FIU | FLORIDA INTERNATIONAL UNIVERSITY

Office of Internal Audit

Audit of the Center for Children and Families

Report No. 17/18-11

May 1, 2018

FLORIDA INTERNATIONAL UNIVERSITY

OFFICE OF INTERNAL AUDIT

MEMORANDUM

DATE: May 1, 2018

TO: William E. Pelham Jr, Director - Center for Children and Families

FROM: Allen Vann, Chief Audit Executive

SUBJECT: **Audit of the Center for Children and Families, Report No. 17/18-11**

We have completed an audit of the Center for Children and Families (Center) for the period from July 1, 2015 through January 31, 2017. The primary objective of our audit was to evaluate whether financial controls and procedures relating to the Center's revenue and expenditures are: (1) adequate and effective; (2) being adhered to; and (3) in accordance with University policies and procedures, State and Federal laws and regulations, including the Office of Management and Budget Uniform Guidance. In addition, our objective ensured that Information Technology risks are mitigated.

With its 36 employees and a team of researchers and clinicians, the Center provides state of the art services to approximately 3,500 families each year through clinical services and research programs. The Center has also provided professional development training to more than 6,000 teachers and nearly 450 schools. The Center generated total revenues of $14 million and incurred total expenses of $16.4 million, while receiving an additional $2 million in E&G funding.

Our audit disclosed that controls over the Center operations needs strengthening, particularly in the areas of: revenue controls, employee background checks, and gift card controls. We also identified Information Technology areas that need strengthening particularly in malware prevention, review of audit logs, off-boarding user access, disabling non-active firewall rules, and business continuity plan procedures. The audit resulted in 25 recommendations, which management agreed to implement.

We would like to take this opportunity to express our appreciation to you and your staff for the cooperation and courtesies extended to us during the audit.

Attachment

C: FIU Board of Trustees
Mark B. Rosenberg, University President
Kenneth G. Furton, Provost and Chief Operating Officer
Kenneth A. Jessell, Chief Financial Officer and Senior Vice President
Javier I. Marques, Chief of Staff, Office of the President
Robert Grillo, Vice President of Information Technology and CIO
Michael R. Heithaus, Dean - College of Arts, Sciences and Education

TABLE OF CONTENTS

OBJECTIVES, SCOPE AND METHODOLOGY

Pursuant to our approved annual plan for 2016-2017, we have completed an audit of the Center for Children and Families (CCF/Center) for the period from July 1, 2015 through January 31, 2017. The primary objective of our audit was to evaluate whether financial and operational controls and procedures relating to the Center's revenue and expenditures are: (1) adequate and effective; (2) being adhered to; and (3) in accordance with University policies and procedures, State and Federal laws and regulations, including the OMB (Office of Management and Budget) Uniform Guidance. Our objective was also to ensure that Information Technology risks are mitigated.

Over 92% of the Center's revenues were generated from grant funds (see page 2 for financial details). Since grant funds revenues are mainly the result of expenses reimbursed, our audit of revenue-related transactions focused on other unrestricted funds. Similarly, grant funds accounted for 81% of all expenses, followed by E&G (Education & General) funds (13%), and other unrestricted funds (6%). Our audit focused on expenditure transactions from two selected grants, along with E&G and other unrestricted funds expenditures.

We also examined information technology controls to ensure the confidentiality, availability, and integrity of the Center's sensitive data. We reviewed University policies and procedures, and applicable State and Federal laws and regulations, observed current practices and processing techniques, interviewed responsible personnel, and tested selected transactions and devices. Grants selected and samples sizes used for testing were determined on a judgmental basis.

The audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing and included tests of the accounting records and such other auditing procedures, as we considered necessary under the circumstances.* To accomplish specific Information Technology control objectives, we applied a governance, risk and compliance framework, which utilizes the *Control Objectives for Information and Related Technology (COBIT) 5.0 Framework and the National Institute of Standards and Technology (NIST) Special Publications (SP) 800-53A Revision (Rev.) 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations*. Audit fieldwork was conducted from March 2017 through July 2017 and from late September 2017 through January 2018.

This was our first internal audit conducted of the Center for Children and Families. There were no other prior recommendations related to the Center.

BACKGROUND

The Center for Children and Families (CCF/Center) is an FIU Preeminent Program clinical research center for children and families struggling with mental health problems. Their mission is to develop models for evidence-based, cost effective, integrated clinical services for children and adolescents with mental health and learning problems that are exportable for primary care-based, clinic-based, school-based, and community-based care throughout the United States and internationally. CCF provides the infrastructure for a focused array of research, services, and education that spans a variety of mental health and educational problems.

CCF provides state of the art services to approximately 3,500 families each year through clinical services and research programs. Some of their services include early childhood services, individualized and group programs for parents, group and home-based therapy for children, nationally acclaimed summer camp programs, and Video Teleconferencing therapy.

CCF also provides education and training opportunities for the next generation of mental health professionals nationwide through academic programs offered at the FIU Department of Psychology and the Summer Treatment Program (STP). They also provide continuing education opportunities in evidence-based approaches for psychologists, mental health professionals, and educators. Through CCF's partnership with Miami-Dade County Public Schools (M-DCPS) and The Children's Trust, the Center has also provided professional development training to more than 6,000 M-DCPS teachers and nearly 450 schools.

Financial Details

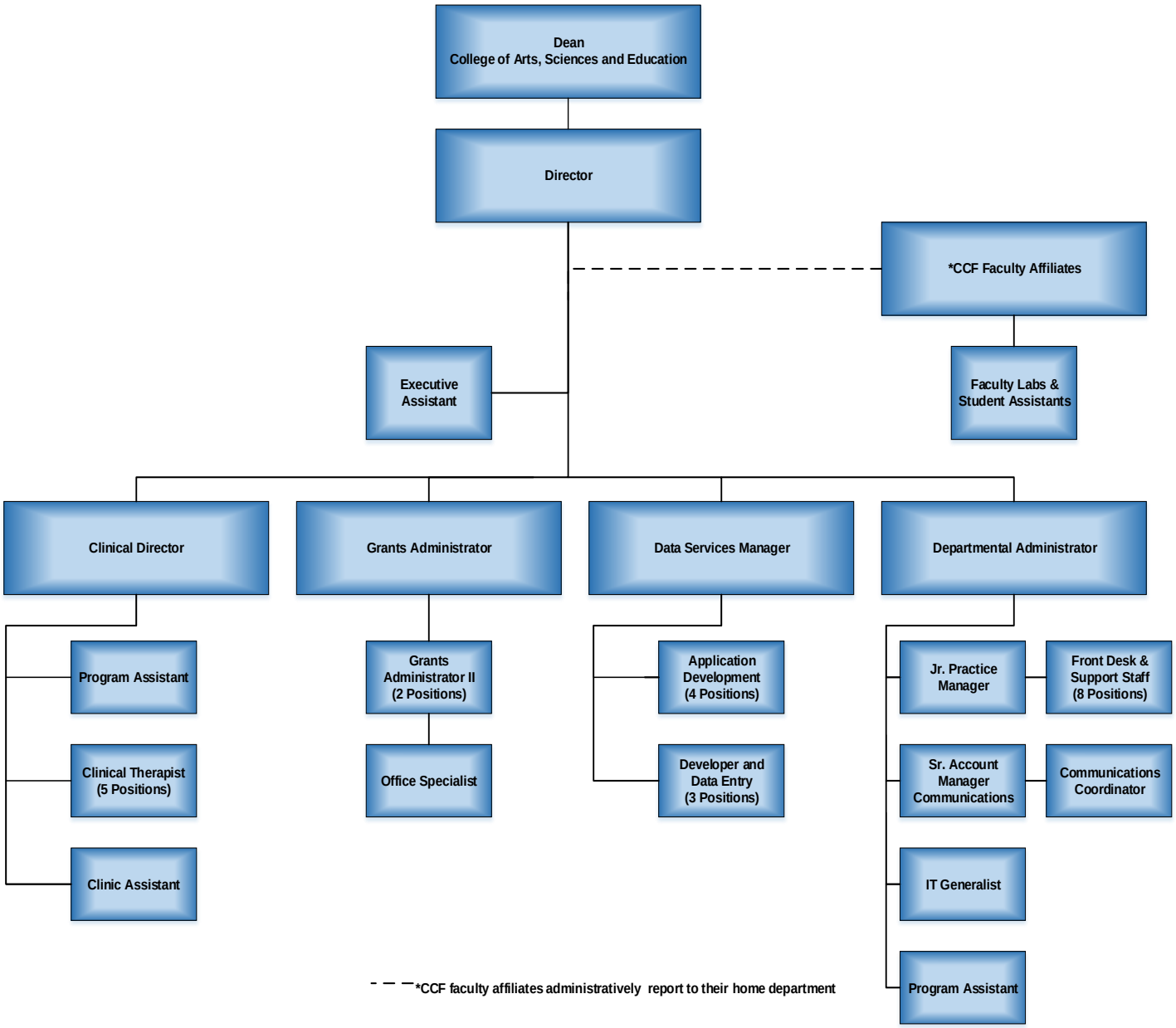
During our audit period from July 1, 2015 through January 31, 2017, the Center's financial results were as follows:

Fund Type	Revenues	Expenses	Difference
Grant Funds	$ 12,940,491	$ 13,228,012	$ (287,521)
Other Unrestricted Funds	948,179	958,689	(10,510)
Foundation Funds	81,280	80,444	836
Auxiliary Funds	30,377	39,852	(9,475)
Scholarship Funds	-	18,844	(18,844)
Education and General (E&G) Funds[1]	-	2,046,970	(2,046,970)
Totals[1]	**$ 14,000,327**	**$ 16,372,811**	**$ (2,372,484)**

[1] The Center received appropriations sufficient to cover the expenses of $2,046,970 from E&G funding. Thus, the actual difference was $(325,514).

Personnel

As of February 2018, CCF consists of 36 employees, along with a team of researchers and clinicians who report administratively to their home departments.



FINDINGS AND RECOMMENDATIONS

Our audit disclosed that the Center's controls and procedures needs improvement. We found that internal controls should be strengthened in the following areas: revenue controls, employee background checks, and gift card controls. Additionally, the Center needs to continue to strengthen their information security controls. Opportunities for improvement include malware prevention, audit logs reviews, off-boarding users, disabling non-active firewall rules, and continuity plan procedures. Our overall evaluation of internal controls is summarized in the table below.

INTERNAL CONTROLS RATING			
CRITERIA	**SATISFACTORY**	**FAIR**	**INADEQUATE**
Process Controls		**X**	
Policy & Procedures Compliance		**X**	
Effect		**X**	
Information Risk		**X**	
External Risk		**X**	

INTERNAL CONTROLS LEGEND			
CRITERIA	**SATISFACTORY**	**FAIR**	**INADEQUATE**
Process Controls	Effective	Opportunities exist to improve effectiveness	Do not exist or are not reliable
Policy & Procedures Compliance	Non-compliance issues are minor	Instances of non-compliance are evident	Non-compliance issues are pervasive, significant, or have severe consequences
Effect	Not likely to impact operations or program outcomes	Impact on outcomes contained	Negative impact on outcomes
Information Risk	Information systems are reliable	Data systems are mostly accurate but need to be improved	Systems produce incomplete or inaccurate data which may cause inappropriate financial and operational decisions
External Risk	None or low	Moderate	High

SECTION I
Financial and Operational Controls

1. Controls over Revenues

The Center's revenues totaled $14 million, of which $12.9 million were grant related and thus, mainly the result of expenditure reimbursements. Of the remaining $1.1 million, we tested 86%. We examined the Summer Treatment Program (STP), totaling $593,690, and other clinical services fees, totaling $354,489, to ensure fees charged were properly assessed and collected.

In order to test program fees assessed, we requested and examined the documents contained in each selected client's file. This information was compared against the fee schedules for each program. The results of our testing follows.

Summer Treatment Program (STP) Fees

The Summer Treatment Program (STP) is an 8-week comprehensive summer camp program for children ages 5-12 with ADHD (Attention Deficit Hyperactivity Disorder) and related behavioral, emotional, and learning challenges. STP is funded by service fees and The Children's Trust. Fees for the STP vary as they are based on family size and household income. This is determined during the application and screening process. We selected 34 out of 136 clients enrolled in the 2016 STP to ensure fees charged were properly assessed and collected. We reviewed all pertinent invoices for the clients selected and found anomalies with 15 of the 34 (44%) clients' fees, as follows:

- For 11 clients, either the fee assessed and collected was not in accordance with the established fee guideline or the files lacked adequate supporting documentation to properly determine the household income.
    - For 7 clients, the assessed fees were less than those mandated by the established fee guidelines.
        - For four clients (two families each with two children), the fee assessment was based on a total of $800 per family ($400 per child). However, based on their individual household income and family size the clients should have been charged $1,200 ($600 per child). As a result, the Center under-assessed the two families a total of $800.
        - For three clients (one family with three children), the Center obtained a 2014 tax return for only one parent and billed a total of $2,400 for the three children ($800 per child) based on the one tax return. However, since the *Client Registration Form* disclosed a 50/50 custody situation and a household income in excess of $150,000, the Center should have charged a total of $6,000 ($2,000 per child). As a result, the clients' fee was under-assessed by $3,600.

- For 3 clients, the Center assessed fees based on incomplete or no tax return information:

    - For one client, no tax return was obtained but the Center billed the client the minimum amount of $400 per child.

    - For two clients, the Center obtained the tax return of only one parent and billed the client the minimum amount of $400 per child. However, the *Client Registration Form* disclosed that those parents were both married. Therefore, the Center should have either obtained each parent's tax return or otherwise billed the maximum amount.

- For 1 client, the family was initially billed $1,400. However, the client appealed for a fee reduction via email and the Center reduced the fee to $1,000. We were informed that the Clinical Director verbally approved the reduction of the fee. However, in the absence of written procedures for approval of a fee reduction, we could not evaluate the appropriateness of the fee reduction.

- For 4 clients, the Center did not collect the full amount that was billed and a payment plan was not adequately documented.

    - In three instances, a *Financial Agreement Form* was provided to the client. However, a total of $580 remained uncollected.

        - In one instance, a letter was sent to the client to notify them of service termination. Nonetheless, no payment was received and the service was not terminated.

        - In another instance, the client did not sign the *Financial Agreement Form* and the service was still provided.

    - In one instance, the Center incorrectly credited $150 to a client's account when no payment had been collected.

Clinical Services Fees

We tested the Saturday Treatment and Individual Treatment programs as they generated $318,518, representing 90% of all clinical services fees revenues. The Center requires each clinician to complete a *Daily Client Encounter Form*, which includes the type of services and number of hours provided, the clinician's education level, and the amount to be charged. We selected 14 clients to determine if their fees were properly assessed and collected.

- For 11 of the 14 clients (79%), a *Daily Client Encounter Form* was not evident. As such, we were unable to determine if the fees assessed were appropriate.

- For 1 of the 3 clients with a *Daily Client Encounter Form* found, a $50 fee for one-hour of service provided by a PhD level clinician was charged. According to the Center's clinical fee schedule, services provided by PhD clinicians should be assessed at $200 per hour.

In addition, we reviewed 20 *Daily Client Encounter Forms* for one clinician where the minimum fee per the guidelines was $10 and the maximum fee was $50. Clients who received the identical clinical services from that clinician were charged different amounts, ranging from no fee in four instances to $50. The clients were not asked to provide any household income or family size documentation.

The Individual Treatment Program revenues totaled $253,129 for our audit period. Related revenue reconciliations performed by the Center were inaccurate. The reconciling items omitted revenues collected, and excluded refunds provided to clients. Net differences totaled $20,136. Upon inquiry, the Center staff re-performed the reconciliation and corrected the discrepancies.

Cash Collection

According to University Policy No. 1110.010, *Cash Control Policy*, and Departmental Cash Collection procedures, all checks or money orders must be made out to Florida International University and must be restrictively endorsed immediately upon receipt. All checks are to be brought to Student Financials within 48 hours of receipt for bank deposit.

Cash collection controls were tested to ensure that checks collected by the Center were properly endorsed and timely deposited. We tested five deposits, totaling $2,870. The sample included a combination of 40 checks and money orders received by the Center. We found the following during our review:

- 39 of the checks were deposited 3 to 41 days after receipt, with an average of 18 days.

- Checks and money orders were placed inside a drawer to be deposited but were not properly endorsed. Personnel were unaware of the required endorsement procedures.

Client Files

As part of our revenue testing, we examined the client files provided. The files provided support for the amounts charged as they include the *Client Registration Form*, tax returns, any financial agreement forms, the *Daily Client Encounter Form,* and etcetera. The Center currently maintains the client files in a locked file room where any personnel working on the case needs to request access. A log of the file request, receipt, and return date is maintained on a "*Clinic File Sign-out Sheet*" which is managed by the administrative staff. We noted the sign-out sheet was missing some key information such as the file return date and the name of the person who received the file. In addition, the files provided

during our testing, including those requested that were being used by the staff, were not recorded on the sign-out sheet.

Recommendations

Center for Children and Families should:	
1.1	Obtain and review required documents from clients and properly assess fees for various programs based on established fee schedules and criteria.
1.2	Ensure that a financial payment plan is properly completed and signed by the client and CCF staff and monitor payment plans to ensure collection of fees.
1.3	Establish criteria or guidelines for fee waivers or reductions, and document all waivers/reductions.
1.4	Ensure the general ledger accounts are reconciled monthly.
1.5	Ensure checks are being timely deposited (within 48 hours) and properly endorsed.
1.6	Maintain complete records of client file checkout on the "*Clinic File Sign-Out Sheet"*.

Management Response/Action Plan:

1.1 The intake department quotes families over the phone based on their responses to household income and the number of people living in the home. Once they come in, they will have to bring a copy of their most recent tax form (1040, 1040A, or 1040 EZ) along with a W2, 1099, or Schedule C from their current employer or business so that we can verify their income and to properly quote them a fee. Families who have "shared custody" (if listed on the client registration form) will have to provide forms from both parents so that both incomes can be combined and included.

Implementation Date: Fall 2018

1.2 We have made multiple changes to ensure that payment plans are completed and signed and to facilitate the collection of fees. Payment plan forms are currently generated electronically as a pilot for the Summer Treatment Program-Elementary, to be rolled out for the rest of the clinic programs, in order to facilitate the signing of the form and to easily monitor for payments. Families, who have not signed the form, will receive daily-automated reminders via email to sign, after appropriate consent is obtained. In order to more easily collect payment, we will ensure that payment plans are shorter (do not exceed the duration of the program) to ensure). We will also be working on a collection procedure for addressing unpaid balances.

Implementation Date: Fall 2018

1.3 Families who are requesting a reduced fee must now complete a Request for Reduced Fee form. The form is to be completed by the parent/legal guardian requesting the reduction and should include any applicable supporting documents. Approved families (by the Clinical Director) will receive a standard 25% discount and will have to sign a new financial agreement form with their new fee.

Implementation Date: Immediately

1.4 We are downloading the general ledger report from FIU PantherSoft Financials on a monthly basis for our clinical accounts. We are then uploading the information onto a reconciliation worksheet and addressing any discrepancies for that month, as compared to our internal financial tracking mechanism.

Implementation Date: Immediately

1.5 Upon learning that the check endorsement was a requirement, the change was implemented immediately. Now, at the time of receipt, the front desk staff member handling the payment stamps the back of the check with the appropriate endorsement. Additionally, beginning in March 2018, we have been depositing checks on Mondays, Wednesdays, and Fridays, which allows all checks to be deposited within 48 hours of payment.

Implementation Date: Immediately

1.6 The CCF has transitioned to the use of electronic medical records; therefore, there will not be a need to maintain a "clinic file sign-out sheet" to track files being signed out. Staff will access files electronically.

Implementation Date: Immediately

2. Expenditure Controls

The Center's expenditures totaled $16.4 million, of which $10.4 million were payroll related, and are covered in Finding No. 3, Personnel Administration, on page 15. Of the non-payroll related expenditures, we tested 120 transactions, totaling $581,647. These transactions, which included expenditures from two grants, as well as E&G and other unrestricted funds, were tested for compliance with University policies and procedures and applicable laws, rules, and regulations. The results of our testing follows.

Credit Card and Other Purchases

We tested 41 transactions, totaling $500,808, related to other than credit card or travel transactions, and found them to be appropriate, allowable, and in accordance with University policies and procedures, applicable laws, rules, and regulations.

We also tested 59 credit card transactions, totaling $72,490, and found 10 exceptions, as follows:

The Department Card Guidelines and Procedures Manual provides a list of items that may not be purchased with the Departmental Card unless pre-authorized by the Controller's Credit Card Solutions program team. Some unallowable purchases include gratuity exceeding 15%, items shipped to a personal home address, promotional items, and Florida sales tax.

- We found seven transactions, totaling $6,564, where unallowable purchases were made.

    - Two transactions, totaling $5,809, were for the purchase of promotional items for recruitment purposes. These purchases were made from an E&G fund. Promotional items are explicitly listed as unallowed in both the funding and departmental card guidelines.

    - Three transactions, totaling $524, were related to pizza delivery orders where the gratuity ranged from 20% to 43%.

    - One transaction for the purchase of medical supplies, totaling $181, was shipped to an employee's home address.

    - Another transaction included $50 in Florida sales taxes.

In addition, 4 of the 59 credit card transactions were for the purchase of gift cards used in the Center's research. We found the following exceptions:

Per the FIU Gift Card procedures, the PI (Principal Investigator) or designee must maintain a Gift Card Distribution Log and a Gift Card Monthly Reconciliation Form for all gift card purchases. The reconciliation should verify the physical cards against the

distribution log. Any discrepancies must be logged into the Gift Card Distribution Log. The reconciliation should then be signed by the PI and a copy must be sent to the Office of the Controller.

- The log and reconciliation form for one gift card transaction, totaling $1,308, was not evident. We were informed that the log and reconciliation form was lost.

- Two transactions, totaling $12,360, for the purchase of gift cards did not reconcile to the distribution log provided:

    - We obtained the reconciliation form and invoice for the purchase of 68 gift cards worth $20 each, totaling $1,360. However, the distribution log stated that 69 gift cards were distributed. No discrepancy was noted by the preparer or reviewer in the reconciliation log.

    - We found the reconciliation form and invoice for the purchase of 110 gift cards worth $100 each, totaling $11,000. However, the distribution log stated that 127 gift cards were distributed. No discrepancy was noted by the preparer or reviewer in the reconciliation log.

In addition, we contacted the Office of the Controller in reference to the reconciliation forms that should be provided to them. We found that there currently is no process in place as to what should be done after receiving the reconciliation form. They are currently stored in a stack with no monitoring process. We were unable to locate any forms related to the samples selected.

Travel Expenditures

We examined 20 travel transactions, totaling $8,349, and found the following exceptions:

- An approved Travel Authorization (TA) is the traveler's permission to incur expenses and travel on behalf of the University. This includes employees and students traveling on behalf of the University. Payment of travel expenses using the procurement card or by the traveler is prohibited without an approved TA.

  There were 24 instances within 14 Expense Reports (ER), totaling $4,111, where airline travel and/or conference registration fees were paid without an approved TA.

- The Travel Manual indicates that after returning from a trip or incurring an expense, reimbursement is made by completing an ER with accompanying receipts. The ER must be submitted within 10 business days after the completion of the trip or incurrence of the expense.

  There were 14 instances where the ERs, totaling $6,132, were submitted between 1 and 79 business days late.

- The University Travel Manual states that travelers may not be reimbursed for airfare purchased using reward points or mileage memberships. We found one instance, totaling $112, where the employee used mileage points to purchase the airfare ticket, which was fully reimbursed.

Recommendations

Center for Children and Families should ensure:	
2.1	Compliance with the University's Department Card Guidelines and Procedures Manual and University funding guidelines.
2.2	Gift Card Distribution Logs are properly maintained and reconciled per University procedures.
2.3	Compliance with University travel policies and procedures.

Management Response/Action Plan:

2.1 The CCF has instituted a monthly new employee orientation where an introduction to purchasing guidelines are shared. CCF Administrative staff (who oversee purchases on the Department's E&G accounts) have also been given guidance on the prohibition of paying for promotional items from E&G accounts. Reviewers and approvers pay close attention to the correct account identification, the allowability of the charge, and the waiver of FL sales tax. When reviewers find an instance that is questionable, they contact the Pcard holder for additional information and include comments on the resolution of the issue with the transaction record. Pcard holders who have made a mistake are asked to make reasonable attempts to correct the mistake (i.e., obtain a refund for sales tax, refund FIU for purchases that were not allowable and explain in writing how the mistake occurred and steps taken to avoid a recurrence).

Implementation Date: Immediately

2.2 The CCF Grants Office has instituted a tracking spreadsheet in REDCap that identifies which projects are out of compliance with monthly reconciliation expectations. On a monthly basis, the Grants Office will run the report and inform Principal Investigators and Gift Card Custodians that they need to reconcile immediately with the Office of the Controller. Project staff will be invited to meet with the Grants Office for Gift Card training and support as needed.

Implementation Date: Immediately

2.3 The CCF Grants Office has sent an email to all CCF faculty, staff, and students reiterating the requirement to complete a Travel Authorization before incurring any travel expenses on behalf of the University and to submit an Expense Report within 10 business days of returning from travel. Additionally, during the newly established Staff Orientation, we provide the FIU Travel Manual as a reference guide and encourage those who will be traveling to set up time to meet with the CCF staff member who processes travel for the Center.

Implementation Date: Immediately

3. Personnel Administration

During our audit period, salaries and fringe benefits totaled $10.4 million. Our review of payroll expenditures focused on the payroll approval process, effort reporting and certification, and on background checks.

Payroll Approval Process

The University's payroll guidelines require managers/proxies to have first-hand knowledge of the employee's work and/or leave hours or obtain written confirmation from the employee's supervisor of the hours being reported prior to approving the payroll.

We reviewed time and attendance records from July 1, 2015 through January 31, 2017, which included 21,856 entries. Our review revealed that:

- An appropriate level supervisor approved 14,978 entries (69%);
- 240 entries (1%) tested were properly approved by a proxy with appropriate support maintained for audit records; however,
- 6,372 entries (29%) were approved by default by the University's Payroll Department without the Center's approval of the work or leave hours reported; and
- 180 entries (1%) tested were approved by a proxy without written confirmation from the supervisor.

Effort Reporting and Certification

University Policy No. 2330.020, *Effort Reporting and Certification*, states: an after-the-fact certification of effort is required of all individuals performing services on a sponsored project when all or a portion of their salary is charged to a sponsored project. Effort reports must be a reasonable estimate of the individual's time and effort during the time period certified. The effort report must be certified by either the individual whose time and effort is being certified or someone having firsthand knowledge of the activities performed by the employee.

We reviewed payroll expenditures for one selected federal grant from April 1, 2015 through March 31, 2016, totaling $344,433, to determine if effort reporting adequately captured salaries and wages charged to the grant. We examined the grant award document and effort reports and noted that all changes in effort percentages by the PI were proper and in compliance with federal regulations and University Policy, and found no exceptions.

Employee Background Checks

The Center is required to comply with Florida Statutes, and with University Policy 1710.257, *Background Check Requirements*, where background screening Level 2 is required for those employees working with minors. Employees are required to obtain a level 2 clearance prior to employment and every five years thereafter.

We obtained the list of 42 temporary employees, full-time employees, and doctorate students who worked with children. We found the following:

- Four of the nine full-time employees had originally obtained a level 2 background screening through Miami-Dade County Public Schools in 2010-2011. However, no evidence was found that the required re-screening every five years was performed.

- One of the 30 temporary employees had their level 2 background screening completed almost six months after being hired for the 2016 Summer Treatment Program. The screening was completed after the program had ended and they were no longer employed.

Recommendations

Center for Children and Families should ensure:	
3.1	That either the managers/proxies have first-hand knowledge of the employee's hours, or they obtain written confirmation from the employee's supervisor of the hours being reported prior to approving the payroll.
3.2	That level 2 background checks for existing employees are completed prior to employment and renewed every five years.

Management Response/Action Plan:

3.1 The CCF community was informed of the expectations in this area in a memo explaining employee requirements and supervisor responsibilities sent to all CCF faculty, staff and students on March 20, 2018.

Implementation Date: Immediately

3.2 CCF relies on FIU HR to manage the clearing responsibility for CCF employees. At recruitment stage, CCF always identifies the Level 2 clearance requirement. However, CCF does not receive information back from FIU HR about clearing dates. The CCF will work with FIU HR to discuss how to best track clearance so that an appropriate plan is put in place that includes contacting employees as well as hiring managers when employees reach their renewal anniversary. In the event that FIU

HR is unable to perform this task, CCF will request clearing dates on a monthly basis and track them in a spreadsheet and arrange for the rescreening.

Implementation Date: December 31, 2018

4. Asset Management

Per the University's Asset Management records, as of March 13, 2017, the Center had 8 capital assets with associated costs totaling $141,926. All of the Center's capital assets were properly accounted for during the audit period without exception.

In addition, the Center is responsible for tracking its attractive/sensitive property, such as laptops, desktops, iPads, and printers that cost less than $5,000, and are particularly vulnerable to theft and misuse, as required by the University Property Manual. The Center had 576 such attractive property items. We selected 111 items for physical observation and determined that controls over attractive property assignment and tracking need improvement. We found:

- Ten iPad minis were loaned out to the families that are participating in a research study in which the family is allowed the distribution of the iPads. We noted the iPads did not have a serial number on the attractive property listing to be able to identify them properly.

- One laptop was checked out by a Center employee to use in the field and was not recorded on the sign-out sheet.

- One iPad's location per the attractive property listing was in a different location than where it was found.

- One instance where the attractive property listing contained a duplicate MAC address, as such, the item was not recorded properly.

- We noted the sign-out sheet used when attractive property items are checked out by the staff was missing some key information such as a serial number, location, date the item was checked out and returned, and the name of the person who received the returned item.

Recommendation

Center for Children and Families should ensure:	
4.1	That all attractive property is accounted for at all times.

Management Response/Action Plan

4.1 The CCF is in the process of updating its IT inventory to ensure that all attractive property is tagged and inventoried.

Implementation Date: June 2018

5. Controls Over Medication Inventory

We reviewed the Center's process to ensure that all medication dispensed was properly accounted for, received, and stored.

The Center orders all medication from the University Pharmacy where pharmacists prepare the drug according to prescriptions. The medication is then stored at the Center for immediate dispensing to the parents and is kept in a secure room while awaiting pickup. The room is secured by a key card entry and an alarm system activates as soon as an individual enters the room. We reviewed the list of individuals with access to the room and access to the alarm system. We noted that 352 employees had access to the room. This list was mostly made up of public safety, facilities/custodial staff, EH&S (Environmental Health & Safety) personnel, and a few Center employees. However, 45 other Center-related employees with access no longer required access. Upon notification, the Center immediately deleted access to the 45 employees. Center Access to the alarm system was limited to 8 Faculty Affiliates and Center employees.

The Center uses a SharePoint system to keep track of the medicine received and dispensed to patients. When the medicine is picked up from the Pharmacy, the information is entered into the system, and is updated when the medicine is dispensed to the patient/parent. When patients come in to pick up the medicine the patient/parent is required to sign their name acknowledging that they have received the medicine. However, the quantity of medication received is not acknowledged by the parent. The quantity dispensed is entered into the system by Center staff. Parents are then required to return the medicine package every month to show that the medicine was used and return any unused medicine. The information is updated in the system and any unused medicine is returned to the Pharmacy for disposal. We reviewed 15 clients' records within SharePoint and ensured that medication ordered from the pharmacy, dispensed to the parents, and returned to the pharmacy reconciled. Although we noted no exceptions, we were unable to determine the accuracy of the medication dispensed or returned by the parents since no independent records exist.

We noted that when the Center orders the medication from the University Pharmacy, it is the Pharmacy that maintains track of the Center's inventory. The Center does not reconcile how much medication has been purchased, received and used in relation to each program. Not reconciling inventory medication can result in inventory discrepancies.

Recommendations

Center for Children and Families should:	
5.1	Routinely evaluate individual access controls to ensure that access to the room where the medicine is stored is programmatically necessary.
5.2	Have patient acknowledge the quantity of medication they are receiving and/or returning.
5.3	Periodically reconcile medication inventory to the University Pharmacy records.

Management Response/Action Plan

5.1 Although the audit report states that more staff from the CCF had access to the medication room than should have had, we would like to clarify that only 8 individuals had access to the alarm codes and the locked cabinets that contained the medications; therefore, only 8 individuals had access to the medications. The majority of the individuals in the report are University custodial/facilities/public safety staff and high-level administrators, and the CCF has no control over which personnel in these specific departments is given swipe access to the door. However, none of these individuals had or have access to the alarm code or locked cabinets containing medications. For those CCF members who inadvertently were given access to the door (again, not the alarm code or the locked cabinets), access was removed immediately upon discussion with the auditors. The CCF has now established procedures for granting access that require that supervisors request access (after clearance is obtained) for only the physical spaces that the individual needs based on their role in the center. For the medication room, no one will be given access unless approved by the Center Director, who is the PI on the only medication grants in the CCF. As an extra precaution, beginning May 2018, we will routinely run an access report of the medical room every 3 months to maintain the approved personnel access only. This will ensure that the room, and more importantly, the controlled substances in it are secure and accessible only to authorized personnel.

Implementation Date: Immediately

5.2 The procedures we use to track medications are those required by state and federal laws to deal with controlled substances in research studies. These procedures were established with and approved by the FIU Pharmacy, the Director/PI of the projects that utilize controlled substances, and the former Radiation/Laser/Controlled Substances and Nanotechnology Safety Officer in the University Office of Environmental Health and Safety. Although we track very carefully the amount of medication given to parents, as well as the amount returned, as required by our

established procedures, we have not required parents to sign a form specifying the number of pills given and returned. We will work with the University Pharmacy to add that information to the existing forms that have been used to obtain parental signatures when medication is dispensed and returned.

Implementation Date: June 2018

5.3 As stated above, our procedures for dealing with medication were established with the University Pharmacy and University Safety Officer and comply with all federal and state laws regarding controlled substances and their dispensing. The official records reside with the Pharmacy. As requested, however, we will develop a procedure with the University Pharmacy to establish records that complement their inventory, and we will compare our record of inventory to the Pharmacy's records annually. Any discrepancy will be addressed directly with the Pharmacy.

Implementation Date: June 2018

SECTION II
Information Technology Controls

6. Information Systems Security

Information Systems Security includes preventive, detective and corrective measures, which are implemented and maintained (especially up-to-date security patches and virus definitions) on endpoint devices that connect to the Center's network and protects them from malware, brute force attacks and unauthorized access.

Malware Prevention

Malware, if undetected in endpoint devices, can disrupt computer operations, or gain unauthorized access to sensitive information. According to FIU Procedure 1930.020c, *IT Security Procedure: System and Application Management*, all FIU owned endpoint devices that connect to FIU's network must have anti-virus software running within 24 hours of their release. The Division of IT has approved the use of the McAfee product suite to prevent the implementation of malware on University controlled endpoint devices.

We selected 11 endpoint devices based on their use of sensitive data. The endpoints are used to enter and retrieve Personal Identifiable Information (PII)[2] and HIPAA[3]-related data[4]. In performing malware prevention software testing, we identified that 3 of the 11 endpoint devices' anti-virus application was installed 874, 92, and 9 days, respectively, after connecting to the network. By not timely installing the approved antivirus application, the devices were at an increased risk of malware while connected to the University's network. The FIU Procedure also states that the Division of IT will control the distribution of anti-virus definition files and operating system updates. To accomplish this, the Division of IT must centrally manage all of the Center's endpoint devices. According to the Division of IT, they managed 10 of the 11 selected endpoint devices.

Unpatched vulnerabilities allow malware to exploit known security weaknesses to gain unauthorized entry onto the network. Using the vendor based security analysis tool, we identified that 4 of 11 endpoint devices tested were missing between 10 and 21 Microsoft Office updates, and 5 to 36 operating system security updates. Endpoint devices that operate on the network without anti-virus protection, and are/or missing security updates reduce the overall effectiveness of the Center's malware prevention controls.

Risk Assessment

Risk Assessments provide critical information to support risk-based decisions that take into account risk factors, such as threat types, frequency, and magnitude of loss. According to the NIST SP 800-53 Rev.4, RA-3*, Risk Assessment*, the Center should conduct a thorough risk assessment and the results shared with key stakeholders whenever there are significant changes that affect the security state of the information systems environment.

[2] Information, such as, name, date of birth, phone number used to identify a specific individual.
[3] Health Insurance Portability and Accountability Act.
[4] Health information that relates to the past, present or future physical or mental health or condition of an individual.

On July 7, 2017, the Office of Research and Economic Development completed a HIPAA Tech Assessment to assist the Center in identifying potential security gaps in their IT environment. The assessment's findings were shared with members from the Division of IT, the Office of Research & Economic Development, and the Center for Children and Family. Subsequently, regularly scheduled meetings between the groups, including the Office of General Counsel, have occurred to determine the best course of action. Additionally, the Office of General Counsel has apprised the University Compliance Office on the assessment's findings. The assessment identified 34 security related action item areas specific to the scope of this audit. The most notable action items included in the File Share server, Research Electronic Data Capture System, and Workstations, were as follows:

- File Share server:
    - Has 22 Terabytes of video containing sensitive and ePHI (electronic protected health information)-related data and resides in a non-HIPAA compliant environment.
    - Does not track when videos are added or removed.
- Research Electronic Data Capture System:
    - Contains programs that have sensitive information including ePHI and resides in a non-compliant HIPAA environment.
    - Sensitive data at rest is not encrypted.
- Workstations:
    - Over 350 members could potentially use computers/mobile devices to store and transmit ePHI.
    - Expect that the IT inventory (workstations) have ePHI.

According to the Center, the File Share server and the Research Electronic Data Capture System are their highest risk systems and they anticipate the implementation of mitigating controls by summer 2018. The assessment identified security gaps that, if not mitigated, can adversely affect the confidentiality, integrity, and availability of the Center's sensitive data.

Media Sanitization

According to the *FIU Property Control Manual*, all media storage devices must be assigned a Media Sanitation Compliance Identification (MSCID) number for proof of sanitation compliance. As part of our examination, we requested the list of the Center's surplus devices from the Division of IT and the Center. The Division of IT provided us with list of six items with an MSCID number, whereas the Center had 343 devices. Although the two lists included the devices' MSCID number, we were unable to reconcile them. The Center's IT Generalist informed us that he scheduled the three devices identified in the Malware Prevention section (see page 23) for surplus. We also noted that 1 of the 11 devices tested was missing from the provided inventory list.

In addition, FIU Policy 1910.005, *Responsibilities for FIU Network and/or System Administrator*, requires departments' IT administrators to send a quarterly report to the Division of IT of any systems implementation or changes to the IT environment. The Center was aware of the policy but unsure on how to report to the Division of IT. Discussed in Report No. 17/18-02, Audit of the University's IT Network Security Controls Follow-up, interviews with IT Administrators showed there was no formal guidance on how they can ensure the governance of policies in their department. Though not provided quarterly, since November 2017, the Center is working with the Chief Information Security Officer on assigning a risk rating to the inventory list. A report that categorizes the risk of each device will increase the effectiveness of the University's cybersecurity and the Center's asset management controls.

Recommendations

Center for Children and Families should:	
6.1	Work with the Division of IT to ensure identified computers do not contain malware, install security updates in a timely manner, and centrally manage all endpoint devices.
6.2	Continue to mitigate the security gaps identified in the HIPAA Risk Assessment.
6.3	Reconcile the surplus list to ensure all items are properly disposed and send a quarterly inventory report to the Division of IT, which includes risk rating for each device.

Management Response/Action Plan:

6.1 UTS (Security IT Officer) has begun to provide weekly and monthly Risk and DLP reports which allows us to monitor updates and pending issues on our equipment so we can maintain such equipment up-to-date. We will be working with the FIU IT Security Administrator to ensure we have all the tools necessary to maintain all equipment up-to-date.

Implementation Date: Immediately

6.2 The CCF team has been working with different departments across FIU: ORED, UTS, GC's office, Compliance, among others, since early 2017 to conduct our own internal risk assessment and find and implement solutions to all identified gaps. Given the number of entities involved, this is a work in progress. Some of the solutions we have begun working towards include transitioning REDCap and several applications to a secure server in Amazon, implement Haivision for video management, and develop procedures that address HIPAA components. Additionally, FIU has engaged a company to conduct a full risk assessment, which will be helpful moving forward.

Implementation Date: December 31, 2018

6.3 The CCF IT Generalist is maintaining a list of all equipment that is surplused. Any equipment that is tagged for surplus is sanitized by the FIU Information Security Office, as coordinated by the CCF IT Generalist before being sent to surplus. Now that we are aware that we have to report on this, the CCF IT Generalist will provide quarterly reports to the Division of IT on all computer activity.

Implementation Date: Immediately

7. Identity Access Management

According to NIST SP 800-53A Rev.4, AC 2, *Account Management,* user identity and logical access controls should ensure that all accounts are established, modified and disabled in a timely manner The Identity Access Management Controls we reviewed included policies, procedures, and the unique identification of user accounts.

Audit Log Controls

FIU Policy No. 1670.015, *Authentication and Audit Controls for ePHI* states that the University will continuously perform monitoring, inspection, testing and auditing of such systems and software access logs in order to ensure the confidentiality, integrity, and availability of ePHI. Additionally, NIST SP 800-53A Rev.4, AC-2(4), *Account Management,* the information system should automatically notify defined personnel about account creation, modification, enabling, disabling, and removal actions in the application and monitor the use of information system accounts. The Research Electronic Data Capture System log file includes information such as gender, name, and e-mail, date of birth, phone number, password, and data export actions by users in clear text format. Access to the log file is discussed in the User Access Controls section below.

Monitoring information disclosure

According to NIST SP 800-53 Rev.4, AU-13[1], *Monitoring for Information Disclosure*, should employ automated monitoring mechanisms for evidence of unauthorized disclosure of sensitive information. According to the Center, when requested, either the Principal Investigator or Application Administrator informally review the Research Electronic Data Capture System log file as a detective control. However, without periodically reviewing the log in a formal manner, the Center increases the risk of inappropriate access, changes, and exfiltration of sensitive information.

In addition to the 11 devices discussed in the Information Systems Security Section (see page 23), we also selected 13 additional devices based on the users' ability to export sensitive data from the Research Electronic Data Capture System. The results provided by the Division of IT showed that 18 of the 24 devices tested did not have DLP (data loss prevention) installed. Without the application, DLP cannot monitor users' actions when transmitting sensitive data in an unauthorized manner.

User Access Controls

According to COBIT 5 DSS06.03.03, *Manage roles, responsibilities, access privileges and levels of authority*, the control's objective is to allow authorized users access only to what is necessary to accomplish assigned tasks in accordance with their business functions and remove access rights immediately if the staff member leaves.

Least Privilege Access

According to the vendor's best practices, the following privileges should only include Principal Investigators, Administrators, and Project Coordinators:

- Access to Logging: This module lists all changes made to the project, including sensitive data changes, and users' passwords.
- Access to export Full Data Set: Allows the user to export sensitive data to another information system including their endpoint device.
- User rights: The ability to change individual user privileges. Any person with this access can alter all privileges for all other users.

Based on the vendor's security recommendations, we noted the following reduction of user access between September 2017 and March 2018:

- Reduced from 553 to 214 active user accounts with unassigned project roles.
- Reduced from 102 to 48 (of 138) active user accounts ability to view log files.
- Reduced from 96 to 76 (of 138) active user accounts ability to export sensitive data.
- Reduced from 106 to 54 (of 138) active user accounts that have administrative privileges to modify user rights.

It is typical on new applications to grant users additional access than necessary as part of the software's initial implementation. In their ongoing effort, the Center continues to review and assign access-based roles thereby reducing the least privilege access risk to sensitive data.

User Off-boarding

User account controls prevent unauthorized changes to the Center's data. Of the 55 deactivated accounts tested in the application, we found 26 users active in the Research Electronic Data Capture System after their reported termination. Though a potential for unauthorized use, we determined that 23 of the 26 accounts tested were a medium risk as there was no activity recorded by the application's log. However, 3 users did access the application after their termination date.

According to the Center, one former FIU employee now works for another university and collaborates with the Center on a temporary basis. The account remained active for over three years after her termination prior to deactivation. Subsequently, the Center reactivated her account twice for a total of 76 days. The account has the ability to export sensitive data from the Research Electronic Data Capture System. However, an examination of the provided log file showed that the user did not download data while reactivated.

The Center also stated that, due to lack of trained IT support, the remaining 2 accounts were unsuspended at the request of management to assist in specific matters. The Center

deactivated the former Research Scientist's account two days after his termination. Approximately six months later, his account was unsuspended for five days in order to provide application code support for the Center. When reactivated, the account had the ability to view the log file, export data and modify user access. An examination of the log showed that the user did not perform any of the high-risk activities while reactivated.

The Center also deactivated the third account 220 days after her termination. According to the provided logs, she accessed the application 4 days after her termination to create a record, which took one day. There was no activity for the balance of the 216 days. Though the user had the ability to view logs and export data, an examination of the log showed that she did not perform any of the high-risk activities after her termination.

On average, the 26 user accounts were active for 183 days after their reported termination. According to the Center, they are aware of the security gap in their off-boarding process and contacted the Division of IT in 2016 about implementing a single sign-on based on FIU's active directory. Presently, the authentication mechanism that affects off-boarding, is a manual process and relies on the Center to update user accounts. The use of an automated off-boarding process will decrease the risk of unauthorized access to sensitive data.

Recommendations

Center for Children and Families should:	
7.1	Formally review the Research Electronic Data Capture System logs periodically to detect any unauthorized access or changes to sensitive information.
7.2	Ensure all devices are running a DLP solution.
7.3	Continue to review and assign roles or disable where appropriate users with access in Research Electronic Data Capture System beyond their business needs.
7.4	Work with the Division of IT on an automated off-boarding process.

Management Response/Action Plan:

7.1 We are working on implementing reports in the CCF Reporting Server using log data and user rights information, which will allow us to easily monitor the users that were granted access to sensitive information and monitor all the downloaded data from REDCap. The Data Services team will periodically send notifications to the PIs to communicate our findings. These reports will allow us to detect any unauthorized access.

Implementation Date: Summer 2018

7.2 DLP has been deployed to the entirety of the CCF organizational unit. Reports are produced weekly and shared with CCF for follow up.

Implementation Date: Immediately

7.3 We have designed REDCap user roles that apply the Principle of Least Privilege (PoLP) that will be used for all the new REDCap projects. We are requesting all users to review and sign user agreements that delineate expectations, and supervisors must request access for their employees based on their role in the project. We will continue to reduce the access to more sensitive user rights for existing projects and to define polices for archiving projects when the data capturing process is over.

Implementation Date: Summer 2018

7.4 We are working with the Division of IT to implement a single sign-on authentication method based on the CCF active directory, which will mean that anyone who leaves the CCF/FIU will automatically lose access to our systems.

Implementation Date: Summer 2018

8. Network Security Controls

Network Security includes defining and protecting internal and external boundaries; limiting access points to the boundaries through the use of firewalls to allow for more comprehensive monitoring of inbound and outbound data traffic; documenting exceptions to the implemented firewall rules; and protecting the information during transit outside of controlled areas. Network diagrams provided by the Division of IT show that the data is adequately segregated using routers and firewalls. In addition, VLANs[5] separate data traffic flow and server logs connect to the Security Information and Event Management (SIEM) system[6]. In addition, access from outside of the internal network requires dual factor authentication over an encrypted virtual private connection.

Monitoring Access Points

According to NIST SP 800-53A Rev.4, SC-7(3), the Center should limit the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic. We asked the Division of IT to run a zero hit count on the two in-scope servers' firewall rules to see which ones were no longer actively in use. The results showed that only 3 of 268 firewall connections have been used in the last 12 months. Inactive firewall connections that are no longer needed provide unnecessary potential entry points for network attacks.

The Center's servers firewall configurations are set to deny all access. However, we noted that both servers allow "Campus Wide" (everyone in the FIU network) access to them. We examined the list of users for the two servers and found that access to each server is adequately limited to the Center's users.

Data Flow Traffic

According to NIST SP 800-53A Rev.4, SC-7(4)(d), *Boundary Protection, External Telecommunications Services*, organizations should document each exception to the traffic flow policy with a supporting mission and/or business need and the duration of that need. Appropriate network access requests should include specific endpoint IPs, ports, duration and business need. We reviewed the requests sent to the Division of IT for the Research Electronic Data Capture System's and the File Share servers and found documentation for 48 of 90, and 26 of 178 rules, respectively. None of the combined 268 rules included the duration and business need. In addition, the Center should periodically review their firewall rules. The lack of periodic formal network traffic reviews increase the risk that network connections are still active and no longer support their mission/business need. Inactive firewall rules provide unnecessary potential entry points for network attacks.

[5] Virtual Local Access Networks partition and isolate computer network traffic.
[6] SIEM provides real-time analysis of security alerts generated by application and network hardware.

Security Awareness Training

According to the FIU Security Website, all FIU faculty and staff are required to participate in security awareness training. The University offers a comprehensive security awareness training to all employees in order to protect the organization and address the multitude of vulnerabilities day-to-day employee activity creates. Inattentive staff or employees not familiar with basic IT security best practices can create opportunities for hackers to compromise the University's network and sensitive data.

Examining a security awareness training completion report for the Center provided by the Division of IT, we found that training was completed by 29 of 35 Center employees. Upon notification, the remaining 6 employees successfully completed the training. Security awareness training ensures that employees know and comprehend the importance of maintaining the confidentiality of sensitive data to secure it appropriately from loss.

Recommendation

Center for Children and Families should:	
8.1	Work with the Division of IT to review firewall rules, disable all inactive connections and include business need and duration for all active rules.

Management Response/Action Plan:

8.1 The Division of IT manages the firewall rules, not the CCF. We will work with the Division of IT to ensure that the CCF equipment is set up with the appropriate rules.

Implementation Date: December 2018

9. Business Continuity Plan

The purpose of Business Continuity is to establish and maintain a plan that enables the business and IT to respond to incidents and disruptions in order to continue operations of critical business processes at a level acceptable to the Center.

BCP Plan and Procedure

According to FIU Policy 180.105, *Emergency Management and Continuity of Operations* (EMCOP), the Continuity Plan's purpose is to effectively mitigate against, prepare for, respond to, and recover from disasters. For our testing, we requested the Department of Emergency Management provide us a copy of the Center's Continuity Plan.

The Center's EMCOP defines critical functions as follows:

- Critical 1: must be continued at normal or increased service load. Cannot pause.
- Critical 2: must be continued if possible, perhaps in reduced mode. Pausing completely will have grave consequences.
- Critical 3: may pause if forced to do so, but must resume in 30 days or sooner.
- Deferrable: may pause; resume when conditions permit.

Listed in the table below, are the self-identified ratings for the in-scope systems tested.

Function	Critical Rating
Clinical Care of Clients	2
Research	3

The Plan adequately addresses key personnel's roles, responsibilities, and assigned individuals by the Center's critical functions. However, the Plan is:

- Not including items critical to the continued operations such as applications, servers, workstations, back up and recovered strategies.
- Missing IT procedures necessary to meet the critical ratings restoration priorities.
- Past due for review. Last review was in January 2016.
- Not formally communicated to key personnel.

Without written procedures for the Center's critical information systems, the Center is unable to ensure that they can meet their operational requirements in the event of a disaster.

BCP Testing

According to NIST SP 800-53A Rev.4, CP-4, *Contingency Plan Testing*, the Center should test the contingency plan to determine the effectiveness of the Plan and the organizational readiness to execute the Plan; review the contingency plan test results; and initiate corrective actions, if needed. The Center's Departmental Administrator informed us that they were not aware that the Center needed to conduct a Continuity Plan

test or table top exercise. It is good practice to test continuity plans on a regular basis to exercise the recovery plans against predetermined outcome. This will allow solutions to be developed and help to verify over time that the Plan will work as anticipated. Without proper testing, management is unable to determine the Plan's viability and its ability to safeguard sensitive information.

Recommendations

Center for Children and Families should:	
9.1	Review and update if necessary the Center's Continuity Plan at least once a year.
9.2	Conduct yearly Continuity Plan testing and document test results and lessons learned.

Management Response/Action Plan:

9.1 The FIU Ready plan (Continuity Plan) will be updated by May 2018, as required by FIU.

Implementation Date: Immediately

9.2 We will work with the different entities involved to facilitate a tabletop exercise at the CCF and document lessons learned for incorporation in future plans.

Implementation Date: December 2018