FLORIDA COURTS E-FILING AUTHORITY

SOC 1 Type 2 Report

REPORT ON FLORIDA COURTS E-FILING AUTHORITY'S DESCRIPTION OF ITS E-FILING PORTAL SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS

Pursuant to Statement of Standards for Attestation Engagements No. 18

(SSAE 18) Type 2

For the Period July 1, 2021 through June 30, 2022

PURVIS GRAY

CERTIFIED PUBLIC ACCOUNTANTS

Sarasota • Tallahassee • Gainesville • Ocala • Orlando • Lakeland

Table of Contents

SECTION 1: INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Board of Directors
Florida Courts E-Filing Authority

Scope

We have examined the Florida Courts E-Filing Authority's (the Authority or service organization) description of its E-Filing Portal system for processing user entities' transactions entitled "Description of Florida Courts E-Filing Authority's E-Filing Portal System" throughout the period of July 1, 2021 to June 30, 2022 (description), and the suitability of design and operating effectiveness of the controls included in the description to achieve related control objectives stated in the description based on the criteria identified in the "Florida Courts E-Filing Authority's Assertion" (assertion). The controls and control objectives included in the description are those that management of the Authority believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the E-Filing Portal system that are not likely to be relevant to user entities' internal control over financial reporting.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of the Authority's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

The Authority uses a subservice organization to provide for off-site data center storage of its backup data and two subservice organizations for merchant payment processing and payment authentication services, collectively the 'subservice organizations'. The description includes only the control objectives and related controls of the Authority and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by the Authority can be achieved only if complementary subservice organization controls assumed in the design of the Authority's controls are suitably designed and operating effectively, along with the related controls at the Authority. Our examination did not extend to controls of the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organizations' controls.

There were controls stated in the Authority's description that did not operate because the circumstances that warrant the operation of those controls did not occur and, therefore, Purvis Gray was unable to test those controls. For more information see Section 4 Controls 4.7 and 6.2.

INDEPENDENT SERVICE AUDITOR'S REPORT

Service Organization's Responsibilities

In Section 2, the Authority 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 Authority is responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and 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 stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively 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.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, 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 July 1, 2021 to June 30, 2022. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls 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 the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion.

- 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.

- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.

- Evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment.

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing 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 ineffective.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section 4.

Opinion

In our opinion, in all material respects, based on the criteria described in the Authority's assertion:

a. The description fairly presents the E-Filing Portal system that was designed and implemented throughout the period July 1, 2021 to June 30, 2022.

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 July 1, 2021 to June 30, 2022, and subservice organizations and user entities applied the complementary controls assumed in the design of the Authority's controls throughout the period July 1, 2021 to June 30, 2022.

c. The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period July 1, 2021 to June 30, 2022, if complementary subservice organizations and user entity controls assumed in the design of the Authority's controls operated effectively throughout the period July 1, 2021 to June 30, 2022.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of the Authority, user entities of the Authority's E-Filing Portal system during some or all of the period July 1, 2021 to June 30, 2022, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

Purvis Gray

October 26, 2022
Tallahassee, Florida

SECTION 2: ASSERTION OF THE MANAGEMENT OF FLORIDA COURTS E-FILING AUTHORITY

ASSERTION OF THE MANAGEMENT OF FLORIDA COURTS E-FILING AUTHORITY

October 26, 2022

We have prepared the description of Florida Courts E-Filing Authority's (the Authority or service organization) E-Filing Portal system entitled "Description of Florida Courts E-Filing Authority's E-Filing Portal system," for processing user entities' transactions throughout the period July 1, 2021 to June 30, 2022 (description), for user entities of the system during some or all of the period July 1, 2021 to June 30, 2022, and their auditors who audit and report on such user entities' financial statements or internal control over financial statement reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves when assessing the risks of material misstatements of user entities' financial statements.

The Authority uses a subservice organization to provide for off-site data center storage of its backup data and uses a subservice organization for merchant payment processing and payment authentication services collectively the 'subservice organizations'. The description includes only the control objectives and related controls of the Authority and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively, along with the related controls. The description does not extend to controls of the subservice organizations.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of the Authority's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that:

1) The description fairly presents the E-Filing Portal system made available to user entities of the system during some or all of the period July 1, 2021 to June 30, 2022, for processing user entities' transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

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

        i) The types of services provided, including, as appropriate, the classes of transactions processed.

        ii) The procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.

        iii) The information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

iv) How the system captures and addresses significant events and conditions other than transactions.

v) The process used to prepare reports and other information for user entities.

vi) The services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.

vii) The specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the controls.

viii) Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

b) Includes relevant details of changes to the E-Filing Portal system during the period covered by the description.

c) Does not omit or distort information relevant to the system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors and may not, therefore, include every aspect of the E-Filing Portal system that each individual user entity of the system and its auditor may consider important in its own particular environment.

2) The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period July 1, 2021 to June 30, 2022, to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of the Authority's controls throughout the period July 1, 2021 to June 30, 2022. The criteria we used in making this assertion were that:

a) The risks that threaten the achievement of the control objectives stated in the description have been identified by management.

b) The controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

c) The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

3) There were controls stated in the description that did not operate because the circumstances that warrant the operation of those controls did not occur. For more information see in Section 4 of the report, Controls 4.7 and 6.2.

SECTION 3: DESCRIPTION OF FLORIDA COURTS E-FILING AUTHORITY'S E-FILING PORTAL SYSTEM

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT

Overview of the E-Filing Portal

The Clerks of the Circuit Court are the official custodians of court records within their respective jurisdictions. The Clerk of the Florida Supreme Court is the official custodian of records for the Florida Supreme Court. In 2009, the Florida Legislature and Florida Supreme Court recognized the need for the development and implementation of a statewide electronic court filing system. As a result, Chapter 28.22205, Florida Statutes, was passed into law:

> 28.22205 Electronic filing process – Each clerk of court shall implement an electronic filing process. The purpose of the electronic filing process is to reduce judicial costs in the office of the clerk and the judiciary, increase timeliness in the processing of cases, and provide the judiciary with case-related information to allow for improved judicial case management. The Legislature requests that, no later than July 1, 2009, the Supreme Court set statewide standards for electronic filing to be used by the clerks of court to implement electronic filing. The standards should specify the required information for the duties of the clerks of court and the judiciary for case management. The clerks of court shall begin implementation no later than October 1, 2009. The Florida Clerks of Court Operations Corporation shall report to the President of the Senate and the Speaker of the House of Representatives by March 1, 2010, on the status of implementing electronic filing. The report shall include the detailed status of each clerk office's implementation of an electronic filing process, and for those clerks who have not fully implemented electronic filing by March 1, 2010, a description of the additional steps needed and a projected timeline for full implementation. Revenues provided to counties and the clerk of court under s. 28.24(12)(e) for information technology may also be used to implement electronic filing processes.

The Florida Association of Court Clerks, Inc. (d/b/a Florida Court Clerks and Comptrollers) (FCCC), in conjunction with the Florida Supreme Court, responded to this mandate by creating the Florida Courts E-Filing Authority (the Authority or service organization). This was accomplished by an Interlocal Agreement creating a public agency pursuant to Chapter 163, Florida Statutes, comprised of Clerks of the Circuit Court who join the Authority and the Clerk of the Supreme Court.

The Authority contracted with the FCCC to design, develop, implement, operate, upgrade, support, and maintain a uniform statewide electronic portal for the filing of court records. The portal provides attorneys and pro se litigants with a common entry point for filing and transmitting court records electronically. In addition, the portal provides these same persons and other authorized persons the ability to view court records electronically. The features of the portal include the following:

- A single statewide log-in.
- A single internet access to court records by authorized users.
- Transmission to and from the appropriate courts.
- The ability to provide electronic service of notification receipt of an electronic filing and confirmation of filing in the appropriate court file.
- Open standards-based integration ability with existing statewide information systems and county E-Filing applications.
- Compliance with electronic court filing standard 4.0, the global justice extensible markup language and oasis legal markup language.

The portal was launched in January 2011, as required by the Interlocal Agreement. As of June 30, 2022, a majority of the counties were filing court records through the statewide portal.

Florida Supreme Court Opinion 11-399 required that attorneys e-file documents in criminal cases and civil cases filed in probate, family, circuit, and county civil court. The Authority expects continued growth and is considering adding more non-attorney users to the E-filing system.

An electronic filing may be submitted to the portal 24 hours per day and seven days per week. Electronic time/date stamps are attached to the documents as they are filed. However, the filing is not official information of record until it has been stored on the Clerk's case management system. All dates and times, including when the filing is received at the portal and accepted by the Clerk, are stored in the portal database.

Control Environment

The Authority'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 several 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 Authority's Board of Directors has ultimate responsibility for overseeing Authority operations. The Board is comprised of 9 members consisting of the following:

- Board Chairman – the chair of the FCCC Technology Committee, as selected by the FCCC President each year.
- Seven Clerks of the Circuit Court – in addition to the chair, each of the seven FCCC districts nominate a Clerk from the district to serve on this board.
- Clerk of the Supreme Court – the Clerk of the Supreme Court serves as the Chief Justice's designee on behalf of the state courts.

The Authority contracted with the FCCC to develop and maintain a uniform statewide electronic portal for the filing of court records. As a result, the remainder of this section of the report is discussed with respect to the structure and operations of the FCCC.

The FCCC Technology Committee has closer involvement to the technical aspects of the portal. 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 E-Filing Portal system, operations, controls, etc.). The Technology Committee is comprised of nine Clerks presiding in the State of Florida. This committee meets frequently throughout the year.

The FCCC is headed by the Chief Executive Officer who reports directly to the Executive Committee. Overseeing the day-to-day operations of the E-Filing Portal is the E-portal division

The Technical Division performs the following functions:

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

Supporting the FCCC Technology Division is the accounting function which is responsible for recording and reconciling the daily activity processed through the E-Filing portal.

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 portal.

Personnel Policies and Procedures:

The FCCC has implemented sound human resource practices that help attract and retain competent and trustworthy employees.

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 recognizes the need for its employees to receive annual performance evaluations. 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.

Information and Communication Systems

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 the portal. 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 IT projects, including the portal. ITSM/ITIL is an internationally recognized best practice approach for managing IT 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 the portal. 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 portal 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.

Monitoring Controls

Management monitors operations, performance, quality, and internal controls as a normal part of their activities. Management and staff, engaged in the technical and operational responsibilities, meet on a routine basis to discuss various issues pertaining to the portal. The type of issues discussed include, but are not limited to: problem resolution, system modification and enhancements, processing, transaction volume, and banking issues. The FCCC has implemented various key reports (i.e., Budget, Transaction Volume, and Financial Activity Reports) that measure the results of the portal.

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):

An independent 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 (Annual):

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 the portal, 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.

DESCRIPTION OF THE SYSTEM

The primary control objective of FCCC is to ensure that all transactions are properly initiated, authorized, recorded, processed, reported, and maintained. These controls are evident in every aspect of the business. The core service areas are E-Filing portal processing, administration, information technology and systems security.

FCCC's control objectives and related controls are included in "Section 4—Information Provided by Independent Service Auditor" to eliminate the redundancy that would result from listing them in both Sections 3 and 4. Although the control objectives and related controls are included in Section 4, they are an integral part of FCCC's description of the system.

Description of Transaction Processing

Account Setup (Filer):

Prior to utilizing the portal, filers must establish an account. This can be accomplished by accessing the E-Filing log-in page at www.myflcourtaccess.com. Filers are prompted to complete all available fields on the screen. For security purposes, the user is required to create a username and password. In addition, a security question must be selected from the drop-down menu.

Filers receive two separate email notifications associated with the account setup process. The first email notification provides the filer with confirmation that the registration process was successful and provides the filer with profile information entered during the registration process. The second email notification provides the filer with an activation link which the filer must click on to complete the registration process. Prior to activation the filer must select the same security question selected during the registration process and the correct answer.

Account Management:

The filer has access to various links to make changes to profile information and to manage their accounts. For example, the "my filings" link allows the filer to view a list of filings entered using the portal. This page shows the status filings for a specified date range.

Case Filings:

The filer can select an existing case from a list of filings and append additional documents. The filer is required to perform a series of steps and complete all required fields. Prior to submission the filer is given the opportunity to review and edit the information and documents.

Users can file new cases through the portal. The first step in the process is to enter the new case information. Filing fees are automatically calculated based on selections made by the filer. At this point, documents can be added to the case. The filer is able to browse and attach the document.

The portal accepts documents in Word, WordPerfect, or PDF. All documents are converted to the PDF format by the portal. By default, the portal will provide the PDF format to the local record system. Each county will also have the option to receive the original Word document if available.

An electronic filing may be submitted to the portal 24 hours per day and seven days per week. Electronic time/date stamps are attached to the documents as filed. However, the filing is not official information of record until it has been stored on the Clerk's case management system. All dates and times, including when the filing is received at the portal and accepted by the Clerk, are stored in the portal database.

Payments:

After a case is added, the filer is then directed to the payment screen. A list of filing fees is presented in the "fee information" portion of the screen. The screen also provides an explanation (in red) of how the convenience fee is calculated.

There are three payment options available: credit card, e-check, or fee waiver. The user is required to enter payment information. The system prompts the user if required information is missing. The filing cannot be submitted with missing data. Once the filer selects the submit button, the credit card and 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): This 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.

Filers receive a confirmation upon successful filing.

Confirmation of Filing:

The filer receives three confirmations during the filing process:

1. Screen Confirmation: Immediately upon submitting the filing, the filer will receive a confirmation notice on the portal screen. A filing reference number is provided. This number is needed for communication with the county prior to a case number being assigned.

2. Email Confirmation: The filer receives an email that verifies the case was successfully submitted.

3. Email Confirmation: Clerk Review: subsequent to the Clerk's review of the filing, the user receives another email verifying that the filing was processed successfully.

In addition to the confirmations above, the document now appears in the "my filings" section on the portal website with the completion date populated.

Accounting and Reconciliation of Portal Transactions:

All transaction data is captured by the portal 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 the portal are sequentially numbered. Orders are given a unique identifier at the point that users initiate transactions.

Prior to November of 2021, the FCCC utilized an interface called the "IPAS reconciliation system" (Access Database) between the portal 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 outline the processes for successful reconciliation. For November of 2021 and after, the majority of processing transactions were migrated to a new version of the payment engine. The new payment engine allows for the summary reports to be produced from the system, eliminating the need for the IPAS reconciliation system. In addition, a new payment processor was contracted to process these specific transactions.

The FCCC Accounting function performs monthly bank reconciliations of the portal bank account. 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 the portal. Once completed, the bank reconciliations are reviewed by FCCC Management.

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

The Authority Banking function performs a daily confirmation/verification process on E- Filing Portal ACH Files. The purpose of this process is to verify that the transfer amount according to the bank agrees to the E-Filing Portal 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, and 4) staff initials performing the process.

Information Technology and Systems Security

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 Organization 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 FCCC IT network and other IT Systems. FCCC has leased high-speed communication lines to connect to the Internet.

Description of General Computing Controls

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. Backups are performed on a schedule which is at a minimum daily.

Data is backed up on premise to a backup server. The data and network documents are backed up to a local backup recovery appliance and replicated to a remote backup recovery appliance 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 in Tallahassee, Florida. Controls are in place to provide 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 located at the front of the building. Access is controlled and monitored by the FCCC'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 authorized employees. The server room features dedicated air-conditioning units to protect the room from heat and humidity.

Fire extinguishers are located throughout the building 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-referencing to these diagrams.

To protect FCCC data and information, an industry standard 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 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, applications, and databases.

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.
- Password complexity.
- Password expiration.
- Password history is maintained.
- Account lockout after a number of 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 on-line 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.

To ensure that sensitive data transmitted to the above website is protected against disclosure to third parties, the website uses Hypertext Transfer Protocol with Privacy, which connects with AES 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.

System Change Management:

System changes are authorized by FCCC management prior to deployment. Applicable system changes are tested in segregated environments prior to deployment and deployment is restricted to authorized personnel. Based on risk evaluation, rollback plans are in place in the event there are post-deployment issues.

STATEMENT ON COVID-19

FCCC believes that COVID-19 and its response to it had no significant impacts to either's internal controls. There were no other significant changes to the design, existence, or operations of the specified internal controls as a result of COVID-19. In addition, there have been no significant changes to FCCC's control objectives, reporting responsibilities, or complementary user entity and complementary subservice organization controls as a result of COVID-19.

SUBSERVICE ORGANIZATIONS

FCCC has contracted with DXC Technology (DXC) as its off-site data recovery center. FCCC staff observed applicable physical security controls were in place at the DXC site when visiting the site for disaster recovery testing. E-Filing backup data is encrypted prior to being transmitted to the DXC Site.

The following criteria and controls are expected to be implemented by DXC:

1. The third-party data center has physical access controls in place to restrict access to authorized personnel only.

2. The third-party data center has physical access controls in place to remove access when no longer required.

FCCC utilizes CyberSource to process payment solution transactions for merchant processing purposes and provides payment authentication services. FCCC monitors payment processing through the various banking and processing controls as listed above.

The following criteria and controls are expected to be implemented by CyberSource:

1. Controls are implemented at CyberSource to provide reasonable assurance that changes to data formats that integrate with FCCC's payment engine application are required to be authorized and tested prior to deployment.

During the reporting period, FCCC contracted with a new merchant processer, Adyen, to process payment solution transactions for merchant processing purposes and provide payment authentication services. FCCC monitors payment processing through the various banking and processing controls as listed above.

The following criteria and controls are expected to be implemented by Adyen:

1. Controls are implemented at Adyen to provide reasonable assurance that changes to data formats that integrate with FCCC's payment engine application are required to be authorized and tested prior to deployment.

COMPLEMENTARY USER ENTITY CONTROLS

User Entity Clerk Controls

ID	Control Activities Expected to be Implemented at User Entities	Related Control Objective
1	Controls are in place for user clerk organizations to ensure compliance with contractual requirements.	**Control Objective 1:** Controls provide reasonable assurance that management identifies and assesses risks and provides oversight, standards of conduct, and a structure for carrying out internal controls.

2	Controls are in place to manage and report public users' (customers) reported payment issues to CiviTek.	**Control Objective 2:** Controls provide reasonable assurance that the information and communication component include the procedures and records established by CiviTek to initiate, process, and report the user organizations' (Clerks) transactions and maintain accountability for the transactions.
3	Controls are in place to ensure that document filing fees are accurate.	**Control Objective 10:** Controls provide reasonable assurance that service fees are properly charged based on approved schedules.
4	Controls are in place to notify E-Filing in the event that a portal administrator leaves the clerk organization.	**Control Objective 6:** Controls provide reasonable assurance that security measures are in place around sensitive data and logical access to programs, data, and computer resources is restricted to authorized and appropriate users.

SECTION 4: INFORMATION PROVIDED BY THE INDEPENDENT SERVICE AUDITOR

PURPOSE AND OBJECTIVES OF THE REPORT

This report is intended to provide user entities with information about controls at the FCCC that may affect the processing of user entities' transactions and to provide users with information about the operating effectiveness of the controls that were tested. This report, when combined with an understanding and assessment of the internal controls at user entities, is intended to assist the user auditor in: (1) planning the audit of the user's financial statements, and in (2) assessing control risk for assertions in the user's financial statements that may be affected by controls at FCCC.

Our examination was restricted to the description of the system, control objectives, and the related control procedures specified in Section 3 by FCCC management and was not extended to procedures described elsewhere in this report but not listed, or to procedures that may be in effect at the user clerk entity. Our examination was performed in accordance with the American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements No. 18 (SSAE 18). It is each user auditor's responsibility to evaluate this information in relation to the controls in place at each user entity. If certain complementary user entity controls are not in place at the user entity organization, FCCC's controls may not compensate for such weaknesses.

The description of the system and control objectives are the responsibility of FCCC's management. Our responsibility is to express an opinion about whether:

1. The description fairly presents the E-Filling Portal system that was designed and implemented throughout the period July 1, 2021 to June 30, 2022.

2. 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 July 1, 2021 to June 30, 2022, and subservice organizations and user entities applied the complementary controls assumed in the design of the Authority's controls throughout the period July 1, 2021 to June 30, 2022.

3. The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period July 1, 2021 to June 30, 2022, if complementary subservice organizations and user entity controls assumed in the design of the Authority's controls operated effectively throughout the period July 1, 2021 to June 30, 2022.

TESTS OF OPERATING EFFECTIVENESS

Our examination of the control activities was performed using the following testing methods:

Test	Description
Inquiry	Made inquiries of appropriate personnel responsible for the performance of the control activity and corroborated responses with management.
Observation	Observed the application of a specific control activity, often times through the use of sampling.
Inspection	Inspected documents and reports indicating the performance of the control activity.
Walkthrough	Followed the performance of procedures for a specific control activity from inception to conclusion.
Re-Performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether a SSAE 18 report meets the user auditor's objectives, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the processing of the user organization's transactions.
- Understand the flow of significant transactions through the service organization.
- Determine whether the control objectives are relevant to the user organization's financial statement assertions.
- Determine whether the service organization's controls are suitability designed to prevent or detect processing errors that could result in material misstatements in the user organization's financial statements and determine whether they have been implemented.

CONTROL ENVIRONMENT AND RISK ASSESSMENT			
Control Objective 1: Controls provide reasonable assurance that management identifies and assesses risks and provides oversight, standards of conduct, and a structure for carrying out internal controls.			
Ref	**E-FILING'S CONTROLS**	**SERVICE AUDITOR'S TESTS**	**TEST RESULT(S)**
1.1	The FCCC has an organizational structure in place to establish and communicate key areas of authority, responsibility, and appropriate lines of reporting. The organizational structure is reviewed and updated periodically, but not less than annually. The FCCC organization reports to the CEO who reports directly to the Executive Committee.	Obtained a copy of FCCC's most recent organizational chart and noted that the organization reported directly to the Executive Director who reported directly to the executive committee. Through corroborative inquiry with management about the organizational chart, verified that reporting lines and levels of authority and responsibility appeared to be appropriate based on position titles and that the organizational chart was up-to-date and reviewed annually.	No deviations noted.

CONTROL ENVIRONMENT AND RISK ASSESSMENT			
Control Objective 1: Controls provide reasonable assurance that management identifies and assesses risks and provides oversight, standards of conduct, and a structure for carrying out internal controls.			
Ref	**E-FILING'S CONTROLS**	**SERVICE AUDITOR'S TESTS**	**TEST RESULT(S)**
1.2	FCCC maintains established policies and procedures applicable to E-Filing, which outline operating practices and business conduct for employees. Policies and procedures are reviewed periodically (but not less than annually), updated when needed and communicated to employees. The policies and procedures include the following: ■ Employee Handbook ● E-Mail Utilization ● Standards of Conduct ■ Information Security Policies ● General Use and Ownership ● Classification of Information ● Password Security ● Email Use ● Virtual Private Network (VPN) ● Systems Configuration and Management ● Physical Security ● Enforcement	Obtained copies of the FCCC's most recent versions of the policies and procedures listed below, noting the documents were reviewed and included items such as: ■ Employee Handbook ● E-Mail Utilization ● Standards of Conduct ■ Information Security Policies ● General Use and Ownership ● Classification of Information ● Password Security ● Email Use ● Virtual Private Network (VPN) ● Systems Configuration and Management ● Physical Security ● Enforcement Selected a sample of newly hired employees during the examination period and verified that they signed a statement to confirm that they received, read, and understood the employee handbook.	No deviations noted. No deviations noted.

CONTROL ENVIRONMENT AND RISK ASSESSMENT			
Control Objective 1: Controls provide reasonable assurance that management identifies and assesses risks and provides oversight, standards of conduct, and a structure for carrying out internal controls.			
Ref	**E-FILING'S CONTROLS**	**SERVICE AUDITOR'S TESTS**	**TEST RESULT(S)**
1.3	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.	Inspected documentation resulting from the FCCC's risk assessment performed during the examination period and verified that it identified significant risks and internal controls were implemented to address each risk identified.	No deviations noted.
1.4	The FCCC conducts employment background checks and criminal history checks on external candidates selected to fill vacant positions.	Inspected HR evidence that background checks were performed for a sample of new hires during the examination period.	No deviations noted.
1.5	Written position descriptions are maintained by the FCCC. These are periodically updated.	Inspected job descriptions for a sample of employee positions involved with E-Filing activities and verified that job descriptions were updated.	No deviations noted.

CONTROL ENVIRONMENT AND RISK ASSESSMENT			
Control Objective 1: Controls provide reasonable assurance that management identifies and assesses risks and provides oversight, standards of conduct, and a structure for carrying out internal controls.			
Ref	**E-FILING'S CONTROLS**	**SERVICE AUDITOR'S TESTS**	**TEST RESULT(S)**
1.6	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.	Through collaborative inquiry verified that evaluations take place on an annual basis. Inspected annual performance evaluations for a sample of those employees involved with the E-Filing system. Verified the following: ■ Annual performance evaluations were present in the file ■ Each evaluation was signed by the employee and member of management ■ Evaluation included the employees' goals and objectives ■ Evaluation contained feedback and constructive criticism	No deviations noted. No deviations noted.
1.7	The FCCC maintains a high level of control consciousness and oversight of various systems. Specifically, the FCCC has the following audits/reviews: A. Annual Financial Statement Audits B. Annual Technical Security Review C. Third-Party Quarterly Security Reviews	Inspected reports and correspondence from each audit/review to verify that the audits and reviews were performed, and any internal control issues noted were addressed.	No deviations noted.
1.8	The FCCC is organized into the following separate functional areas to provide adequate separation of duties: ■ Systems Engineering and Operations ■ Application Development ■ Service Center ■ Technical Projects ■ Accounting ■ Banking	During the examination observed various duties/ functions being performed by the FCCC staff indicating segregation of functions were in place. Inspected employee rosters to verify that functional areas were separated. Inspected various system configurations to verify that personnel were restricted from accessing functions outside of their assigned areas.	No deviations noted. No deviations noted. No deviations noted.

INFORMATION AND COMMUNICATION			
CONTROL OBJECTIVE 2: Controls provide reasonable assurance that the information and communication component include the procedures and records established by the FCCC to initiate, process, and report the user organizations' (Clerks) transactions and maintain accountability for the transactions.			
Ref	**E-FILING'S CONTROLS**	**SERVICE AUDITOR'S TESTS**	**TEST RESULT(S)**
2.1	See Controls 1.1 and 1.2		
2.2	The FCCC has routine operational meetings to discuss special processing requests, operations, and the development and maintenance of projects.	Through corroborative inquiry verified that operational meetings were performed during the examination period. Inspected operational meeting documentation from a sample of meetings to verify that meetings and any in-scope issues noted were followed up on.	No deviations noted. No deviations noted.
2.3	Members of the Operational Management Team periodically report on operational projects, various operational metrics, and issues to the Florida Courts E-Filing authority Board.	Inspected the minutes of board meetings for a selection of board meetings to verify that Operations Management reported to the board.	No deviations noted.
2.4	The FCCC has implemented an Information Technology Service Management (ITSM) framework and Information Technology Infrastructure Library (ITIL) best practices for FCCC technical projects and selected staff have been trained and earned the ITSM/ITIL Foundation certification.	Inspected ITSM/ITIL employee certifications to verify that employees were certified during the examination period.	No deviations noted.
2.5	The FCCC produces several reports that assist management in the monitoring objective of E-Filing. These reports are distributed to key management and staff and are discussed at routine meetings.	Inspected examples of monitoring reports that Management was provided for meetings to verify that monitoring reports were available for Management. Inspected operational meeting minutes and Board minutes and noted that operational reports were prepared.	No deviations noted. No deviations noted.

INFORMATION AND COMMUNICATION			
CONTROL OBJECTIVE 2: Controls provide reasonable assurance that the information and communication component include the procedures and records established by the FCCC to initiate, process, and report the user organizations' (Clerks) transactions and maintain accountability for the transactions.			
Ref	**E-FILING'S CONTROLS**	**SERVICE AUDITOR'S TESTS**	**TEST RESULT(S)**
2.6	The FCCC has a Service Center function that provides on-going support for E-Filing customers and internal personnel. Procedures are in place to ensure that calls and emails are acknowledged and resolved in a timely manner.	Inspected the Help Desk Policies and Procedures to verify that service center function procedures were in place. Inspected board minutes for a selection of board meetings to verify that the FCCC Service Center Manager reported to the Board regarding Service Center service levels. Inspected the E-Filing portal and noted that it had a support contact information email address to verify that it was in place to provide support, and that emails to this address automatically created a support ticket in the ticket system for support personnel to address and track the incident. Observed and inspected incident tickets with the FCCC Service Center Personnel to verify that calls, voicemails, or emails from customers were tracked and followed up on in a timely manner.	No deviations noted. No deviations noted. No deviations noted. No deviations noted.
2.7	The FCCC provides necessary training to Clerks engaged in services offered by E-Filing. This is to ensure that the Clerks understand how to use and navigate the various systems administered by the FCCC (including E-Filing).	Inspected Clerk users training documentation to verify that training was available to Clerk users. Examined testing documentation for a sample of new clerks to verify that Clerks were trained in the system.	No deviations noted. No deviations noted.
2.8	Procedure Guides have been developed for the users of E-Filing. This is to ensure that the users understand how to navigate the system.	Through inquiry verified the type of training/operational procedures that were in place. Inspected E-Filing portal to verify that user procedure manuals were made available to E-Filing users.	No deviations noted. No deviations noted.

MONITORING ACTIVITIES			
Control Objective 3: Controls provide reasonable assurance that systems are monitored, and deviations, problems and errors are identified, tracked, recorded and resolved in a complete, accurate and timely manner.			
Ref	**E-FILING'S CONTROLS**	**SERVICE AUDITOR'S TESTS**	**TEST RESULT(S)**
3.1	IT operations monitors critical/relevant systems for errors. Errors are logged and alerts are generated to notify IT staff when conditions exceed defined threshold settings.	Inspected the monitoring systems in place and inquired of IT management to validate systems were monitored for the period. Inspected the monitoring systems' configuration to verify they were configured to generate alerts to IT when conditions exceed threshold settings.	No deviations noted. No deviations noted.
3.2	FCCC uses third-party software to monitor the websites and portals to confirm sites are operating and that connections can be made.	Inspected the website monitoring software to verify that connections are configured to be monitored and that authorized emails are configured to receive alerts.	No deviations noted.
3.3	A process exists to ensure that systems incidents, problems, and errors are reported, analyzed, and acknowledged in a timely manner.	Inspected the Help Desk Policies and Procedures to verify that an incident management and escalation process was in place. Observed the service ticket process with the Service Center Personnel to verify that calls or emails from customers or internal users were tracked and followed up on. Inspected a selection of monthly monitoring reports to verify that service tickets were processed in accordance with service level commitments.	No deviations noted. No deviations noted. No deviations noted.

PHYSICAL ACCESS			
Control Objective 4: Controls provide reasonable assurance that physical access to computer system and other system resources are restricted to authorized and appropriate personnel.			
Ref	**E-FILING'S CONTROLS**	**SERVICE AUDITOR'S TESTS**	**TEST RESULT(S)**
4.1	Electronic badge devices control access to all entrances to the FCCC building. The main entrance remains unlocked during business hours (8:00am-5:00pm) for visitors and is locked after business hours.	Verified through inspection that electronic badge readers and/or key locks were used to control access to the FCCC buildings. Observed that main entrance was locked after business hours.	No deviations noted. No deviations noted.
4.2	Electronic badge devices control the access to the FCCC server room. Only specified technical staff have access to this secured location.	Observed an electronic badge reader was installed at the server room entrance to restrict access. Inspected the Access Control System report for users with access to the server room and confirmed with management that access to the server room was appropriate.	No deviations noted. No deviations noted.
4.3	The Facility Manager processes daily access reports from the Access Control system to review for unauthorized physical access.	Observed automated electronic reports were generated daily for review by the Facilities Manager. These reports displayed all traffic in and out of the access doors and alert messages for unauthorized attempts.	No deviations noted.
4.4	Camera system is used to monitor FCCC building entrances and other sensitive areas within the building.	Inspected the recorded video feeds to verify camera systems were installed.	No deviations noted.
4.5	FCCC has an alarm system in place that is monitored by a third-party for unauthorized access to the facilities.	Through corroborative inquiry verified that the alarm system was in place and monitored and authorized staff would be notified in the event of alarm being triggered. Inspected the vendor contract to verify that alarm system was in place and that the vendor was responsible for monitoring for unauthorized access. Inspected vendor invoices for a sample of months to verify that vendor was contracted to monitor the facilities.	No deviations noted. No deviations noted. No deviations noted.

PHYSICAL ACCESS			
Control Objective 4: Controls provide reasonable assurance that physical access to computer system and other system resources are restricted to authorized and appropriate personnel.			
Ref	**E-FILING'S CONTROLS**	**SERVICE AUDITOR'S TESTS**	**TEST RESULT(S)**
4.6	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.	Inspected the building to verify that the front entrance was the only unlocked entrance during normal office hours. Observed that visitor log was in place at the front desk and that it contained visitor log in information. Inspected visitor logs for sample of months to verify that visitors were required to be issued an assigned badge	No deviations noted. No deviations noted. No deviations noted.
4.7	Employee or Contractor access to FCCC facilities is removed upon termination.	Inspected termination documentation for a sample of terminated employees to verify that facility access was removed upon termination. Reviewed with Management and verified that there were no contractors terminated who would have had facility access during the examination period; therefore, no testing was performed.	No deviations noted. The operating effectiveness of the contractor portion of this control could not be tested, as there was no related activity during the examination period.
4.8	Physical controls at the backup third-party data center are monitored by the FCCC staff by confirming that the third-party data center had a third-party attestation report examination performed and that the objectives of Physical Security controls were included.	We inquired of operations personnel and noted that physical access controls observations were documented by the team during their on-site disaster recovery testing.	No deviations noted.

ENVIRONMENTAL CONTROLS			
Control Objective 5: Controls provide reasonable assurance that environmental controls are installed to adequately protect the servers, network equipment, and storage media.			
Ref	**E-FILING'S CONTROLS**	**SERVICE AUDITOR'S TESTS**	**TEST RESULT(S)**
5.1	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 air conditioning systems.	Observed the FCCC server room and verified that air conditioning systems were present in the server room. Inspected the vendor reports to verify the inspections on the air conditioning systems were performed.	No deviations noted. No deviations noted.
5.2	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.	Performed a walk-through of the FCCC server room and observed an installed FM-200 system including the smoke and heat detectors on the ceiling throughout the room. Inspected a FM-200 inspection report to verify that inspections were performed during the period.	No deviations noted. No deviations noted.
5.3	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 annual maintenance.	Performed a walk-through of the FCCC server room and observed UPS units were installed. Inspected the test record logs to verify that UPS units were tested. Inspected the UPS maintenance report to verify that annual maintenance was performed.	No deviations noted. No deviations noted. No deviations noted.
5.4	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.	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 the generator was inspected on an annual basis.	No deviations noted. No deviations noted.

LOGICAL ACCESS AND SECURITY			
Control Objective 6: Controls provide reasonable assurance that security measures are in place around sensitive data and logical access to programs, data, and computer resources is restricted to authorized and appropriate users.			
Ref	**E-FILING'S CONTROLS**	**SERVICE AUDITOR'S TESTS**	**TEST RESULT(S)**
6.1	A network diagram illustrates the physical and logical connections of FCCC information systems and documents the boundaries of the system.	Inspected the FCCC System/Network Diagram to verify that that physical and logical connections were documented.	No deviations noted.
6.2	New or modified access to the network, systems and applications is timely granted or changed after the completion of an access request form that is authorized by appropriate individuals.	Inspected the completed access request form and user access rights for a sample of new system users to verify that the request was authorized by a supervisor or manager. Reviewed the active employee list and noted no changes in employee positions that would indicate a change in access that would have been required and verified with Management that there was no request for access modifications during the examination period therefore no testing was performed.	No deviations noted. The operating effectiveness of the access modification portion of this control could not be tested, as there was no related activity during the examination period.
6.3	Administrator access to the network, application, and related databases is restricted to authorized personnel.	Inspected network, application, and database administrators' system list and inquired with management to verify whether administrator access to systems was appropriate based on the individual's job responsibilities.	No deviations noted.
6.4	A human resources representative notifies security administrators of resignations or terminations of employees or consultants resulting in the person's logon ID being disabled and/or the password reset.	Inspected the current access rights for a sample of terminated employees to verify their network and application security access was updated and access was removed. Inspected termination documentation for a sample of terminations to verify that logical access was removed timely.	No deviations noted. No deviations noted.

LOGICAL ACCESS AND SECURITY			
Control Objective 6: Controls provide reasonable assurance that security measures are in place around sensitive data and logical access to programs, data, and computer resources is restricted to authorized and appropriate users.			
Ref	**E-FILING'S CONTROLS**	**SERVICE AUDITOR'S TESTS**	**TEST RESULT(S)**
6.5	Windows network system, password management controls include the following: ■ Minimum Password Length ■ Password Expiration/Change Frequency ■ Password Complexity ■ Invalid Password Attempts ■ Password Storage	Inspected the network domain security password settings and noted that minimum password length, password expiration/change frequency, password complexity, invalid password attempts, and password storage were enforced.	No deviations noted.
6.6	VPN connections are utilized over public networks for encrypting sensitive information and management limits the remote access to authorized individuals.	Inspected the VPN settings to verify that VPN rules control remote access, user account and password was required, and that encrypted connection was required. Inspected VPN rules to verify that users were restricted to authorized personnel.	No deviations noted. No deviations noted.
6.7	The E-Filing portal web application requires users to login and submit password via secure connection using HTTPS requiring RSA 256 encryption.	Inspected the web application software to verify whether security protocol (Hypertext Transport Protocol Secure) was enabled. Observed the secure web application to verify that a username and password was required for access. Inspected the SSL configuration of the web server to verify SSL certificate was current.	No deviations noted. No deviations noted. No deviations noted.
6.8	A Uniform Resource Locator (URL) filter is in place to detect and block potentially malicious links from being accessed.	Inspected URL filter configuration to verify that the configuration was in place to detect and block potentially malicious links.	No deviations noted.

LOGICAL ACCESS AND SECURITY			
Control Objective 6: Controls provide reasonable assurance that security measures are in place around sensitive data and logical access to programs, data, and computer resources is restricted to authorized and appropriate users.			
Ref	**E-FILING'S CONTROLS**	**SERVICE AUDITOR'S TESTS**	**TEST RESULT(S)**
6.9	A firewall is in place to control network traffic and prevent unauthorized traffic from passing between the internal and external networks.	Inspected the firewall configuration to verify that a firewall was in place to control network traffic and prevent unauthorized traffic from passing between the internal and external networks. Inspected the system generated list of firewall administrators and inquired of management to verify their access was authorized.	No deviations noted. No deviations noted.
6.10	Various FCCC functions are separated into VLANs that provide access restrictions.	Inspected the network configurations to verify that VLANS were in place separating FCCC functions and access restrictions were enforced.	No deviations noted.
6.11	Anti-virus software is installed and configured on all production Windows servers, email gateway, and workstations to automatically scan and update virus definitions on a daily basis.	Inspected the anti-virus software configuration on a selection of Windows production systems and workstations to verify that anti-virus software was configured to automatically scan and update virus definitions on a daily basis. Inspected the email gateway configuration to verify that the email traffic is scanned for malware and/or anti-virus and is blocked and alerts are sent to IT administrators. Inspected the system generated list of anti-virus administrators and inquired of management to verify their access was authorized.	No deviations noted. No deviations noted. No deviations noted.
6.12	Vulnerability assessments are performed by a third-party vendor to test for known vulnerabilities on the network and production systems annually.	Reviewed the independent third-party vulnerability test results to verify that vulnerability assessments were performed by a third-party vendor annually. See 6.13 testing below.	No deviations noted.

LOGICAL ACCESS AND SECURITY			
Control Objective 6: Controls provide reasonable assurance that security measures are in place around sensitive data and logical access to programs, data, and computer resources is restricted to authorized and appropriate users.			
Ref	**E-FILING'S CONTROLS**	**SERVICE AUDITOR'S TESTS**	**TEST RESULT(S)**
6.13	A security consulting company, under contract with the FCCC, performs an annual review of the FCCC system's security within which E-Filing 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. Remediation plans are put in place to address identified deficiencies based on risk.	Inquired to FCCC Management about the security consulting engagement and method of addressing recommendations. Inspected the security consulting report to verify that the review was performed and confirmed with Management that based on risk, remediation plans were put in place to address recommendations.	No deviations noted. No deviations noted.
6.14	IT personnel periodically review availability of patches on production systems and critical patch updates are installed by IT personnel.	Inspected logs of updates and implemented patches within the examination period to verify that critical patch updates were installed by IT personnel.	No deviations noted.
6.15	FCCC uses managed software to enforce security on Personal Digital Assistant (PDA) devices.	Inspected the written PDA policy contained in the Security Policies and Procedures document to verify that requirements were in place. Inspected mobile device managed software to verify that policy requirements were enforced.	No deviations noted. No deviations noted.
6.16	FCCC Encrypts backup data at rest.	Inspected backup configuration setting to verify that data is encrypted.	No deviations noted.

SYSTEM CHANGE MANAGEMENT			
Control Objective 7: Controls provide reasonable assurance that changes to systems, applications, databases, and infrastructure are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.			
Ref	**E-FILING'S CONTROLS**	**SERVICE AUDITOR'S TESTS**	**TEST RESULT(S)**
7.1	Management authorizes and approves the implementation of new and changes to existing systems, applications, and databases according to approved policies.	Inspected the FCCC Change Management Policy and noted that it specifies approval requirements. Inspected board minutes to verify that status of E-Filing portal changes deployments was reported by the Change Advisory Board (CAB) to the Board of Directors. Inspected release documentation for a sample of deployed releases to verify that the release was approved by the CAB. Inspected change documentation for a sample of application changes to verify that the change was approved for deployment by Management. Inspected Infrastructure System change tickets deployed during the examination period and verified that changes were approved by Management for implementation.	No deviations noted. No deviations noted. No deviations noted. No deviations noted. No deviations noted.
7.2	When applicable, based on the risk, FCCC tests changes to applications, and databases in a segregated environment prior to system implementation.	Inspected the change documentation for a sample of changes to verify that testing was performed prior to system implementation. Inspected the system documentation to verify that there were segregated environments between testing and production.	No deviations noted. No deviations noted.

SYSTEM CHANGE MANAGEMENT			
Control Objective 7: Controls provide reasonable assurance that changes to systems, applications, databases, and infrastructure are authorized, tested, documented, approved, and implemented to result in the complete, accurate, and timely processing and reporting of transactions and balances.			
Ref	**E-FILING'S CONTROLS**	**SERVICE AUDITOR'S TESTS**	**TEST RESULT(S)**
7.3	System change deployments are restricted to authorized personnel.	Inspected system change documentation for a sample of deployed system changes to verify that deployment to production was performed by authorized personnel. Inspected access configurations for application and database servers and the database systems to verify that system changes were restricted to authorized personnel.	No deviations noted. No deviations noted.
7.4	System changes are evaluated for risk and, based on the risk, rollback plans are required.	Inspected the change documentation for a selection of system changes to verify the changes were evaluated for risk and that rollback plans were required based on the risk.	No deviations noted.
7.5	Source code management software is utilized for version control of development projects and to control access to source code libraries.	Inspected the configuration of the source code management software to verify that software was used to manage version control of development projects and to control access to source code libraries.	No deviations noted.

BACKUP AND RECOVERY			
Control Objective 8: Controls provide reasonable assurance that critical applications and data are backed up regularly and are available for restoration in the event of processing errors or unexpected processing interruptions.			
Ref	**E-FILING'S CONTROLS**	**SERVICE AUDITOR'S TESTS**	**TEST RESULT(S)**
8.1	At a minimum, daily application server and database backups are performed.	Inspected server and database backup configurations utilized by FCCC staff to verify that backups were performed as scheduled.	No deviations noted.
8.2	IT administrators are alerted in the event that a backup process fails.	Inspected the IT administrator's email inboxes for backup alerts to verify that backup processes were monitored for failure.	No deviations noted.
8.3	Restoration procedures for recovery of data have been developed and are tested at least annually.	Inspected annual data restoration tests to verify whether the recovery process was configured to successfully recover data.	No deviations noted.

TRANSACTION PROCESSING AND RECONCILIATION			
Control Objective 9: Controls provide reasonable assurance that transactions that are processed through the E-Filing portal system are authorized, recorded completely, accurately, and timely.			
Ref	**E-FILING'S CONTROLS**	**SERVICE AUDITOR'S TESTS**	**TEST RESULT(S)**
9.1	See Control 1.8		
9.2	The FCCC Accounting function performs monthly bank reconciliations of E-Filing bank accounts. The E-Filing 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 E-Filing. The bank reconciliations are reviewed by FCCC Senior Management.	Inspected the bank reconciliation for a sample of months during the examination period to verify the following: ■ Verified that reconciling items were properly documented and that the FCCC provided reasonable explanations as to the nature of the reconciling items. ■ Verified that source documents existed and were available for amounts on the bank reconciliations. ■ Verified the mathematical accuracy of the bank reconciliations selected. ■ The reconciliation was completed timely (within 30 days of month-end). Inspected bank reconcilement review sheets for a sample of months that the required review and approvals were performed by FCCC Management and was documented.	No deviations noted. No deviations noted.
9.3	Transactions that flow through the E-Filing portal are automatically sequentially numbered and assigned as unique identifier. Orders are given a unique identifier at the point that users initiate transactions and are stored in the E-filing database.	Inspected the E-Filing database and verified that transactions entered in the examination period were assigned a sequential unique identifier and based on sample of transactions reviewed that the required fields were populated.	No deviations noted.

TRANSACTION PROCESSING AND RECONCILIATION			
Control Objective 9: Controls provide reasonable assurance that transactions that are processed through the E-Filing portal system are authorized, recorded completely, accurately, and timely.			
Ref	**E-FILING'S CONTROLS**	**SERVICE AUDITOR'S TESTS**	**TEST RESULT(S)**
9.4	The E-Filing filer input screens provides input validity checks for various critical required fields that must be passed before acceptance of the data from the user and in addition a user account and password is required to access the portal. First time filers receive two separate email notifications associated with the account setup process as part of the registration and confirmation process. A process is in place to confirm filing on the portal screen and that the filer is automatically notified and sent an email confirmation that the case was successfully submitted.	Observed the input screens and tested that input validation checks were performed, and invalid data input was rejected before the data was accepted. Observed that payer users must have an established account and a password before accessing the web site, and a new user must follow the account setup process before accessing the site. Observed that a payer user was automatically notified on the portal screen that a file was successfully submitted and that an automatic confirmation email was sent to the filer.	No deviations noted. No deviations noted. No deviations noted.
9.5	The FCCC utilizes an interface called the "IPAS reconciliation system" (Access database) between E-Filing portal 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. **Note: During November 2021, portal transactions were migrated to a new process which does not utilize the IPAS reconciliation system.**	Inspected reports generated from the IPAS system. Verified the accuracy and completeness of the reports by re-footing the total of the reports and reconciled the repot totals to the bank statement totals. Traced selected receipt/disbursement records for a sample of transactions from the IPAS database through to the accounting system and bank statements to verify agreement to the underlying database. Observed the reconciliation procedure being performed and verified the consistency with the documented reconciliation process.	No deviations noted. No deviations noted. No deviations noted.

TRANSACTION PROCESSING AND RECONCILIATION			
Control Objective 9: Controls provide reasonable assurance that transactions that are processed through the E-Filing portal system are authorized, recorded completely, accurately, and timely.			
Ref	**E-FILING'S CONTROLS**	**SERVICE AUDITOR'S TESTS**	**TEST RESULT(S)**
9.6	The FCCC Accounting function scans physical paper checks for certain transactions received in the mail daily. The scanning process electronically sends a deposit to E-Filing bank accounts. All other payments made on-line via credit card or e-check in E-Filing are automatically sent as a deposit to E-Filing bank accounts through E-Filing 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.	Performed a walkthrough of the paper scan process with the banking person who performed the process and verified the following: ■ The deposit was automatically sent to the E-filing bank account. ■ A report was produced as the deposit slip. ■ Verified the accuracy of the report with information entered. ■ Agreement of the total deposited to the check total that was logged by the mail clerk. Reperformed the process by reconciling the deposit documentation for a sample of months from the bank statement to the mail logs to verify that deposits were logged correctly. Inspected the mail logs from the above test to verify that the mail clerk signed off on the mail log.	No deviations noted. No deviations noted. No deviations noted.
9.7	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 E-Filing 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 4) staff initials performing the process.	Performed a walk through with banking personnel of the daily ACH file confirmation process to verify the process agrees with documented 9.7 control. Inspected daily logs for a sample of days to verify the ACH process had been performed and documented in the ACH File Transfer Log for the following: ■ Confirmation Number ■ Date of File ■ ACH Dollar Amount ■ Staff Initials	No deviations noted. No deviations noted.

TRANSACTION PROCESSING AND RECONCILIATION			
Control Objective 9: Controls provide reasonable assurance that transactions that are processed through the E-Filing portal system are authorized, recorded completely, accurately, and timely.			
Ref	**E-FILING'S CONTROLS**	**SERVICE AUDITOR'S TESTS**	**TEST RESULT(S)**
9.8	E-Filing portal 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)	Observed FCCC staff attempting to make several credit card payments on the E-Filing portal using invalid credit card numbers or invalid addresses to verify automatic authorization process.	No deviations noted.

SERVICE FEE			
Control Objective 10: Controls provide reasonable assurance that service fees are properly charged based on approved schedules.			
Ref	**E-FILING'S CONTROLS**	**SERVICE AUDITOR'S TESTS**	**TEST RESULT(S)**
10.1	E-Filing has an approved (contractual) service fee schedule governing on-line transactions.	Obtained the approved fee schedule from Management and confirmed that the fee schedule was approved.	No deviations noted.
10.2	E-Filing portal automatically calculates the service fee based on the type of payment and approved fee structure.	Observed for the several types of payment that the E-Filing portal automatically charged as a service fee based on type of payment and verified the amounts agreed with the approved fee schedule. Inspected a selection of payment transactions to verify that the correct service fee was charged.	No deviations noted. No deviations noted.
10.3	Users are informed prior to submitting on-line payment of the service fee charged. In addition, the user is requested to confirm order (payment information).	Observed that the E-Filing portal website informed the user of the service fee amount prior to submitting the order and that the user was requested to confirm the order.	No deviations noted.