

# REPORT ON CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS (SSAE NO. 16) FOR

# **CLERC System**

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



LANIGAN & ASSOCIATES, PC CERTIFIED PUBLIC ACCOUNTANTS

# TABLE OF CONTENTS

SECTION I.	INDEPENDENT SERVICE AUDITOR'S REPORT	1
SECTION II.	GENERAL DESCRIPTION OF THE CLERC SYSTEM CONTROL STRUCTURE AND OPERATIONS	5
	Florida Association of Court Clerk's Assertion	6
	Overview of the CLERC System	8
	General Description of the CLERC System Control Structure1	0
	Description of Information Systems1	4
	General Description of the File Transmission Process1	7
	Control Objectives and Related Controls1	8
	Types of Tests Performed1	8
SECTION III.	DESCRIPTION OF CONTROLS, CONTROL OBJECTIVES, RELATED CONTROL PROCEDURES, AND TESTS OF OPERATING EFFECTIVENESS	9
	Objective 1. Organizational and Administrative Controls2	0
	Objective 2. Transmission of the State Disbursement Unit's Receipt File (270) and Exceptions File (375)2	.3
	Objective 3. Transmission of the County Repository, SDU and FDOR Files: A125 IV-D Collection, Non IV-D Disbursement (305), and OTC (950)	6
	Objective 4. Physical Security2	9
	Objective 5. Environmental Controls	2
	Objective 6. Network Security and Internet Access	3
	Objective 7. Information and Communication	7
	Objective 8. Segregation of Functions (Internal)	9
	Objective 9. Segregation of Functions (External)4	1
	Objective 10. Data Backup and Recovery4	2

# SECTION I. INDEPENDENT SERVICE AUDITOR'S REPORT

### LANIGAN & ASSOCIATES, P.C. CERTIFIED PUBLIC ACCOUNTANTS BUSINESS ADVISORS www.lanigancpa.com

# **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 CLERC 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.

2

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.

Independent Service Auditors' Report November 28, 2017

### Description of tests of controls

The specific controls tested and the nature, timing, and results of those tests are listed on pages 20-43.

# Restricted use

This report, including the description of tests of controls and results thereof on pages 20-43, is intended solely for the information and use of the FCCC, user entities of the CLERC System 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 CLERC SYSTEM CONTROL STRUCTURE AND OPERATIONS

# FLORIDA COURT CLERK AND COMPTROLLERS' ASSERTION

We have prepared the description of the CLERC System for user entities of the system 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 system 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 CLERC System 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 CLERC System, 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 system that each individual user entity of the system and its auditor may consider important in its own particular environment.
- B. 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 Linda Harmon, Acting Chief Financial Officer

# **OVERVIEW OF THE CLERC SYSTEM**

# CLERC System Description and Tasks:

The Florida Court Clerks and Comptrollers' (FCCC) is a not-for-profit corporation required by §61.181(2)(b)(1), Florida Statutes, to design, establish, operate, upgrade and maintain the CLERC System to automate the child support depositories operated by the 67 individual Clerks of Court. The purpose is to provide a single, unified data network for the transmission of child support information between the Clerks of Court, the Florida Department of Revenue (DOR) and Florida State Disbursement Unit (SDU).

The CLERC system consists of the CLERC Application, the FCCC Central Site and the FCCC Network. The CLERC System interfaces with the SDU, the DOR, and MyFloridaCounty.com and provides a common application for the processing of child support case information, receipts and disbursements. There are four basic types of child support cases:

- 1. IV-D (A child support enforcement action, involves DOR).
- 2. Non IV-D, required to be processed by SDU (the case is dated after 12/31/93 and includes an Income Deduction Order (IDO).
- 3. Non IV-D, not required to be processed by SDU, either due to a pre-1/1/94 date or because there is no IDO. These are able to be handled by the Clerks and not go through the SDU.
- 4. These are type 3's that the Clerk prefers to have the SDU process. Referred to as Contracted Disbursements.

Depositories are defined as the central governmental depository established pursuant to 61.181 Florida Statutes to perform depository functions related to the processing of child support payments.

The FCCC Central Site in conjunction with the CLERC Application and the FCCC Network, is responsible for coordination of all file transmissions between the DOR, SDU, and local Clerk depositories.

# CLERC System Functionalities:

- 1. Transmission of Title IV-D and Non Title IV-D Order Information: Clerk Depositories, utilizing the CLERC System, create and update child support case order information.
- 2. Transmission of Title IV-D and Non Title IV-D Address Change Information: Clerk Depositories, utilizing the CLERC System, update address information.
- 3. Non IV-D Case Validation of Receipt and Preparation of Disbursement: Clerk Depositories, utilizing the CLERC System, will receive receipt information in

advance of disbursement on all Non IV-D cases required to be processed by the SDU to validate receipt and prepare disbursement information for the SDU.

- 4. Transmission of Non Title IV-D Receipt Information: Clerk Depositories, utilizing the CLERC System, receive child support receipt information on all Non IV-D cases required to be processed by the SDU to update the official payment record.
- 5. Transmission of Title IV-D Receipt Information: Clerk Depositories, through the FCCC Central Site, receive Title IV-D receipt information from the SDU so that official records can be updated prior to the disbursement. The Clerk Depository will transmit Title IV-D receipt information to DOR through the FCCC Central Site.
- 6. Transmission of Over the Counter (OTC) Title IV-D and Non Title IV-D Data Files: Clerk Depositories, utilizing the CLERC System, EFT over the counter payments and transmits associated payment data to the SDU on those cases required to be processed by the SDU.
- 7. Data Sorting and Maintenance: The FCCC Central Site sends and receives files from Clerk Depositories, the SDU, and the DOR. Prior to transmission to a Clerk Depository, the FCCC Central Site is responsible for splitting receipt data by County for Title IV-D and Non Title IV-D cases that are required to be processed by the SDU.

# FCCC Lockbox Functionalities:

Lockbox is a name the FCCC has established for the receipt file originating at the SDU. The SDU collects child support payments throughout the day and then creates a master receipt file. This file is transmitted electronically to the FCCC Central Site. Upon arrival at the FCCC, the Lockbox is validated for any transmission errors and duplicate receipts while FCCC awaits confirmation via email with the file size and the total dollar amount for the day. Once the file is confirmed to be free of errors, the FCCC Central Site splits the file into separate individual receipt files and transmits them to each Clerk Depository.

The FCCC Quality Control function monitors the transmissions for any errors, interruptions, discrepancies, etc. If the FCCC has not received the receipt file from the SDU by the 3:15 PM deadline, the Service Center function notifies the Clerks with an explanation of the delay and an estimated time the file should arrive at the County. Subsequent to transmission of the Lockbox file, several other files (Misapplied, Insufficient Funds, Change of Address, Stop/Void Payment) are transmitted to each Clerk Depository. These are commonly referred to as the Exception Files.

Once the Clerk has received both the Lockbox file and the Exceptions file, receipt processing begins using the CLERC application. Once the Clerk has finished processing the receipt file, the CLERC application creates three separate files (A125 IV-D, OTC File, and Non IV-D Disbursement File) and transmits them to the FCCC Central Site. The files are merged into one file and then transmitted to both the FDOR and the SDU.

# GENERAL DESCRIPTION OF THE CLERC SYSTEM 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

### Structure of Organization:

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 CLERC 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 CLERC 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 the CLERC System.

The FCCC believes that it has good 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 authority 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, the FCCC conducts employment background checks and criminal history checks 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 consists 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 "Tests 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 CLERC System. The type of issues discussed include, but are not be limited to; 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 (Annually):

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.

2. Security Review (Annually):

An outside consulting company, under contract with the FCCC, performs an annual stringent review of security for FCCC systems within which the CLERC system 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 quarterly review focuses on internet security and is performed by an outside consulting firm. Upon completion the FCCC is provided a certification for processing transactions.

4. SSAE No.16 (Annually):

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 monthly basis with FDOR and the SDU to discuss on-going projects associated with the CLERC system. In addition, there are numerous ad-hoc meetings among FCCC 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. 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 FCCC's role and responsibilities in processing transactions. These communication channels also ensure that the users understand how to use and navigate in the various systems administered by the FCCC. For example, the FCCC makes available to those users of the CLERC System detailed training/procedures manuals. In addition, the FCCC conducts training classes for new Clerk staff. User organizations are encouraged to communicate questions and problems to the FCCC liaisons.

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.

# **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 standalone.

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 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 data and network documents are backed up to a local Data Domain Disk Vault and replicated to a remote Data Domain 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 organization'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 actively monitors data and traffic with virus signature definitions that are updated on an periodic 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.

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 re-assure 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 with an account are required to use a user ID and password to gain access to their accounts. 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.

# **General Description of the File Transmission Processes**

The FCCC Central Site, in conjunction with the CLERC Application and the FCCC Network, is responsible for coordination of all file transmissions between the DOR, SDU, and local Clerk depositories. Listed next is a summary for each of the processes performed by the FCCC:

- 1. <u>27001 (Receipt File) Process:</u> The purpose of the 27001 process is to monitor, process and validate the daily SDU receipts file. After the quality control and validation process, the file is split and sent to each County repository.
- 2. <u>375001 (Exceptions) Process:</u> The purpose of the 375001 process is to monitor, process and validate the daily exceptions file received from the SDU. Subsequent to the quality control and validation process, FCCC transmits the file to DOR and to each County repository.
- 3. <u>95001 (Over the Counter) Process:</u> The purpose of the 95001 process is to monitor, process and validate the daily Over the Counter (OTC) file received from each local County repository. After the quality control and validation process, the file is sent to the SDU and DOR.
- 4. <u>A125 (Receipts) Process:</u> The purpose of the A125 process is to monitor, process and validate the daily collections file received from each local County repository. Once received by FCCC, a composite file is created that is validated and subjected to critical quality control checks prior to being transferred to DOR.
- 5. <u>30501 (Disbursements) Process:</u> The purpose of the 30501 process is to monitor, process and validate the daily disbursement file received from each local County repository. Once received by FCCC, a composite file is created that is validated and subjected to critical quality control checks prior to being transferred to the SDU and DOR.
- 6. <u>30601 (Disbursements) Process:</u> The purpose of the 30601 process is to monitor, process and validate the daily disbursement file from the DOR. Once received by FCCC, the file is validated and subject to critical quality control checks. After the quality control and validation process, the file is sent to the SDU.
- 7. <u>110 (Case Information File) Process:</u> The purpose of the 110 process is to retrieve the case information file from each local County repository. Once received by FCCC, a composite file is created and transferred to the SDU.

# **Control Objectives and Related Controls:**

The FCCC's 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. <u>Re-performance</u>

• 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 Entity personnel as represented.

# 4. <u>Inquiry</u>

• 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 ADMINSTRATIVE 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.

Description of Controls	Test of Controls	Test Results
<ul> <li>The FCCC maintains a high level of control consciousness and oversight of the CLERC System process. Specifically, the FCCC has the following audits/reviews:</li> <li>A. Annual Financial Statement Audits</li> <li>B. Annual Technical Security Review</li> <li>C. Quarterly Technical Security with respect to internet security</li> <li>D. Annual SSAE No. 16 Type II Engagement.</li> </ul>	<ol> <li>Inspected reports and correspondence from each audit/review.</li> <li>Interviewed FCCC management about their policies for maintaining appropriate control consciousness.</li> </ol>	No exceptions noted.
Routine meetings are held to discuss special processing request, operational performance and the development and maintenance of projects.	<ol> <li>Interviewed FCCC management about routine meetings that occur related to the CLERC system.</li> <li>Inspected documents from meetings (correspondence, agendas, minutes, etc).</li> </ol>	No exceptions noted
FCCC management provides oversight for system security.	<ol> <li>Inquired to management about system security.</li> <li>Inspected most recent Security Consulting Report.</li> </ol>	No exceptions noted.
Written position descriptions are maintained by the Organization. These are periodically updated.	<ol> <li>Inspected job descriptions for all employees involved with the CLERC system and FCCC Central Site.</li> <li>Interviewed employees to verify accuracy of documents.</li> </ol>	No exceptions noted.

### SECTION III ORGANIZATIONAL AND ADMINSTRATIVE 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.

<b>Description of Controls</b>	Test of Controls	Test Results
Written performance evaluations are administered on an annual basis. These reviews include stated goals and objectives. Performance evaluations are prepared by Senior Management and become part of the employee's personnel file.	<ol> <li>Inquired to management and discussed the evaluation process. Verified that evaluations take place on an annual basis.</li> <li>Reviewed a sample of annual performance evaluations for those employees involved with the CLERC system. Verified the following:         <ul> <li>Annual performance evaluations were present in the file</li> <li>Each evaluation was signed by the employee and member of management</li> <li>Evaluation included the employee goals and objectives</li> <li>Evaluation contained feedback and constructive criticism</li> </ul> </li> </ol>	No exceptions noted.
The Organization has a signed contract with the Florida Department of Revenue authorizing FCCC to process child support transaction data files through the CLERC system.	<ol> <li>Inquired to management about the nature of the contract and the requirements.</li> <li>Inspected the contract to verify that it is complete and signed by both the FCCC and FDOR.</li> </ol>	No exceptions noted.

### SECTION III ORGANIZATIONAL AND ADMINSTRATIVE 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.

Description of Controls	Test of Controls	Test Results
FCCC staff involved in the CLERC system are competent and possess the necessary professional experience.	1. Interviewed FCCC management on policy for hiring practices.	
	2. Reviewed background and technical experience information in employee's personnel file (i.e. work experience, education, certifications, etc).	No exceptions noted.
	3. Interviewed staff to verify their background and technical experience.	

### SECTION III. TRANSMISSION OF SDU'S RECEIPT FILE (270) AND EXCEPTIONS FILE (375)

**CONTROL OBJECTIVE 2:** Controls provide reasonable assurance that data files (270-receipt file and 375 exception files) generated at the SDU are transmitted through the FCCC Central Site to the sixty-seven County Depositories completely, accurately and timely.

Description of Controls	Test of Controls	Test Results
The FCCC has written process flow documents for transmitting files between the Child Support State Disbursement Unit, each individual County depository, and the Florida Department of Revenue. These process flow documents include problem resolution.	<ol> <li>Confirmed through corroborative inquiry with management that the control activity stated is in place.</li> <li>Inspected process flow documents and verified consistency with file transmission observation.</li> </ol>	No exceptions noted.
The FCCC has an Interface Control Document (ICD) for child support related files transmitted through FCCC Central Site.	<ol> <li>Confirmed through corroborative inquiry with management that the control activity stated is in place.</li> <li>Inspected ICD and verified accuracy with actual file layout.</li> </ol>	No exceptions noted.
The transmission process is automated requiring very little manual intervention.	<ol> <li>Confirmed through corroborative inquiry that the control activity stated is in place.</li> <li>Observed the file transmission process for the SDU receipt files and exceptions files.</li> <li>Verified that a majority of the process is automated.</li> </ol>	No exceptions noted.
The entire transmission process is logged and saved on the network. FCCC management and staff monitor the transmission process.	<ol> <li>Observed management and staff reviewing system generated logs of the file transmission process.</li> <li>For selected dates, requested and inspected file transmission logs.</li> </ol>	No exceptions noted.

#### SECTION III. TRANSMISSION OF SDU'S RECEIPT FILE (270) AND EXCEPTIONS FILE (375)

**CONTROL OBJECTIVE 2:** Controls provide reasonable assurance that data files (270-receipt file and 375 exception files) generated at the SDU are transmitted through the FCCC Central Site to the sixty-seven County Depositories completely, accurately and timely.

Description of Controls	Test of Controls	Test Results
Files received by the FCCC are validated to verify that the file is complete. Specifically, the End of File (EOF) trailer record counts and record amounts match the actual count and actual record amounts in the individual receipt detail records.	<ol> <li>Observed FCCC staff performing this procedure.</li> <li>For selected dates, inspected file transmission logs to verify the trailer record agreed to individual receipt detail records.</li> </ol>	No exceptions noted.
	1. Confirmed through corroborative inquiry that the control activity stated is in place.	
The SDU sends an email confirmation that is compared to the file record count and record amounts included in the associated file transmission log. In the event that a discrepancy exists, the FCCC immediately contacts the SDU for resolution.	2. During file transmission process, observed FCCC staff comparing the record count and amount included on each fax sheet sent from the SDU to the associated file transmission log record count and amount.	No exceptions
	3. For selected dates, inspected emails sent from the SDU and compared to final transmission logs.	
Detail file records are loaded into the SDU Central Site database. During this part of the process new data is compared to existing data (previous 14 days) to identify any duplicate records.	<ol> <li>Observed FCCC staff performing this procedure.</li> <li>For selected dates, inspected file transmission logs to verify that the duplicate record search occurred.</li> </ol>	No exceptions

#### SECTION III. TRANSMISSION OF SDU'S RECEIPT FILE (270) AND EXCEPTIONS FILE (375)

**CONTROL OBJECTIVE 2:** Controls provide reasonable assurance that data files (270-receipt file and 375 exception files) generated at the SDU are transmitted through the FCCC Central Site to the sixty-seven County Depositories completely, accurately and timely.

Description of Controls	Test of Controls	Test Results
The FCCC executes a program that separates the SDU receipt file into individual County receipt files for transmission to each County. Once the separation procedure is complete, the process validates the record count from the SDU receipt file and matches against the total record count of each individual receipt file.	<ol> <li>Observed file transmission process. Specifically, observed file split into separate files for each County.</li> <li>Observed FCCC validate individual county files.</li> <li>For selected dates, inspected file transmission logs to verify that the automated process performed a validation.</li> </ol>	No exceptions noted.
Prior to transmitting the individual receipt files to each County, FCCC staff performs a final review of the file log.	<ol> <li>Confirmed through corroborative inquiry that the control activity stated is in place.</li> <li>Observed FCCC perform this process.</li> </ol>	No exceptions noted.
All transmission issues, errors or concerns are logged and recorded by the FCCC staff in their problem tracking software (HEAT). Each incident recorded is assigned a unique control number. FCCC staff follows up on all problems logged in the system.	<ol> <li>Confirmed through corroborative inquiry that the control activity stated is in place.</li> <li>For selected dates, identified file transmission issues and traced to reports generated by the problem tracking software.</li> </ol>	No exceptions noted.

#### SECTION III. TRANSMISSION OF COUNTY REPOSITORY, SDU AND FDOR FILES: A125 IV-D COLLECTION, NON IV-D DISBURSEMENT (305), AND OTC (950)

**CONTROL OBJECTIVE 3:** Controls provide reasonable assurance that data files (A125, Non IV-D and OTC) generated at each County Depository are transmitted through the FCCC Central Site to the SDU and DOR completely, accurately, and timely.

Description of Controls	Test of Controls	Test Results
The FCCC has written process flow documents for transmitting files between the Child Support State Disbursement Unit, each individual County depository, and the Florida Department of Revenue. These process flow documents include problem resolution.	<ol> <li>Confirmed through corroborative inquiry with management that the control activity stated is in place.</li> <li>Inspected process flow documents and verified consistency with file transmission observation.</li> </ol>	No exceptions noted.
The FCCC has an Interface Control Document (ICD) for child support related files transmitted through FCCC Central Site.	<ol> <li>Inspected the ICD document.</li> <li>Compared the ICD document to actual file layout for accuracy.</li> </ol>	No exceptions noted.
The transmission process is automated requiring very little manual intervention.	<ol> <li>Confirmed through corroborative inquiry that the control activity stated is in place.</li> <li>Observed the file transmission process for the subject files.</li> <li>Verified that a majority of the process is automated.</li> </ol>	No exceptions noted.

#### SECTION III. TRANSMISSION OF COUNTY REPOSITORY AND FDOR FILES: A125 IV-D COLLECTION, NON IV-D DISBURSEMENT (305), AND OTC (950)

**CONTROL OBJECTIVE 3:** Controls provide reasonable assurance that data files (A125, Non IVD and OTC) that are generated at each County Depository are transmitted through the FCCC Central Site to the SDU and DOR completely, accurately and timely.

Description of Controls	Test of Controls	Test Results
The entire transmission process is logged and saved on the network. FCCC management and staff monitor the transmission process.	<ol> <li>Observed management and staff reviewing system generated logs of the file transmission process.</li> <li>For selected dates, requested and inspected file transmission logs.</li> </ol>	No exceptions noted.
After each individual County file is retrieved using the FTP program, the monitoring process checks for any identically named files in the process directory.	<ol> <li>Confirmed through corroborative inquiry that the control activity stated is in place.</li> <li>For selected dates, examined the file log and verified this process was performed.</li> </ol>	No exceptions noted.
Individual County files received by the FCCC are validated to verify that the file is complete. Specifically, the End of File (EOF) trailer record counts and record amounts match the actual record count and actual record amounts for each file received. Errors are identified and listed in the file log.	<ol> <li>Inquired to management about the file transmission process.</li> <li>For selected dates, observed the file transmission process.</li> <li>Inspected the file program source code that compares the End of File trailer record counts and amounts.</li> <li>In a test environment, altered actual record amounts and record counts in a selected file and verified the system flagged each as an exception (failure).</li> <li>For selected months, inspected file log for exceptions (failures) identified.</li> </ol>	No exceptions noted.

#### SECTION III. TRANSMISSION OF COUNTY REPOSITORY AND FDOR FILES: A125 IV-D COLLECTION, NON IV-D DISBURSEMENT (305), AND OTC (950)

**CONTROL OBJECTIVE 3:** Controls provide reasonable assurance that data files (A125, Non IVD and OTC) that are generated at each County Depository are transmitted through the FCCC Central Site to the SDU and DOR completely, accurately and timely.

Description of Controls	Test of Controls	Test Results
All County files are concatenated into a single composite file. Detail file records are loaded into the SDU Central Site database. During this part of the process new data is compared to existing data (previous 7 business days for A125 file and previous 5 business days for 305 file) to identify any duplicate records.	<ol> <li>Observed FCCC staff performing this procedure.</li> <li>For selected dates, inspected file transmission logs to verify that the duplicate record search occurred.</li> </ol>	No exceptions noted
All transmission issues, errors or concerns are logged and recorded by the FCCC staff in their problem tracking software. Each incident recorded is assigned a unique control number. FCCC staff follows up on all problems logged in the system.	<ol> <li>Confirmed through corroborative inquiry that the control activity stated is in place.</li> <li>For selected dates, identified file transmission issues and traced to reports generated by the problem tracking software.</li> </ol>	No exceptions noted.

### SECTION III. PHYSICAL SECURITY

**CONTROL OBJECTIVE 4:** Controls provide reasonable assurance that physical access to computer equipment, storage media, and program documentation is restricted to properly authorized individuals.

Description of Controls	Test of Controls	Test Results
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.	<ol> <li>Observed that all entrances (with exception of main entrance) remained locked at all times.</li> <li>Observed the presence of electronic key devices at the entrances to the FCCC building.</li> </ol>	No exceptions noted.
Electronic badge devices control the access to the FCCC server room. Only specified technical staff has access to this secured location.	<ol> <li>Verified the server room is locked.</li> <li>Observed the presence of an electronic key device at the entrance of the server room.</li> </ol>	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.	<ol> <li>Inspected a listing of individuals with access to the server room. Verified that only current employees have access.</li> <li>Observed non-authorized staff unsuccessfully attempt access.</li> </ol>	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.	<ol> <li>Verified the front entrance is the only un-locked entrance during normal office hours.</li> <li>Observed visitors entering and exiting the building.</li> <li>Observed receptionist providing visitor badges.</li> </ol>	No exceptions noted.

### SECTION III. PHYSICAL SECURITY

**CONTROL OBJECTIVE 4:** Controls provide reasonable assurance that physical access to computer equipment, storage media, and program documentation is restricted to properly authorized individuals.

Description of Controls	Test of Controls	Test Results
An escort (FCCC staff) is called to greet their visitors in the lobby.	1. Verified through observation that guests are accompanied by a FCCC staff employee at all times.	No exceptions noted.
The FCCC conducts employment background checks and criminal history checks on external candidates selected to fill vacant positions.	<ol> <li>Inspected Human Resource procedures to verify that background checks are required for all new employees.</li> <li>Inspected background/criminal history check log for all employees hired in 2016 fiscal period.</li> <li>For selected employees, inspect background/ criminal history check documentation.</li> </ol>	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 the CLERC system operates. The consulting company conducts an annual Exit Conference, issues an Executive Summary Report, issues detailed technical report and provides to FCCC Senior Management recommendations for improvement.	<ol> <li>Inquired to FCCC Management about the Security Consulting engagement and method of addressing recommendations.</li> <li>Inspected the most recent security consulting report.</li> </ol>	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.	<ol> <li>Inspected contract with vendor to verify the existence of alarm system.</li> <li>Performed a walkthrough of the building to verify the existence of an alarm system.</li> </ol>	No exceptions noted.

### SECTION III. PHYSICAL SECURITY

**CONTROL OBJECTIVE 4:** Controls provide reasonable assurance that physical access to computer equipment, storage media, and program documentation is restricted to properly authorized individuals.

Description of Controls	Test of Controls	Test Results
	1. Interviewed management to verify that a camera system was in place.	
Camera system is used to monitor building entrances and other sensitive areas within the building.	2. Observed cameras in place throughout the building.	No exceptions noted.
	3. Observed sample of recorded videos to verify functioning properly.	

### SECTION III. ENVIRONMENTAL CONTROLS

**CONTROL OBJECTIVE 5:** Controls provide reasonable assurance that the physical environmental devices are installed to adequately protect the servers, network equipment, and storage media.

<b>Description of Controls</b>		Test of Controls	Test Results
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. 2.	Observed the FCCC Server Room and verified that an air conditioning system is present in the data center. Verified that a maintenance agreement exists on the system.	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. 2.	Observed the FCCC data center and noted the FM-200 release heads were present throughout the server room. 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. 2.	Toured facility and verified the presence and location of UPS. 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. 2.	Observed the diesel generator at the FCCC facility and verified that a diesel generator was in place to provide backup power to the facility. Inspected the maintenance agreement and verified that generator is inspected on an annual basis.	No exceptions noted.

Description of Controls	Test of Controls	Test Results
Network diagram illustrates the physical and logical connections of FCCC information systems.	1. Inspected the FCCC System/Network Diagram.	No exceptions noted.
Communication equipment and servers are labeled to facilitate cross-reference of these diagrams.	<ol> <li>Inquired to management about the FCCC systems/networks.</li> <li>Observed the server room and compared physical equipment (labeled) to the network diagram.</li> </ol>	No exceptions noted.
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.	<ol> <li>Verified inclusion of firewalls on system diagram.</li> <li>Observed the FCCC produce firewall logs for a specific time frame.</li> <li>Verified that this log reflects all attempted access to the systems.</li> </ol>	No exceptions noted.
Antivirus protection has been implemented at FCCC server, email gateway, and workstation levels to protect company data from infection by malicious code or viruses.	<ol> <li>Verified antivirus software exists on servers and a selection of workstations.</li> <li>Reviewed written antivirus policies contained in the Security Policies and Procedures Manual.</li> <li>Obtained log of periodic virus scans on servers and workstations.</li> </ol>	No exceptions noted.
FCCC uses managed software to enforce security on Personal Digital Assistant (PDA) devices.	Reviewed written PDA policy contained in the Security Policies and Procedures document. Verified managed software is present with PIN enforcement settings.	No exceptions noted.

Description of Controls	Test of Controls	Test Results
The FCCC Internet Portal contains a Digital Certificate (SSL - Web Certificate). Certificates have been issued by a known certificate authority and an authentic seal is accessible on the website.	<ol> <li>Inspected certificate documentation provided from vendor. Verified that the current certificate was current and had not expired.</li> <li>Observed website to verify that the digital certificate is displayed.</li> </ol>	No exceptions noted.
Windows and Network password management controls include the following: -Minimum password length -Character complexity components -Password expiration/change frequency -Invalid password attempts/account lock out -Password history	<ol> <li>Obtained the domain security policy and confirmed consistency with parameters in the system.</li> <li>Observed employee unable to log into system with invalid passwords.</li> <li>Viewed history of password expiration.</li> </ol>	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.	<ol> <li>Confirmed through corroborative inquiry with Management of IT that the control activity stated is in place.</li> <li>Obtained a list of terminated employees during audit period.</li> <li>Inspected the active directory to verify that all terminated employees were disabled or eliminated.</li> </ol>	No exceptions noted.

Description of Controls	Test of Controls	Test Results
FCCC encrypts the hard drives of laptops to prevent unauthorized access in the event of loss or theft.	<ol> <li>Observed the managed console of the drive encryption software.</li> <li>Randomly selected laptops to verify that encryption is active and functioning properly.</li> </ol>	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.	<ol> <li>Read most recent annual security report.</li> <li>Verified that the report does not identify major problems or weaknesses in the system.</li> <li>Verified that recommendations are provided to management for improvement.</li> </ol>	No exceptions noted.
FCCC uses third party software to monitor the websites and portals to confirm sites are operating and that connections can be made.	<ol> <li>Confirmed through corroborative inquiry with Management of IT that the control activity stated is in place.</li> <li>Observed access to the monitoring software and confirmed it was active.</li> <li>Inspected periodic email reports sent to FCCC IT that reflects monitoring results and any potential issues with the FCCC websites.</li> </ol>	No exceptions noted.
FCCC uses Microsoft Server Update Services (WSUS) to manage and install Microsoft critical and security patches.	<ol> <li>Observed FCCC gain access to the WSUS software.</li> <li>Inspected reports of managed FCCC servers and workstations.</li> </ol>	No exceptions noted.

<b>Description of Controls</b>	Test of Controls	Test Results
A Uniform Resource Locator (URL) filter is in place to detect and block potentially malicious links from being accessed.	<ol> <li>Verified with management the existence of the URL filtering device.</li> <li>Inspected sample logs of blocked potentially malicious URLs.</li> </ol>	No exceptions noted.

### SECTION III. INFORMATION AND COMMUNICATION

**CONTROL OBJECTIVE 7:** 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.

<b>Description of Controls</b>	Test of Controls	Test Results
The FCCC has written process flow documents for transmitting files between the Child Support State Disbursement Unit, each individual County depository, and the Florida Department of Revenue. These process flow documents include problem resolution.	<ol> <li>Confirmed through corroborative inquiry that the control activity stated is in place.</li> <li>Inspected process flow documents. Observed actual process to confirm accuracy of written documents.</li> <li>For selected dates, identified file transmission issues and traced to reports generated by the problem tracking software.</li> </ol>	No exceptions noted.
The FCCC maintains an organizational chart for the Technical Division that clearly depicts lines of authority.	<ol> <li>Inspected FCCC organizational chart as it relates to the CLERC System. Obtained explanations from the FCCC on the various functions presented.</li> <li>During the course of the audit, observed various positions to verify work is performed consistent with organizational chart and job descriptions.</li> </ol>	No exceptions noted.
The FCCC has routine meetings to discuss special processing requests, operations, and the development and maintenance of projects.	Inquired to management about the existence of routine technical meetings. Requested explanation for issues discussed at these meetings.	No exceptions noted.

### SECTION III. INFORMATION AND COMMUNICATION

**CONTROL OBJECTIVE 7:** 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.

Description of Controls	Test of Controls	Test Results
All transmission issues, errors or concerns are logged and recorded by the FCCC staff in their problem tracking software. Each incident recorded is assigned a unique control number. FCCC staff follows up on all problems logged in the system.	<ol> <li>Confirmed through corroborative inquiry that the control activity stated is in place.</li> <li>For selected dates, identified file transmission issues and traced to reports generated by the problem tracking software.</li> </ol>	No exceptions noted.
The FCCC has a Service Center function that provides on-going support for the existing FCCC applications.	<ol> <li>Inquired to management as to the nature of the FCCC Service Center.</li> <li>During the course of the audit, observed the Service Center staff performing their tasks.</li> <li>Inspected tracking logs or other documentation from database that tracks issues arising from customers.</li> </ol>	No exceptions noted.
The FCCC provides necessary training to Clerks with respect to the CLERC System.	<ol> <li>Inquired to management as to the type of training/operational procedures.</li> <li>Inspected training documents made available to Clerks for the various components of the CLERC system and application.</li> </ol>	No exceptions noted.
The FCCC has implemented an Information Technology Service Management (ITSM) framework and Information Technology Infrastructure Library (ITIL) best practices for FCCC technical projects. Selected staff have been trained and earned the ITSM/ITIL certification.	Inquired to management about the existence of ITSM/ITIL framework and best practices. Inspected ITSM/ ITIL related documents and employee certifications	No exceptions noted.

### SECTION III. SEGREGATION OF FUNCTIONS (INTERNAL)

**CONTROL OBJECTIVE 8:** Controls provide reasonable assurance that FCCC activities are organized to provide internal segregation of functions.

Description of Controls	Test of Controls	Test Results
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.	No exceptions noted.
	3. Observed various duties/ functions being performed by the FCCC staff.	
The FCCC maintains an organizational chart for the Technical Division that clearly depicts lines of authority.	<ol> <li>Inspected FCCC organizational chart as it relates to the CLERC system. Obtained explanations from the FCCC on the various functions presented.</li> <li>During the course of the audit, observed various positions to verify work is performed consistent with organizational chart and job descriptions.</li> </ol>	No exceptions noted.
The CLERC System operations personnel do not perform programming functions. Programming personnel do not perform operations duties.	<ol> <li>Reviewed the IT (Information Technology) organization chart noting the degree to which operations and programming functions are segregated.</li> <li>Interviewed computer operations management to determine adherence to policy.</li> </ol>	No exceptions noted.

### SECTION III. SEGREGATION OF FUNCTIONS (INTERNAL)

**CONTROL OBJECTIVE 8:** Controls provide reasonable assurance that FCCC activities are organized to provide internal segregation of functions.

Description of Controls	Test of Controls	Test Results
Programming personnel do not initiate or authorize transactions.	1. Reviewed the policies and procedures of FCCC.	No exceptions noted.
Written job descriptions have been prepared for FCCC personnel and are periodically updated.	<ol> <li>Reviewed employee job descriptions for those employees involved with the CLERC System.</li> <li>Interviewed management and employees to verify accuracy of these documents.</li> </ol>	No exceptions noted.

### SECTION III. SEGREGATION OF FUNCTIONS (EXTERNAL)

**CONTROL OBJECTIVE 9:** The FCCC and User Organizations (Clerks) are segregated.

<b>Description of Controls</b>	Test of Controls	Test Results
FCCC is physically separate from the user organizations (Clerks) for which it performs processing.	1. Reviewed policies of the organization and contractual obligations that exist between FCCC and user organizations.	No exceptions noted.
The relationship between the FCCC and user organizations is contractual in nature.	1. Reviewed policies of FCCC and contractual obligations that exist between FCCC and user organizations.	No exceptions noted.

### SECTION IV. 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.

Description of Controls	Test of Controls	Test Results
The following schedule of backups and controls are being performed: • Daily • Weekly • Monthly • Annual Backups are performed utilizing a custom script that has been implemented on the server.	<ol> <li>Inspected automated script utilized by FCCC staff in performing the backup.</li> <li>Inquired to management about the system and the backup schedule.</li> <li>Inspected the FCCC system diagram/flowchart to understand the various components, servers, databases and etc.</li> <li>Observed a selection of backup logs for various servers identified on the network diagram.</li> <li>Inspected vendor documents that substantiate that selected days were picked up and taken to storage.</li> <li>Performed backup of a randomly selected folder.</li> </ol>	No exceptions noted.
The backup process is performed in accordance with detailed written procedures.	<ol> <li>Inquired to management about the backup procedures and associated processes.</li> <li>Reviewed the backup schedule in place for the FCCC server and data files.</li> <li>Inspected a selection of backup logs to verify compliance with procedures.</li> </ol>	No exceptions noted.

### SECTION IV. 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.

Description of Controls	Test of Controls	Test Results
Recoveries are performed on a periodic basis.	<ol> <li>Inquired to management about the recovery process procedures.</li> <li>Performed a recovery of randomly sampled file.</li> </ol>	No exceptions noted.