Est	2022 Preliminary Bud
80 Other Expenses						
05 Toll Collection						
130 Administration						
690 Internal Audit						
53410 Contract Personnel	471,496.25	564,000.00	214,967.50	573,246.67	[ ]	0.00
Total Internal Audit	471,496.25	564,000.00	214,967.50	573,246.67		0.00
Total Toll Collection	471,496.25	564,000.00	214,967.50	573,246.67		0.00
Total 80 Other Expenses	471,496.25	564,000.00	214,967.50	573,246.67		0.00
Grand Total	471,496.25	564,000.00	214,967.50	573,246.67		0.00