REPORT ON CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS (SSAE No. 16) FOR MyFloridaCounty.Com

For the period January 1, 2016 through December 31, 2016

LANIGAN & ASSOCIATES, PC
CERTIFIED PUBLIC ACCOUNTANTS
TABLE OF CONTENTS

SECTION I. INDEPENDENT SERVICE AUDITORS’ REPORT ....................................................... 1

SECTION II. GENERAL DESCRIPTION OF THE MFC CONTROL STRUCTUREAND OPERATIONS .......................................................................................... 5

Florida Association of Court Clerk’s Assertion ................................................................. 6
Overview of the MFC’s System Operations ...................................................................... 8
General Description of the MFC Control Structure ......................................................... 10
Description of Information Systems ................................................................................ 14
Description of Functional Services and Processing ......................................................... 17
Control Objectives and Related Controls ....................................................................... 19
Types of Tests Performed ................................................................................................. 19

SECTION III. DESCRIPTION OF CONTROLS, CONTROL OBJECTIVES, RELATED CONTROL PROCEDURES, AND TEST OF OPERATING EFFECTIVENESS ........................................... 20

Objective 1. Organizational and Administrative Controls .............................................. 21
Objective 2. Transaction Processing and Reconciliation ................................................ 24
Objective 3. Physical Security .......................................................................................... 29
Objective 4. Environmental Controls .............................................................................. 32
Objective 5. Network Security and Internet Access ......................................................... 33
Objective 6. Information and Communication ................................................................. 37
Objective 7. Segregation of Functions (Internal) .............................................................. 39
Objective 8. Segregation of Functions (External) ............................................................. 41
Objective 9. Service Fee Schedule .................................................................................. 42
Objective 10. Data Backup and Recovery ....................................................................... 43
SECTION I.
INDEPENDENT SERVICE AUDITORS’ REPORT
INDEPENDENT SERVICE AUDITORS’ REPORT

Board of Directors
Florida Association of Court Clerks and Comptrollers

Scope

We have examined the Florida Association of Court Clerks (FACC) dba Florida Court Clerks & Comptrollers’ (FCCC), hereinafter referred to as FCCC, description of its MyFloridaCounty.com (MFC) system for processing user entities’ transactions throughout the period January 1, 2016 to December 31, 2016 and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description.

Service organization’s responsibilities

On pages 6-7 of the description, the FCCC has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. The FCCC is responsible for preparing the description for the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Service auditor’s responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period January 1, 2016 to December 31, 2016.
Independent Service Auditors’ Report
November 28, 2017

An examination of a description of a service organization’s system and the suitability of the design and operating effectiveness of the service organization’s controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description.

Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description, the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in management’s assertion on pages 6-7. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

*Inherent limitations*

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become inadequate or fail.

*Opinion*

In our opinion, in all material respects, based on the criteria described in the FCCC’s assertion on pages 6-7;

\( a. \) The description fairly presents the system that was designed and implemented throughout the period January 1, 2016 to December 31, 2016.

\( b. \) The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period January 1, 2016 to December 31, 2016.

\( c. \) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period January 1, 2016 to December 31, 2016.

*Description of tests of controls*

The specific controls tested and the nature, timing, and results of those tests are listed on pages 21-43.
Restricted use

This report, including the description of tests of controls and results thereof on pages 21-43, is intended solely for the information and use of the FCCC, user entities of the MFC portal during some or all of the period January 1, 2016 to December 31, 2016, and the independent auditors of such user entities, who have sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements or user entities’ financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Lanigan & Associates, PC

Lanigan and Associates, P.C.
November 28, 2017
SECTION II.
GENERAL DESCRIPTION OF THE MFC CONTROL STRUCTURE AND OPERATIONS
FLORIDA COURT CLERKS AND COMPTROLLERS' ASSERTION

We have prepared the description of the MyFloridaCounty.com (MFC) for user entities of the portal during some or all of the period January 1, 2016 to December 31, 2016, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the portal themselves, when assessing the risks of material misstatements of user entities' financial statements. We confirm, to the best of our knowledge and belief, that:

A. The description fairly presents the MFC Portal made available to user entities during the period January 1, 2016 to December 31, 2016, for processing their transactions. The criteria we used in making this assertion were that the description:

1. Presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including, if applicable:

   • the types of services provided including, as appropriate, the classes of transactions processed.
   
   • the procedures, within both automated and manual systems, by which services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information prepared for user entities.
   
   • the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
   
   • how the system captures significant events and conditions, other than transactions.
   
   • the process used to prepare reports and other information for user entities.
   
   • the specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls contemplated in the design of the service organization's controls.
   
   • other aspects of our control environment, risk assessment process, information and communication systems (including related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.
2. Does not omit or distort information relevant to the scope of the MFC, while acknowledging that the description is presented to meet the common needs of a broad range of user entities of the systems and their financial statement auditors, and may not, therefore, include every aspect of the portal that each individual user entity of the portal and its auditor may consider important in its own particular environment.

B. The description includes relevant details of the changes to the system during the period covered by the description.

C. The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period January 1, 2016 to December 31, 2016, to achieve those control objectives. The criteria we used in making this assertion were that:

1. the risks that threaten the achievement of the control objectives stated in the description have been identified by management;

2. the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

3. the controls were consistently applied as designed and manual controls were applied by individuals who have the appropriate competence and authority.

Sean Hudson, Acting Executive Director

Linda Harmon, Acting Chief Financial Officer
OVERVIEW OF THE MFC SYSTEM OPERATIONS

Company Overview

Launched in February 2002, MyFloridaCounty.com (MFC) is a fully integrated local government e-commerce website that provides public access to government services and information through an internet portal.

The services that are currently available through MFC include:

- Search and Order Official Records Service (ORI)
- Child Support Payment and Inquiry Service
- Traffic Citation Inquiry and Payment Service (TCATS)
- Central Cashiering
- Website hosting service

MFC allows anyone with access to the Internet the ability to inquire on and make payments for the different services listed above.

Search and Order Official Records Service (ORI)

The Official Records Index (ORI) and Document Ordering System of MFC enable the internet user to perform a search of millions of documents/instruments and party names. These records represent documents from 63 counties in Florida. The search interface allows the user to limit their search by party name, and then by county, circuit, or region of the State. The search can be further refined by selecting certain document types or by using a date range. Once a particular document is found, the user has the choice to order a regular or certified copy of that document. The order process includes the ability to select the delivery method (fax, US mail, or overnight mail).

Once a document has been ordered using MFC, the records management staff in each Clerk's office receives email notification of the new order. The order fulfillment process allows the Clerk's staff to manage orders through a secured section of MFC. This secured area also allows the finance staff in each Clerk's office to run reports for performing their bank reconciliations.

Traffic Citation Payment and Inquiry Service (TCATS)

The Traffic Citation Payment and Inquiry Service of MFC allow the user to inquire on and make payments for traffic citations. The Internet user must provide two of the following three identifiers: citation number, license number, and date of birth. Once the correct information is entered, open citations can be viewed and payments on those citations can be made using a credit card.
Once a citation has been paid using MFC, the traffic staff in the Clerk's office receives email notification. The Clerk’s office can access a secured section of the MFC to download the payment information into their local traffic application. Staff can also use the secured MFC area for reports and financial reconciliations.

**Child Support Payment and Inquiry Service**

The Child Support Payment and Inquiry Service of MFC allow the user to inquire and make payments on his or her child support case. Custodial and non-custodial parents can view the most recent payments made on his or her child support case. Non-custodial parents can make an instant payment on their case using a credit card. In addition, non-custodial parents and employers (processing income deduction orders) have the ability to set up MFC payment accounts. The account allows them to monitor the cases for which they make payments. Once a payer’s account is set up, payments can be made via credit card or electronic check.

**Central Cashiering**

The Central Cashiering (formerly called Over the Counter Credit Card Service (OTC)) function provides the Clerks' offices the ability to accept credit card payments at the counter in their offices. This service uses the e-commerce capability provided through MFC. Each participating office has a credit card swipe machine connected to their computer system that utilizes the MFC to process the transactions.

**Website Hosting Service**

The Website Hosting Service of MyFloridaCounty.com gives each participating Clerk's office a local website. These websites provide the ability to present information about the various functions of their offices, including Courts, Jury, Traffic, Marriage and Contact Information.
GENERAL DESCRIPTION OF THE MFC CONTROL STRUCTURE

Control Environment:

The FCCC's control environment reflects the overall attitude, awareness, and actions of the board of directors/committees, management, and others concerning the importance of controls and their emphasis within the organization. The effectiveness of specific controls is established, enhanced or mitigated by various factors, including:

- Management's philosophy and operating style
- Organizational structure
- Board of Directors/Committees
- Assignment of authority and responsibility
- Commitment to competence
- Written policies and practices
- Various external influences that affect an entity's operations and practices, such as audits/reviews from external entities

Organizational Structure:

The organizational structure defines how authority and responsibility are delegated and monitored. It provides a framework for planning, executing, controlling, and monitoring operations.

The FCCC Board of Directors has ultimate responsibility for overseeing FCCC operations. The Board is comprised of Clerks presiding in the State of Florida. The Board of Managers for the FCCC Services Group, LLC, provides policy direction for issues pertaining to the CLERC System. It also is comprised of Clerks presiding in the State of Florida. Both Boards convene at least five times annually.

The FCCC Technology Committee has closer involvement to the technical aspects of the FCCC. The function of the Technology Committee is to provide program and policy direction relating to the application of technology within the Clerks’ offices. In addition, the Committee provides development and management oversight for FCCC sponsored applications (including the MFC system’s operations, controls, etc.). The Technology Committee is comprised of six Clerks presiding in the State of Florida. This committee also meets at least five times during the year at FCCC Conferences.

The FCCC is headed by the Executive Director who reports directly to the Executive Committee. Overseeing the day to day operations of the MFC System is the Information Technology (IT) Director. The FCCC Technology division is comprised of approximately 54 staff.
The Technical Division is segregated into the following functions:

- Systems Engineering and Operations
- Application Development
- Service Center
- Technical Projects

**Integrity and Ethical Values:**

The FCCC believes that maintaining an environment of integrity and ethical values is critical to the establishment and maintenance of its internal control structure. The effectiveness of internal controls is a function of the integrity and ethical values of the individuals who create, administer, and monitor the controls.

**Commitment to Competence:**

Competence is the knowledge and skills necessary to accomplish the tasks that define an individual’s job. The FCCC specifies the competence level for a particular job and translates it into the required level of knowledge and skills. As noted below, the FCCC has job descriptions for each job associated with MFC.

The FCCC believes that it has implemented sound Human Resource practices that help attract and retain competent and trustworthy employees. This is evidenced by the fact that the FCCC has very little employee turnover.

**Personnel Policies and Procedures:**

The FCCC effectively assigns authority and responsibilities throughout the organization. There are several documented controls the FCCC has in place to support this. First, the FCCC has a well specified organizational chart for the Technical Division which indicates the lines of authority and responsibility. Second, the FCCC maintains current employee job descriptions that are reviewed periodically to ensure that employee duties are commensurate with management's expectations. Management ensures that all employees have the required skills to manage the portal and responsibility delegated to them.

The FCCC has formal hiring practices designed to ensure that new employees are qualified for their job responsibilities. All applicants pass through an interview process that assesses their qualifications related to the expected responsibility level of the individual. In addition, background checks and criminal history checks are conducted on all external candidates.

The FCCC's policy requires that all employees receive an annual written performance evaluation and salary review. These reviews are based on goals, responsibilities, and performance factors that are prepared and rated by the employee's supervisor and reviewed with the employee. Completed appraisals are reviewed by senior management and become a permanent part of the employee's personnel file.
The FCCC’s progressive discipline system provides a framework for letting employees know when there are problems, giving the employees an opportunity to correct the problems, and permitting some type of review process for the final decision to terminate the employee.

**Risk Assessment:**

The FCCC has placed into operation a risk assessment process to identify and manage risks that could affect the organization's ability to provide reliable transaction processing for clients. This process requires management to identify significant risks in their areas of responsibility and to implement appropriate measures to address these risks. The risk management systems implemented by the FCCC consist of internal controls derived from its policies, processes, personnel, and systems. Specifically, the primary control activities in place to mitigate these risks are described in the column entitled “Description of Controls” in Section III of this report.

**Monitoring:**

FCCC Management monitors operations, performance, quality and internal controls as a normal part of their activities. FCCC Management and staff, engaged in the technical and operational responsibilities, meet on a routine basis to discuss various issues pertaining to the MFC System. The type of issues discussed include, but are not be limited too; problem resolution, system modification and enhancements, and file processing.

As mentioned previously, the FCCC has established and maintains a comprehensive internal control system. The FCCC engages the following external audits/reviews:

1. Independent Financial Statement Audit (Annual):
   
   External CPA firm performs an annual audit in accordance with professional standards. The purpose of the audit is to express an opinion on the FCCC’s financial statements.


   An outside consulting company, under contract with the FCCC, performs an annual stringent review of security for systems within which the portal operates. This consultant conducts an annual exit conference, issues an executive summary report, issues a detailed technical report and provides to FCCC Senior Management recommendations for improvement.

3. Internet Security Review (Quarterly):

   The FCCC is required by Visa/Mastercard, who provides credit card services for MFC, to undergo quarterly security reviews. The quarterly reviews focus on internet security and are performed by an outside consulting firm. Upon completion the FCCC is provided a certification for processing transactions. This certification is displayed on the MFC website.
4. SSAE No.16 (Annual):

The FCCC, as part of their risk assessment process, requested a Statement on Standards for Attestation Engagements (SSAE) No. 16 engagement. A SSAE No. 16 audit is widely recognized because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes. The FCCC plans to have a SSAE No. 16 engagement performed annually.

**Information and Communication:**

Management has established an organizational structure and has set a tone to help facilitate the communication of important business information. The FCCC has implemented various methods of communication to ensure that all employees understand their roles and responsibilities and to ensure that significant events are communicated in a timely manner. As mentioned previously, the FCCC has an organizational chart for the Technical Division that clearly depicts the lines of authority. The FCCC maintains written job descriptions for all staff. Each description includes the responsibility to communicate significant issues and pertinent information in a timely manner. The FCCC has formal meetings on a routine basis to discuss on-going projects associated with MFC. In addition, there are numerous ad-hoc meetings among management and staff for various reasons that may arise.

The FCCC has implemented an Information Technology Service Management (ITSM) framework and Information Technology Infrastructure Library (ITIL) best practices for all FCCC I.T. projects, including MFC. ITSM/ITIL is an internationally recognized best practice approach for managing I.T. projects. Selected staff have been trained and earned the ITSM/ITIL Foundation Certification.

The FCCC has implemented various methods of communication to ensure that user organizations (Clerks) understand the FCCC’s role and responsibilities in processing transactions. These communication channels also ensure that the users understand how to use and navigate the various systems administered by the FCCC. For example, the FCCC makes detailed training/procedures manuals available to those users participating in MFC. In addition, the FCCC conducts training classes for new Clerk staff. User organizations are encouraged to communicate questions and problems to the FCCC liaisons.

The MFC website contains clear and concise directions that allow the user to navigate through the system and perform inquiries and complete transactions. FCCC staff in the Service Center Function provides ongoing communication with customers. This function maintains records of problems reported by customers and incidents noted during processing. The Service Center Function also communicates information regarding training, changes in processing schedules, system enhancements, and other related information to the user organizations.

The FCCC maintains a contract with Hewlett Packard Business Continuity & Recovery Services Center (BCRSC). The FCCC outlines the equipment necessary to rebuild the current technical infrastructure to insure ongoing operations of critical systems within our environment in the
event of a major disaster necessitating the implementation of the FCCC Disaster Recovery (DR) plan. The designated BCRSC equipment, as per the contract is dedicated for use by the FCCC during a declared disaster and annually for testing purposes to insure operational readiness.

**Description of Information Systems:**

FCCC management has established processing procedures for the information system control environment. The systems and processes are defined as follows:

The FCCC IT environment currently consists of an operating environment that is located in the Organization’s office in Tallahassee, Florida. The office has an onsite server room that supports the company’s ethernet-based local area network (LAN) that is used by company employees and consists mainly of Microsoft Windows based servers (equipped with Intel processors) that are used for network authentication, file/print services, internet access, email service and database servers for the company applications. Workstations and laptop computers throughout the Organization have network connectivity or are stand-alone.

The FCCC IT environment is located inside a network consisting of various layers of industry standard firewalls to ensure that only authorized individuals are permitted access to the IT FCCC Network and other IT Systems. FCCC has high-speed leased communication lines to connect out to the Internet.

**System Data Backup Procedures**

The ability to restore system data after the interruption of services, corruption of data, or failure of computer services is vital to the ability to continue to provide services to users. To ensure that mission, production data is available for restoration in the event of normal production system failure or disaster. The following schedule of backups and controls are currently being performed – daily, monthly, and annual.

Data is backed-up on premise via an EMC Networker backup server. The database and network documents are backed up to a local Data Domain Disk Vault and replicated to a remote Data Domain Disk Vault that is located in Alpharetta, Georgia. The Systems Engineering staff is responsible for verifying that all backup jobs have been completed successfully. In addition, these individuals are responsible for updating all backup information including schedules, devices and procedures.

**Physical and Environmental Protection**

The FCCC facility is located at 3544 Maclay Blvd, Tallahassee, Florida. Controls are in place to provide for intrusion, fire detection and environmental protection.

Security and fire systems are utilized to protect against intrusion and fire. The Security System Vendor monitors the system for both fire and intrusion. In addition, the vendor periodically inspects and maintains the system. The vendor has the ability to provide records of who activates and deactivates the intrusion system.
Camera systems are in place to monitor access to the building and other sensitive areas. This is monitored by an FCCC staff member during regular business hours. The system also allows images to be recorded for viewing subsequent to an incident being reported.

Access to the facility is limited with only one public entrance which is located at the front of the building. Access is controlled and monitored by the company’s receptionist. Clients and visitors must sign-in at the receptionist’s desk and are provided with a visitor’s badge that must be worn at all times. Clients and visitors must be escorted by an FCCC staff member in order to gain access to the second floor. The server room is located on the second floor. The room is secured and access is restricted to a limited list of key employees. Anyone accessing the server room must be accompanied by one of the authorized individuals, log their time, and record their reason for access. The server room features dedicated air conditioning units to protect the room from heat and humidity.

Fire extinguishers are located throughout the building and server room and are maintained on a regular basis by the vendor. An FM-200 Fire Extinguishing System equipped with smoke and heat detectors is installed in the FCCC server room.

Uninterrupted power supply units (UPS), with a constant load, are installed to protect the file servers and telecommunications equipment from power surges and loss of data from sudden power outages. The UPS systems are tested and inspected on a periodic basis.

A diesel generator is located on the company grounds to provide an uninterrupted power solution in the event of a longer term power outage. The generator runs weekly self-tests which are monitored by FCCC personnel. The generator is also inspected and maintained on a regular basis.

Network Security

FCCC maintains network diagrams illustrating the physical and logical connections between interconnecting equipment. The communications equipment and servers are labeled to facilitate cross-reference to these diagrams.

To protect FCCC data and information, a Cisco security appliance is utilized. The security appliance combines dynamic network address translation and packet filtration. Security groups and departments are separated using Virtual Local Area Networks (VLANs) in order to provide an additional layer of security.

Antivirus protection has been implemented at FCCC on the server, email gateway and workstation levels to protect company data from infection by malicious code or viruses. The antivirus software is actively monitoring data and traffic with virus signature definitions that are updated on an active basis.
Logical Security

Logical access controls are utilized to restrict access to the FCCC network, systems, applications and remote access. The IT Department has administrative access rights to the network and has responsibility for assigning and maintaining access rights to the network and applications.

The addition and deletion of user accounts is performed based on requests for new hires and terminations. FCCC management has the authority to add new employees or modify existing employees’ access rights. Requests are initiated by the HR department and communicated to the IT Department for processing.

Management provides notification of terminated employees to the IT Support team. The terminated employee’s access credentials are disabled immediately.

Access to the FCCC network requires a user to authenticate by entering in their network user ID and a confidential password. User ID composition is based on a combination of the user parameters including their first and last names. Security parameters for the network password include:

- Minimum password length - 8 alphanumeric characters
- Must contain at least one number or special character and one capital letter
- Password expiration – 90 days
- Password history is maintained for 10 passwords
- Account lockout after 5 invalid attempts

Virtual Private Network (VPN) access to the FCCC network is available using a Secured Socket Layer (SSL) VPN solution. Users must install a Cisco client on their device to authenticate and gain encrypted VPN access to the FCCC network. Secondary user credentials are also required to create the VPN connection.

As an additional layer, VPN access is restricted in a Windows Active Directory (AD) and security parameters for remote access password management are controlled by the FCCC Domain Security Policy.

Internet Data Authenticity

Since online security remains a primary concern of many customers, FCCC has taken certain steps to ensure that any data transmitted to the application servers is done so in a secure manner. The MFC Portal website that is hosted at FCCC is: https://www.myfloridacounty.com.

To ensure that sensitive data transmitted to the above web site is protected against disclosure to third parties, the website uses Hypertext Transfer Protocol with Privacy, which connects with RSA 256 bit secure socket layer (SSL) encryption. FCCC uses a trusted authority (Secure Server Certificate Authority) as the certificate authority to reassure online customers.
that the website they are visiting is an authentic site. Website customers are authenticated against the application server upon logging into their respective application.

Website customers are required to use a user ID and password to gain access to their accounts. To provide additional customer protection, the web application includes a session idle timeout feature that will automatically end an online session if the session remains idle for a specified time period.

**Description of Functional Services and Processing:**

**Account Setup (Filer):**

Customers can pay child support, traffic citations and order official records by accessing the MFC log-in page at [www.myfloridacounty.com](http://www.myfloridacounty.com). Customers are required to enter necessary information (case, citation no., credit card information, etc.) before the transaction will be accepted.

Child support customers have the option of establishing an account with MFC. By establishing an account, the customer:

- has the option to pay by e-check or credit card.
- no longer has to add case information or credit card information each time. All relevant information is stored in a safe and secure environment.
- has the ability to review account transaction history

To establish an account, customers are prompted to complete all available fields on the screen. Employers can set-up a corporate account for easy online payment of employees’ child support. Payments can be made with either a credit card or electronic debit from the employers’ corporate bank account. The system prompts the user if required information is missing. The transaction cannot be submitted with missing data. Prior to the transaction being processed, the system requests the customer verify the accuracy of the payment information and associated service fee.

Once the customer selects the submit button, the credit card or e-check routing information is verified with the appropriate institution. This authorization process automatically rejects payments made using an invalid credit card number. The following mechanisms are utilized when authorizing transactions:

- **Credit Card Verification Value (CVV):** is a 3 to 4 digit security code found on the back of the credit card. The filer must enter this information.
- **Address Verification System (AVS):** is used to verify the identity of the person claiming to own the credit card. The system will check the billing address of the credit card provided by the user with the address on file at the credit card company.
- Customers receive a confirmation upon successful filing.
Accounting and Reconciliation of Portal Transactions:

All transaction data is captured by MFC database (“payment engine”). This includes the order number, order date, time stamp, transaction history, status, description of service, price and quantity.

Transactions that flow through MFC are sequentially numbered. Orders are given a unique identifier at the point that users initiate transactions.

The FCCC utilizes an interface called the “IPAS reconciliation system” (Access Database) between MFC and the general ledger accounting system. This process provides for an efficient and effective reconciliation of deposits (receipts) and disbursement transactions. This system produces activity summary reports that are used for reconciliation purposes. Written procedures are in place that outlines the processes for successful reconciliation.

The FCCC Accounting function performs monthly bank reconciliations of MFC bank accounts. The payment engine provides the financial data and reports for the "book side" of the bank reconciliation. Accordingly, the bank reconciliations provide control over both safeguarding assets and data integrity for the processing of financial data through MFC. Once completed, the bank reconciliations are reviewed by FCCC Senior Management. The FCCC Banking Function performs a daily confirmation/verification process on MFC System ACH Files. The purpose of this process is to verify that the transfer amount according to the bank agrees to the MFC Payment Engine/Database. This verification process is documented on the "ACH File Transfer Log". This document includes, but is not limited to, the following items by service: 1) confirmation number 2) date of the file 3) dollar amount of the file 3) staff initials performing the process.
Control Objectives and Related Controls:

The MFC control objectives and related controls are included in Section III of this report, Description of Controls, Control Objectives, Related Controls, and Testing of Operating Effectiveness. This is to eliminate the redundancy that would result from listing them in this section and repeating them in Section III. Although the control objectives and related controls are included in Section III, they are nevertheless, an integral part of the FCCC’s description of controls.

Types of Tests Performed

The types of tests performed on the controls specified in Section III are described below:

1. **Inspection**

   Inspected documents and reports indicating performance of the control. This includes, among other things:

   - Examined documents or records for evidence of performance such as the existence of initials or signatures.
   - Examined output control procedures and resulting documents relative to specific transactions to ensure accurate and timely updates of records were achieved.
   - Inspected reconciliations and management reports that age and quantify reconciling items to assess whether balances and reconciling items are properly monitored, controlled and resolved on a timely basis.
   - Examined management exception reports to assess whether exception items are properly monitored, controlled and resolved on a timely basis.
   - Examined source documentation and authorizations to verify propriety of transactions processed.
   - Inspected system documentation, such as operation manuals, flow charts and job descriptions.

2. **Reperformance**

   Re-performed the processing of the control to ensure the accuracy of its operation.

3. **Observation**

   Observed application of specific controls as performed by the FCCC personnel as represented.

4. **Inquiry**

   Inquiries seeking relevant information or representation from personnel were performed to obtain, among other things; knowledge and additional information regarding the control.
SECTION III.
DESCRIPTION OF CONTROLS, CONTROL OBJECTIVES, RELATED CONTROL PROCEDURES, AND TESTS OF OPERATING EFFECTIVENESS
### SECTION III.
ORGANIZATIONAL AND ADMINISTRATIVE CONTROLS

#### CONTROL OBJECTIVE 1: The organization maintains a strong control environment that sets the tone of the organization with respect to the control consciousness of its well-being.

<table>
<thead>
<tr>
<th>Description of Controls</th>
<th>Test of Controls</th>
<th>Test Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>The FCCC maintains a high level of control consciousness and oversight of various systems. Specifically, the FCCC has the following audits/reviews:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Annual financial statement audits</td>
<td>1. Inspected reports and correspondence from each audit/review.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>B. Annual technical security review</td>
<td>2. Interviewed FCCC management about their policies for maintaining appropriate control consciousness.</td>
<td></td>
</tr>
<tr>
<td>C. Quarterly technical security with respect to internet security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D. Annual SSAE No. 16 Type II Engagement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Routine meetings are held to discuss special processing requests, operational performance and the development and maintenance of projects.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Interviewed FCCC management about routine meetings that occur related to MFC.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>2. Inspected documents from meetings (correspondence, agendas, minutes, etc).</td>
<td></td>
</tr>
<tr>
<td>FCCC management provides oversight for system security.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Inquired to management about system security.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>2. Inspected most recent Security Consulting Report.</td>
<td></td>
</tr>
<tr>
<td>Written position descriptions are maintained by the FCCC. These are periodically updated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Inspected job descriptions for all employees involved with MFC activities.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>2. Interviewed employees to verify accuracy of documents.</td>
<td></td>
</tr>
</tbody>
</table>
### SECTION III.
**ORGANIZATIONAL AND ADMINISTRATIVE CONTROLS**

**CONTROL OBJECTIVE 1:** The organization maintains a strong control environment that sets the tone of the organization with respect to the control consciousness of its well-being.

<table>
<thead>
<tr>
<th>Description of Controls</th>
<th>Test of Controls</th>
<th>Test Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Written performance evaluations are administered on an annual basis. These evaluations include stated goals and objectives. Performance evaluations are reviewed by Senior Management and become part of the employees’ personnel file.</td>
<td>1. Inquired to management and discussed the evaluation process. Verified that evaluations take place on an annual basis.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>2. Reviewed a sample of annual performance evaluations for those employees involved with the MFC system. Verified the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Annual performance evaluations were present in the file</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Each evaluation was signed by the employee and member of management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Evaluation included the employees’ goals and objectives</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Evaluation contained feedback and constructive criticism</td>
<td></td>
</tr>
<tr>
<td>The Organization requires a signed contract (on file) from all Clerks prior to executing transactions.</td>
<td>1. Inquired to management that signed contracts are on file for each Clerk participating in MFC services.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Inspected a sample of MFC contracts to verify that the contract is complete and signed by both the FCCC and the respective Clerks.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>3. Inspected contracts to verify that it contained the service fee structure.</td>
<td></td>
</tr>
</tbody>
</table>
### SECTION III.
ORGANIZATIONAL AND ADMINISTRATIVE CONTROLS

**CONTROL OBJECTIVE 1:** The organization maintains a strong control environment that sets the tone of the organization with respect to the control consciousness of its well-being.

<table>
<thead>
<tr>
<th>Description of Controls</th>
<th>Test of Controls</th>
<th>Test Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCCC staff involved in MFC functions are competent and possess the necessary professional experience.</td>
<td>1. Interviewed FCCC management on policy for hiring practices.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>2. Reviewed background and technical experience information in employee’s personnel file (i.e. work experience, education, certifications, etc).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Interviewed staff to verify their background and technical experience.</td>
<td></td>
</tr>
<tr>
<td>Description of Controls</td>
<td>Test of Controls</td>
<td>Test Results</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>The FCCC is organized into separate functional areas to provide adequate segregation of duties.</td>
<td>1. See page 39 for the testing performed on segregation of duties.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>1. Inquired to Management that portal bank reconciliations are performed in a timely manner.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Verified that reconciling items were properly documented and that the FCCC provided reasonable explanations as to the nature of the reconciling items.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Verified that source documents existed and were available for all amounts on the bank reconciliations.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Verified the mathematical accuracy of the bank reconciliations selected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Requested the most recent bank reconciliation to verify that it was completed timely (within 30 days of month end).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. Inspected a sample of bank reconciliations to verify the required review and approvals were performed and documented.</td>
<td></td>
</tr>
</tbody>
</table>

The FCCC Accounting function performs monthly bank reconciliations of MFC bank accounts. MFC payment engine provides the financial data and reports for the "book side" of the bank reconciliation. Accordingly, the bank reconciliations provide control over both safeguarding assets and data integrity for the processing of financial data through MFC.

The bank reconciliations are reviewed by FCCC Senior Management.
**SECTION III. TRANSACTION PROCESSING AND RECONCILIATION**

**CONTROL OBJECTIVE 2:** Transactions that are processed through the MFC system are authorized, processed, recorded completely, accurately and timely.

<table>
<thead>
<tr>
<th>Description of Controls</th>
<th>Test of Controls</th>
<th>Test Results</th>
</tr>
</thead>
</table>
| Transactions that flow through MFC are sequentially numbered. Orders are given a unique identifier at the point that users initiate transactions. | 1. Interviewed management on the methodology in place to uniquely identify portal transactions. Verified that transactions are sequentially numbered.  
2. Inquired to management to verify that order numbers are established at the point a user attempts a transaction.  
3. Requested the first and last order numbers processed through MFC. Inspected a sample of transactions to verify that orders were accounted for and within the fiscal year. | No exceptions noted. |

| The user organizations (Clerks) have online 24/7 access to MFC system financial data and reports. | 1. Interviewed FCCC Management and staff to verify that Clerks have 24/7 access to MFC systems for relevant financial information.  
2. Reviewed FCCC training guide/procedure manuals to verify that guidance is available to clerks.  
3. Requested FCCC IT Management demonstrate the online 24/7 access. Confirmed that the Clerks have access to the system for relevant financial reports and information. | No exceptions noted. |
### SECTION III.
TRANSACTION PROCESSING AND RECONCILIATION

**CONTROL OBJECTIVE 2:** Transactions that are processed through the MFC system are authorized, processed, recorded completely, accurately and timely.

<table>
<thead>
<tr>
<th>Description of Controls</th>
<th>Test of Controls</th>
<th>Test Results</th>
</tr>
</thead>
</table>
| The FCCC utilizes an interface called the “IPAS reconciliation system” (Access database) between MFC and the accounting system. This process provides for an efficient and effective reconciliation of deposit (receipts) and disbursement transactions. This system produces activity summary reports that are used for reconciliation purposes. Written procedures are in place for using the IPAS reconciliation system. | 1. Interviewed the FCCC Management to verify that this is performed.  
2. Inspected reports generated from the system. Verified the accuracy and completeness of the reports.  
3. Traced selected receipt/disbursement transactions from MFC database through to the accounting system and bank statements.  
4. Reviewed reconciliation procedures. Verified the consistency with actual procedures observed. | No exceptions noted. |

The FCCC Banking function scans physical paper checks for certain transactions received in the mail daily. The scanning process electronically sends a deposit to MFC bank accounts. All other payments made on-line via credit card or e-check in MFC are automatically sent as a deposit to MFC bank accounts through MFC payment engine.

- All Checks are logged by the mail clerk.
- Once checks are scanned and deposited, a report is produced that acts as a deposit slip. This is reconciled with the bank.

| | 1. Inquired to FCCC Banking Administrator to gain understanding and verify this process occurs on a daily basis.  
2. Reviewed procedures for scanning of the checks.  
3. Inspected sample mail logs and deposit documentation. | No exceptions noted. |
### SECTION III.
TRANSACTION PROCESSING AND RECONCILIATION

**CONTROL OBJECTIVE 2:** Transactions that are processed through the MFC system are authorized, processed, recorded completely, accurately and timely.

<table>
<thead>
<tr>
<th>Description of Controls</th>
<th>Test of Controls</th>
<th>Test Results</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Interviewed the Banking Administrator to gain understanding of this process. Verified that this process occurs on a daily basis.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>2. Observed the Banking Administrator perform the daily ACH file confirmation process for selected dates.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Inspected daily logs for a selected month to verify the process had been performed and documented.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Requested detailed portal payment engine reports and portal bank statements. Verified that detailed disbursement reports agreed to the transfer amounts listed on the bank statements.</td>
<td></td>
</tr>
<tr>
<td>The FCCC Banking Function performs a daily confirmation/verification process on portal ACH files. The purpose of this process is to verify that the transfer amount according to the bank agrees to MFC Payment Engine/Database. This verification process is documented on the &quot;ACH File Transfer Log&quot;. This document includes, but is not limited to, the following items by service: 1) confirmation number 2) date of the file 3) dollar amount of the file 4) staff initials performing the process.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Reviewed procedures for performing the manual review process.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>Child support credit card transactions flow through the Cybersource Decision Manager Fraud System and MFC Fraud Prevention System. These systems generate case management review reports which display all orders that are outside certain established parameters (based on a list of fraud parameters). When a child support payment is outside the established parameters, it enters a manual review process. FCCC performs a series of steps to determine whether payment is valid.</td>
<td>2. Interviewed FCCC IT staff on procedures used to manually review suspect criteria, including descriptions of the criteria.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Inspected a sample of Cybersource case management review reports.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Observed FCCC IT staff performing the manual review process.</td>
<td></td>
</tr>
</tbody>
</table>
### SECTION III. TRANSACTION PROCESSING AND RECONCILIATION

**CONTROL OBJECTIVE 2:** Transactions that are processed through the MFC system are authorized, processed, recorded completely, accurately and timely.

<table>
<thead>
<tr>
<th>Description of Controls</th>
<th>Test of Controls</th>
<th>Test Results</th>
</tr>
</thead>
</table>
| MFC includes banking controls for credit card transactions. This authorization process automatically rejects payments made using an invalid credit card number. The following mechanisms are utilized when authorizing transactions:  
  - Credit Card Verification Value (CVV)  
  - Address Verification System (AVS) | 1. Inquired to FCCC Management and staff on the Cybersource authorization process.  
  2. Observed FCCC staff attempting to make several credit card payments on portal using invalid credit card numbers. | No exceptions noted. |
## SECTION III.
**PHYSICAL SECURITY**

**CONTROL OBJECTIVE 3:** Controls provide reasonable assurance that physical access to computer equipment, storage media, and program documentation is restricted to properly authorized individuals.

<table>
<thead>
<tr>
<th>Description of Controls</th>
<th>Test of Controls</th>
<th>Test Results</th>
</tr>
</thead>
</table>
| Electronic badge devices control access to all entrances to the building. The main entrance remains unlocked during business hours (8:00am-5:00pm) for visitors. | 1. Observed that all entrances (with exception of main entrance) remained locked at all times.  
2. Observed the presence of electronic key devices at the entrances to the FCCC building. | No exceptions noted. |
| Electronic badge devices control the access to the FCCC server room. Only specified technical staff have access to this secured location. | 1. Verified the server room is locked.  
2. Observed the presence of an electronic key device at the entrance of the server room. | No exceptions noted. |
| Access to the server room is restricted to only members of the FCCC Information Technology Department who are responsible for administration and support of the internal network and the technical environment. | 1. Inspected a listing of individuals with access to the server room. Verified that only current employees have access.  
2. Observed non-authorized staff unsuccessfully attempting access. | No exceptions noted. |
| Automated electronic reports are periodically generated for monitoring of traffic in and out of the FCCC building and server room. | 1. Inspected report generated from the system that lists all traffic in and out of the building and server room. | No exceptions noted. |
| All visitors must use the main entrance of the FCCC facility. FCCC visitors are required to sign a visitor's log upon entering the facility. In addition, all visitors are provided visitor badges. | 1. Verified the front entrance is the only un-locked entrance during normal office hours.  
2. Observed visitors entering and exiting the building.  
5. Observed receptionist providing visitor badges. | No exceptions noted. |
### SECTION III. PHYSICAL SECURITY

**CONTROL OBJECTIVE 3:** Controls provide reasonable assurance that physical access to computer equipment, storage media, and program documentation is restricted to properly authorized individuals.

<table>
<thead>
<tr>
<th>Description of Controls</th>
<th>Test of Controls</th>
<th>Test Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>An escort (FCCC staff) is called to greet their visitors in the lobby.</td>
<td>1. Verified through observation that guests are accompanied by a FCCC staff employee at all times.</td>
<td>No exceptions noted.</td>
</tr>
</tbody>
</table>
| The FCCC conducts employment background checks and criminal history checks on external candidates selected to fill vacant positions. | 1. Inspected Human Resource procedures to verify that background checks are required for all new employees.  
2. Inspected background/criminal history check log for all employees hired in the audit period.  
3. For selected employees, inspected background/criminal history check documentation. | No exceptions noted. |
| A security consulting company, under contract with the FCCC, performs an annual stringent review of the FCCC system's security within which MFC operates. The consulting company conducts an exit conference, issues an executive summary report, issues a detailed technical report and provides recommendations for improvement to FCCC Senior Management. | 1. Inquired to FCCC Management about the Security Consulting engagement and method of addressing recommendations.  
2. Inspected the most recent security consulting report. | No exceptions noted. |
| FCCC has an alarm system in place to monitor and notify the company of any unauthorized access. The alarm system is serviced annually by the vendor to ensure that the system is operating correctly. | 1. Inspected contract with vendor to verify the existence of alarm system.  
2. Performed a walkthrough of the building to verify the existence of an alarm system. | No exceptions noted. |
### SECTION III. PHYSICAL SECURITY

**CONTROL OBJECTIVE 3**: Controls provide reasonable assurance that physical access to computer equipment, storage media, and program documentation is restricted to properly authorized individuals.

<table>
<thead>
<tr>
<th>Description of Controls</th>
<th>Test of Controls</th>
<th>Test Results</th>
</tr>
</thead>
</table>
| Camera system is used to monitor building entrances and other sensitive areas within the building. | 1. Interviewed management to verify that a camera system was in place.  
2. Observed cameras in place throughout the building.  
3. Observed sample of recorded videos to verify functioning properly. | No exceptions noted. |
| The FCCC is required by the credit card companies, who provide credit card services for MFC, to undergo quarterly systems security reviews. The quarterly reviews focus on internet security issues. | 1. Inquired to FCCC Management about the work performed by this company.  
2. Inspected reports to ensure that the FCCC passed the security review.  
3. Verified that the FCCC has posted certification of successful completion on the website. | No exceptions noted. |
### SECTION III.
ENVIRONMENTAL CONTROLS

**CONTROL OBJECTIVE 4:** Controls provide reasonable assurance that the physical environmental devices are installed to adequately protect the servers, network equipment, and storage media.

<table>
<thead>
<tr>
<th>Description of Controls</th>
<th>Test of Controls</th>
<th>Test Results</th>
</tr>
</thead>
</table>
| Multiple air-conditioning units are present in order to regulate the temperature in the FCCC server room. Periodic inspections and preventative maintenance procedures are performed on the equipment. | 1. Observed the FCCC server room and verified that air conditioning systems are present in the server room.  
2. Verified that a maintenance agreement exists on the air conditioning systems. | No exceptions noted. |
| An FM-200 Fire Extinguishing System, equipped with smoke and heat detectors, is installed in the FCCC server room. FM-200 equipment is under service agreement for semi-annual inspections and receives preventative maintenance as required. | 1. Observed the FCCC server room and noted the FM-200 release heads were present throughout the server room.  
2. Inspected maintenance agreements. | No exceptions noted. |
| An uninterruptible power supply system (UPS) has been installed to protect against loss of data during a power failure and is subjected to periodic testing and maintenance. | 1. Tourd facility and verified the presence and location of UPS.  
2. Inspected UPS maintenance and test records. | No exceptions noted. |
| A diesel generator is installed at the FCCC facility to provide backup power in the event of a power failure. Diesel generators are configured to self-exercise periodically and are under a preventative maintenance agreement. | 1. Observed the diesel generator at the FCCC facility and verified that a diesel generator was in place to provide backup power to the facility.  
2. Inspected the maintenance agreement and verified that the generator is inspected on an annual basis. | No exceptions noted. |
**SECTION III. NETWORK SECURITY AND INTERNET ACCESS**

**CONTROL OBJECTIVE 5:** Controls provide reasonable assurance that access to systems (logical) and through internet is restricted to properly authorized individuals.

<table>
<thead>
<tr>
<th>Description of Controls</th>
<th>Test of Controls</th>
<th>Test Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>A network diagram illustrates the physical and logical connections of FCCC information systems.</td>
<td>1. Inspected the FCCC System/Network Diagram.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>Communication equipment and servers are labeled to facilitate cross-reference of these diagrams.</td>
<td>1. Inquired to management about the FCCC systems/networks.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>2. Observed the server room and compared physical equipment (labeled) to the network diagram.</td>
<td></td>
</tr>
<tr>
<td>Firewalls are embedded in the system to prevent unauthorized access. Further, various FCCC functions are separated into VLANs that provide access restrictions. The system is capable of generating firewall logs of activity.</td>
<td>1. Verified inclusion of firewalls on system diagram.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>2. Observed the FCCC produce firewall logs for a specific time frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Verified that this log reflects all attempted access to the systems.</td>
<td></td>
</tr>
<tr>
<td>Antivirus protection has been implemented at FCCC server, email gateway, and workstation levels to protect company data from infection by malicious code or viruses.</td>
<td>1. Verified antivirus software exists on servers and a selection of workstations.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>3. Obtained log of periodic virus scans on servers and workstations.</td>
<td></td>
</tr>
</tbody>
</table>
### SECTION III.
**NETWORK SECURITY AND INTERNET ACCESS**

**CONTROL OBJECTIVE 5:** Controls provide reasonable assurance that access to systems (logical) and through internet is restricted to properly authorized individuals.

<table>
<thead>
<tr>
<th>Description of Controls</th>
<th>Test of Controls</th>
<th>Test Results</th>
</tr>
</thead>
</table>
| The FCCC Internet Portal contains a Digital Certificate (SSL - Web Certificate). Certificates have been issued by a known certificate authority and are accessible on the website. | 1. Inspected certificate documentation provided from vendor. Verified that the current certificate was current and had not expired.  
2. Observed website to verify that the digital certificate is displayed. | No exceptions noted. |
| Windows and Network password management controls include the following:  
- Minimum password length.  
- Character components.  
- Password expiration/change frequency  
- Invalid password attempts  
- Password storage. | 1. Obtained the domain security policy and confirmed the parameters match control details and Security Policies & Procedures document.  
2. Observed employee unable to log into system with invalid passwords.  
3. Viewed history of password expiration. | No exceptions noted. |
| Change requests (moving, adding, changing, etc) are initiated by the Human Resource Function and communicated to the IT Department. | 1. Confirmed through corroborative inquiry with Management of IT that the control activity is in place. | No exceptions noted. |
| The Human Resource Function notifies the IT Department of all new employees and terminations. | 1. Confirmed through corroborative inquiry with Management of IT that the control activity stated is in place.  
2. Obtained a list of terminated employees during audit period. Inspected the Windows Active Directory (AD) to verify that all terminated employees were disabled or eliminated. | No exceptions noted. |
### SECTION III.
NETWORK SECURITY AND INTERNET ACCESS

**CONTROL OBJECTIVE 5:** Controls provide reasonable assurance that access to systems (logical) and through internet is restricted to properly authorized individuals.

<table>
<thead>
<tr>
<th>Description of Controls</th>
<th>Test of Controls</th>
<th>Test Results</th>
</tr>
</thead>
</table>
| FCCC encrypts the hard drives of laptops to prevent unauthorized access in the event of loss or theft. | 1. Observed the managed console of the drive encryption software.  
2. Randomly selected laptops to verify that encryption is active and functioning properly. | No exceptions noted. |
| FCCC engages an outside consulting company to perform an annual stringent review of security for FCCC systems. This company conducts an annual exit conference, issues an executive summary report, and issues a detailed technical report that includes recommendations to management. | 1. Inspected most recent annual security report.  
2. Verified that the report did not identify major problems or weaknesses in the system.  
3. Verified that recommendations were provided to management for improvement. | No exceptions noted. |
| The FCCC is required by the credit card companies to undergo quarterly security reviews. The quarterly reviews focus on internet security and are provided by an outside vendor. | 1. Read quarterly review reports to ensure the FCCC passed security review.  
2. Verified that the FCCC has posted certification of successful completion on the website. | No exceptions noted. |
| FCCC uses Microsoft Window Server Update Services (WSUS) to manage and install Microsoft critical and security patches. | 1. Observed FCCC gain access to the WSUS software.  
2. Inspected reports of managed FCCC servers and workstations. | No exceptions noted. |
## SECTION III.
### NETWORK SECURITY AND INTERNET ACCESS

**CONTROL OBJECTIVE 5:** Controls provide reasonable assurance that access to systems (logical) and through internet is restricted to properly authorized individuals.

<table>
<thead>
<tr>
<th>Description of Controls</th>
<th>Test of Controls</th>
<th>Test Results</th>
</tr>
</thead>
</table>
| FCCC uses third party software to monitor the websites and portals to confirm sites are operating and that connections can be made. | 1. Confirmed through corroborative inquiry with IT Management that the control activity stated is in place.  
2. Observed access to the monitoring software and confirmed it was active.  
3. Inspected periodic email reports sent to FCCC IT that reflects monitoring results and any potential issues with the FCCC websites. | No exceptions noted. |
2. Verified managed software is present with PIN enforcement settings. | No exceptions noted. |
| A Uniform Resource Locator (URL) filter is in place to detect and block potentially malicious links from being accessed. | 1. Verified with management the existence of the URL filtering device.  
2. Inspected sample logs of blocked potentially malicious URLs. | No exceptions noted. |
| FACC assigns NAVISION (Accounting System) access security levels based on the required functions of the respective users, with access being appropriately restricted for each user. | 1. Reviewed and evaluated for reasonableness the FACC’s Accounting System Access Control Narrative.  
2. Observed NAVISION users to ascertain the limits of their respective access and to confirm their access was restricted in accordance with the Control Narrative. | No exceptions noted. |
SECTION III. INFORMATION AND COMMUNICATION

CONTROL OBJECTIVE 6: Controls provide reasonable assurance that the information and communication component includes the procedures and records established by the FCCC to initiate, process, and report the user organizations’ (Clerks) transactions and maintain accountability for the transactions.

<table>
<thead>
<tr>
<th>Description of Controls</th>
<th>Test of Controls</th>
<th>Test Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCCC has established and maintains written policies and procedures for various tasks and activities associated with MFC.</td>
<td>1. Inspected written policies and procedures that pertain to MFC.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>2. Observed certain processes to verify consistency with written procedures.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Inspected FCCC organizational chart as it relates to MFC. Obtained explanations from the FCCC on the various functions presented.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. During the course of the audit, observed various positions to verify work performed was consistent with organizational chart and job descriptions.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Inquired to management about the existence of routine technical meetings.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>2. Inspected documentation from meetings (correspondence, agendas, minutes, etc).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Inquired to management about the existence of ITSM/ITIL framework and best practices for FCCC technical projects.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Inspected ITSM/ITIL related documents.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>3. Inspected employee certifications in ITSM/ITIL.</td>
<td></td>
</tr>
</tbody>
</table>
SECTION III
INFORMATION AND COMMUNICATION

**CONTROL OBJECTIVE 6:** Controls provide reasonable assurance that the information and communication component includes the procedures and records established by the FCCC to initiate, process, and report the user organizations’ (Clerks) transactions and maintain accountability for the transactions.

<table>
<thead>
<tr>
<th>Description of Controls</th>
<th>Test of Controls</th>
<th>Test Results</th>
</tr>
</thead>
</table>
| The FCCC produces several reports that assist management in the monitoring objective of MFC. These are distributed to key management and staff and are discussed at routine meetings. | 1. Confirmed through corroborative inquiry that the control activity stated is in place.  
2. Inspected samples of each report and documented its nature and purpose. | No exceptions noted. |
| The FCCC has a Service Center function that provides on-going support for the existing FCCC applications. | 1. Inquired to management as to the nature of the FCCC Service Center.  
2. During the course of the audit, observed the Service Center staff performing their tasks.  
3. Inspected tracking logs or other documentation from the database that tracks issues arising from customers. | No exceptions noted. |
| The FCCC provides necessary training to Clerks engaged in services offered by MFC. This is to ensure that the Clerks understand how to use and navigate the various systems administered by the FCCC (including MFC). | 1. Inquired to management as to the type of training/operational procedures in place.  
2. Inspected manuals/procedures made available to Clerks for the various components of MFC. | No relevant exceptions noted. |
| Procedure Guides have been developed for the users of MFC. This is to ensure that the users understand how to navigate the system. | 1. Inquired to management as to the type of training/operational procedures in place.  
2. Inspected procedure manuals made available to users of MFC. | No exceptions noted. |
### SECTION III.

#### SEGREGATION OF FUNCTIONS (INTERNAL)

**CONTROL OBJECTIVE 7:** Controls provide reasonable assurance that FCCC activities are organized to provide internal segregation of functions.

<table>
<thead>
<tr>
<th>Description of Controls</th>
<th>Test of Controls</th>
<th>Test Results</th>
</tr>
</thead>
</table>
| The FCCC is organized into separate functional areas to provide adequate separation of duties. | 1. Reviewed job descriptions and organizational chart noting the degree of separation within the FCCC.  
2. Interviewed management and staff to determine adherence to the organizational charts and policies. For example, the accounting department should be separate from system programming and operations.  
3. Observed various duties/ functions being performed by the FCCC staff. | No exceptions noted. |
| The FCCC maintains an organizational chart for the Technical Division that clearly depicts lines of authority. | 1. Inspected FCCC organizational chart as it relates to MFC. Obtained explanations from the FCCC on the various functions presented.  
2. During the course of the audit, observed various positions to verify work is performed consistent with organizational chart and job descriptions. | No exceptions noted. |
| FCCC operations personnel do not perform programming functions. Programming personnel do not perform operations duties. | 1. Reviewed the IT (Information Technology) organization chart noting the degree to which operations and programming functions are segregated.  
2. Interviewed computer operations management to determine adherence to policy. | No exceptions noted. |
### SECTION III. SEgregation of Functions (Internal)

**CONTROL OBJECTIVE 7:** Controls provide reasonable assurance that FCCC activities are organized to provide internal segregation of functions.

<table>
<thead>
<tr>
<th>Description of Controls</th>
<th>Test of Controls</th>
<th>Test Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Programming personnel do not initiate or authorize transactions.</td>
<td>1. Reviewed the policies and procedures of FCCC.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>Written job descriptions have been prepared for FCCC personnel and are periodically updated.</td>
<td>1. Reviewed employee job descriptions for those employees involved with MFC.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>2. Interviewed management and employees to verify accuracy of these documents.</td>
<td></td>
</tr>
</tbody>
</table>
## SECTION III.
SEgregation OF Functions (EXTERNAL)

**CONTROL OBJECTIVE 8:** The FCCC and User Organizations (Clerks) are segregated.

<table>
<thead>
<tr>
<th>Description of Controls</th>
<th>Test of Controls</th>
<th>Test Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCCC is physically separate from the user organizations (Clerks) for which it performs processing.</td>
<td>1. Reviewed policies of the organization and contractual obligations that exist between FCCC and user organizations.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td>The relationship between the FCCC and user organizations is contractual in nature.</td>
<td>2. Reviewed policies of FCCC and contractual obligations that exist between FCCC and user organizations.</td>
<td>No exceptions noted.</td>
</tr>
</tbody>
</table>
## SECTION III
### SERVICE FEE SCHEDULE

**CONTROL OBJECTIVE 9:** Controls provide reasonable assurance that service fees are properly charged and are in accordance with contracts, laws and regulations.

<table>
<thead>
<tr>
<th>Description of Controls</th>
<th>Test of Controls</th>
<th>Test Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>MFC has an approved (contractual) service fee schedule governing on-line transactions.</td>
<td>1. Inspected the uniform MFC service fee schedule.</td>
<td>No exceptions noted.</td>
</tr>
<tr>
<td></td>
<td>2. Verified approval of the service fees by the Board.</td>
<td></td>
</tr>
</tbody>
</table>
| MFC has system parameters (source code) for specific transactions in accordance with the service fee schedule. | 1. Randomly select transactions occurring during the audit period.  
2. Inspected order detail report generated directly from MFC system.  
3. Recalculated the service fee(s) for each order to verify that MFC charged the customer correctly. | No exceptions noted.          |
| Users are informed prior to submitting on-line payment of the service fee charged. In addition, the customer is requested to confirm order (payment information). | 1. Inspected website as user attempts to make a payment. Verified that the service fee is presented prior to submitting order. Verified that customer is requested to confirm order. | No exceptions noted.          |
## SECTION III.
### DATA BACKUP AND RECOVERY

**CONTROL OBJECTIVE 10:** Controls provide reasonable assurance that Backup and Recovery procedures are available to preserve the integrity of programs and data files.

<table>
<thead>
<tr>
<th>Description of Controls</th>
<th>Test of Controls</th>
<th>Test Results</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Inspected automated script utilized by FCCC staff in performing the backup.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Inquired to management about the system and the backup schedule.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Inspected the FCCC system diagram/flowchart to understand the various components, servers, databases and etc.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Observed a selection of backup logs for various servers identified on the network diagram.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Performed a backup of randomly sampled files.</td>
<td>No exceptions noted.</td>
</tr>
</tbody>
</table>

The following schedule of backups and controls are being performed:

- Daily
- Monthly
- Annual

Backups are performed utilizing a custom script that has been implemented on the server.

The backup process is performed in accordance with detailed written procedures.

|                         | 1. Inquired to management about the backup procedures and associated processes. | No exceptions noted. |
|                         | 2. Reviewed the backup schedule in place for the FCCC server and data files.    |              |
|                         | 3. Inspected a selection of backup logs to verify compliance with procedures.    |              |

Recoveries are performed on a periodic basis.

|                         | 1. Inquired to management about the recovery process procedures.                | No exceptions noted. |
|                         | 2. Performed a recovery of randomly sampled files.                             |              |