NEW COLLEGE OF FLORIDA

AGREED UPON PROCEDURES

AS OF JULY 2, 2009

CPA ASSOCIATES
Certified Public Accountants and Consultants

INDEPENDENT ACCOUNTANT'S REPORT
ON APPLYING AGREED-UPON PROCEDURES

Audit Committee
New College of Florida
Sarasota, Florida

This constitutes our report for the June 2009, agreed upon procedures outlined in the engagement letter.

Business Office:	Bonds Payable UBOT and Executive Travel
College Auxiliary Operations:	Cash Receipts
Information Systems:	Disaster Recovery Physical Controls
Registrar Office:	Enrollment Tuition
Research Programs:	State and Local Grants

We have performed certain agreed upon procedures for the benefit and use of New College of Florida. This agreed upon procedures engagement was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. The sufficiency of these procedures is solely the responsibility of those parties specified in this report. Consequently, we make no representation regarding the sufficiency of the procedures described below either for the purpose for which this report has been requested or for any other purpose. The purpose and scope of such operational review procedures performed were set forth in our arrangement letter to you dated May 30, 2008.

We were not engaged to, and did not perform an audit of New College of Florida's financial statements, the objective of which would be the expression of an opinion on the financial statements. Accordingly, we do not express such an opinion on the financial statements of New College of Florida.

Our findings relative to internal control matters were limited to those which came to our attention in connection with performing the aforementioned operational review procedures. We express no opinion regarding the effectiveness of the entity's internal control over financial reporting.

This report is intended solely for your use and the use of New College of Florida's Board of Trustees and management.

We would like to take this opportunity to thank you for the courtesies which were extended to us during the course of the engagement. The cooperation we received from your staff was greatly appreciated.

Should you so desire, we would be happy to discuss these matters with you and assist you in implementing any of the recommendations or suggestions described herein.

CPA Associates

CPA Associates
July 2, 2009

BUSINESS OFFICE: BONDS PAYABLE

A review of bonds payable was conducted to determine:

- New bonds are properly supported by bond agreement and set up according to terms;
- Bond covenants are being monitored and reported to management;
- Bond holders are being paid in accordance with bond agreement;

Procedures Performed

- CPA Associates confirmed there were no new bonds for the review period;
- Reviewed existing bonds for covenants and verified college is monitoring and adhering to the covenant requirements;
- Selected four (4) months of bond account activity and verified activity on bank statements appears reasonable and is properly recorded in the general ledger accounts.

Findings:

No findings were noted during our review.

BUSINESS OFFICE: UBOT AND EXECUTIVE TRAVEL

An understanding of procedures related to travel expenses was obtained and tests were performed to determine:

- Travel expense reports are being properly completed and approved by a supervisor;
- Travel expenses submitted are properly supported by documentation, when applicable;
- Reimbursed expenses do not exceed approved travel limits.

Procedures Performed

Selected fifteen (15) travel expenses during the period of July 1, 2008 through May 31, 2009, from the "Organization Detail Activity" report and verified:

- Travel expense report was properly completed, totaled accurately, and agreed to the transaction activity amount on the Organization Detail Activity Report.
- Expense report was properly approved by a supervisor;
- Expense details were supported by receipts, where applicable, and expenses appeared reasonable based on purpose of travel;
- Travel limits were adhered to and reimbursement to personnel did not exceed those limits.

Findings

06-09-001: During our review of travel expenses, CPA Associates noted that one Travel Expense Report was not signed by a supervisor.

College Response: *We agree. There was some staff changes made during this time period which may have affected the appropriate review and signing of this document. We have changed the processing procedure in both the Executive offices and in the Accounts Payable department to assure that all travel Expense reports will be signed in the future prior to reimbursement.*

COLLEGE AUXILIARY OPERATIONS: CASH RECEIPTS

A review of the College's auxiliary operations was reviewed for the following departments:

- Bike Shoppe
- Campus Space Scheduling
- Fitness Center
- Four Winds Cafe
- Parking Services

We performed a review of the auxiliary cash receipts function and performed certain tests for the purposes of determining:

- Procedures for receipt of money are in place and provide proper segregation of duties;
- Revenue from auxiliary cash receipts is being properly recognized.

Procedures Performed

- Obtained and documented an understanding of the cash receipt process for all auxiliary cash receipts.

Selected twenty (20) auxiliary receipts during the period of July 1, 2008 through May 31, 2009, semesters and determined the following:

- College procedures for receipt of monies are being followed on a consistent basis;
- Proper receipt exists documenting information relating to the receipt of monies;
- A screen print of the student account is completed and the receipt number is written to document posting to Banner, if applicable;
- Receipts collected for the day are properly reported on the "Daily Receipt Report" which documents the total receipts, the bank deposit, and has initials of a preparer and reviewer;
- Total receipts reported on the "Daily Receipt Report" agree to the deposit slip and monies deposited in the bank account;
- Receipt is properly posted to student account in a timely manner, if applicable;
- Bank account reconciliations are prepared and properly reviewed.

Findings

No findings were noted during our review.

INFORMATION SYSTEMS

An understanding of the procedures related to the Information Systems Department was obtained and tests were performed to determine the following:

- Backups of data are completed in a timely manner, retained for a reasonable period and stored off site;
- Security procedures are in place to safeguard data equipment, servers and system data;
- A documented disaster recovery plan for all systems exist and off site disaster recovery centers have been identified;
- Recovery testing is completed with the Central Florida Regional Data Center (CFRDC) and the North Western Regional Data Center (NWRDC) and documented for critical systems to ensure data can be restored from back ups;

Procedures Performed

- Reviewed current policies the College has in place for the IT area's noted above. We also interviewed IT personnel and gained an understanding of the following processes and procedures in place for the items listed below to ensure they appear adequate for the size of the College:

    - Responsibilities of IT employees and IT committee;
    - Hardware/Software currently used and any upcoming changes;
    - Backup of system data;
    - Security over equipment, servers and system data;
    - Disaster recovery plans in place and testing of those plans;
    - Recovery testing of data of the college data;

- Reviewed the disaster recovery plan to verify it contains required information and comprehensive procedures to be followed in the event of a disaster;
- Reviewed connection testing documentation for testing performed on April 15, June 25 and August 23, to ensure the NWRDC and the CFRDC connectivity works.
- Reviewed documentation for critical application testing that was performed on December 27 and February 5 and 10, noting testing was completed successfully;
- Reviewed the warm site disaster recovery test with the NWRDC performed on May 16, noting testing was successful and issues identified during the testing have been resolved.
- Reviewed physical security procedures in place for all critical applications used by the college.

Findings

06-09-002: It was noted the disaster recovery plan has not been formally reviewed and approved by the Technology Advisory Committee or the Audit Committee. This policy should be formally approved and reviewed annually for updates that need to be made.

College Response: *We agree. The plan has been vetted with the Campus Safety Office. Their feedback has been incorporated into the document where appropriate. The document will be acted on by the Technology Advisory Committee at the first meeting of the new term in September or October of 2009.*

06-09-003 The disaster recovery plan lists all the responsible team leaders in the plan for recovery efforts but does not list their contact phone numbers. We recommend this be added to ensure the plan is complete and employees can be contacted in a timely manner after a disaster has happened.

College Response: *We agree. The previous version only had NCF numbers and email addresses. Current personal telephone contact information has been acquired and included as part of the Disaster Recovery Plan.*

<u>IT PRIOR AUDIT FINDINGS UPDATE</u>

During our current review of the IT area, we reviewed all findings for that area that were still outstanding in our May 21, 2008, report that were unresolved from the April 2007 review. Per discussions with the interim CIO the following updates are presented:

- **May 21, 2008, Internal Audit Report**: During our testing, we noted that there was no signed "Data Access and Security Compliance Statement" on file with the IT department for three (3) out of five (5) employees tested. Subsequent to our request, the department had these employees sign the statements. These should be obtained from newly hired employees in a timely manner so that they have an understanding of the College's policies and agree to them.

  During our testing, we noted that there were two (2) out of five (5) employees tested who did not have their passwords locked from Banner in a timely manner. It was determined that this was due to them not appearing on the biweekly report provided to the IT department by the Human Resources department. One employee did not appear on this report for approximately 6 weeks after the termination date. The other employee did not appear on this report for approximately eighteen (18) weeks after their termination date.

- ❖ ***College Response May 21, 2008:*** *We agree. IT has collaborated with Human Resources to make changes to the existing procedure to address both of these findings. Actions taken, effective September 2, 2008, include:*

1. *All new employees, regardless of class or department, will complete a Data Access Compliance form which must have all required signatures and be placed in each employee's permanent file. This is part of the paperwork that each department must execute for all new employees regardless of whether they initially need computer access or not. All existing executed forms have been forwarded from IT to Human Resources to be placed in each existing employee's file.*
2. *The College's "Clearance/Termination Employee Checklist" has been modified to include a requirement that the terminating employee's department take action to "Cancel computer access codes, including e-mail address, network/intranet and Banner." A signed copy of the executed checklist is to be sent to Information Technologies as well as Human Resources. Receipt of this checklist will prompt IT personnel to double check to ensure that the computer access code has been cancelled.*

❖ **Update July 2, 2009:** CPA Associates discussed the above two actions that were to be put into place after our prior audit to ensure they are in place and effectively working. Per discussion with the interim CIO the procedures have been implemented. The IT department maintains a "Data Access Compliance" form for each new employee, which is subsequently placed in their employee file. Human Resources have also implemented a checklist upon termination that is sent to the IT department to ensure accounts are properly locked and access is denied.

- **April 18, 2007, Internal Audit Report:** The College has four (4) policies relating to the IT area: Policy No. 0-500, Using and Protecting Micro-computing Resources; No. 0-501, Appropriate Use of Information Technology Resources; No. 0-504, Information and Communication Security Program; and No. 0-505, Securing Computer Accounts for Terminating Employees. All these policies are dated April 27, 2002, and are USF policies that have not been updated to reflect New College's process and procedures.

❖ ***College Response April 18, 2007****: We agree. These policies are in the process of being re-written to more accurately reflect the NCF environment. A number of new NCF policies have been completed and are currently undergoing legal and executive review. We anticipate they will be in place in September 2007 following authorization by the NCF Board of Trustees.*

❖ **Update May 21, 2008:** Policy No. 0-501 "Appropriate Use of Information Technology Resources" has been updated with Policy No. 4-5006 "Acceptable Use Regulation." Policies numbered 0-500, 0-504, and 0-505 have not yet been updated. After discussion with IT personnel, we reviewed drafts that are currently being updated and will be presented to the Board of Trustees for approval.

❖ ***College Response May 21, 2008:*** *Two new regulations (4-5005 Use and Protection of Information Technology Resources and 4-5007 Information and Communication Security Program.) to replace policies 0-500, 0-504 and 0-505 have been reviewed and published on the NCF website prior to the formal submission to the BOT for approval on September 13, 2008.*

- ❖ **Update July 2, 2009:** Per discussion with the interim CIO the IT Operating Standards and Procedures will address fifteen IT areas. These are detailed procedures for different IT areas and thirteen of the fifteen procedures have been written and approved by the Technology Advisory Committee. They are currently in the process of updating the remaining two for approval.

- **April 18, 2007, Internal Audit Report:** An IT committee is a committee that is important to the organization as the College continues to use computer technology and the data and security risks increase. There is currently no IT committee for the College. It is suggested a committee be formed and meet at least quarterly to review the status of IT items and monitor IT activities.

  - ❖ ***College Response April 18, 2007****: We agree. We will meet with Provost and VP of Finance and Administration in order to address this issue no later than September 2007.*

  - ❖ **Update May 21, 2008:** Per discussion with IT personnel, an IT Committee has not yet formally begun reviewing and monitoring the status of IT items, but the committee has been formed. They are in the process of drafting a charter, which was provided to us for review, which addresses the functions and purpose of the committee.

  - ❖ ***Updated College Response May 21, 2008:*** *We agree. Provost Savin, VP Martin and Interim CIO Harrow collaborated in preparing a draft charter which is now posted on the NCF IT webpage under Policy, Forms and Procedures--Technology Advisory Committee accessible at this link http://www.ncf.edu/it/policies-forms--procedures/technology-advisory-committee. Comments regarding the draft are being solicited from the campus community. Additionally, the tentative dates for the next three (3) committee meetings are also posted on the same web page. The draft charter should be finalized at the meeting scheduled for September 26, 2008.*

  - ❖ **Update July 2, 2009:** A Technology Advisory Committee has been formed and the charter approved. They have had two meetings since our last audit on September 26, 2008 and February 27, 2009. CPA ASSOCIATES reviewed the NCF website noting agenda's for the two meetings.

- **April 18, 2007, Internal Audit Report:** Servers maintained on campus are backed up weekly by the IT Department. The backups are stored in the same room as the servers. These should be stored off campus in case a disaster happens and the College needs to restore data.

  - ❖ ***College Response April 18, 2007****: We agree. We have requested additional budget for the new fiscal year in order to obtain the hardware needed to provide backups stored at a different location and anticipate these new steps being put into operation by the end of December 2007.*

- **Update May 21, 2008:** The backups continue to be stored in the same room as the servers, but the College has secured funding for computer equipment. They are currently in the process of purchasing a hard drive system which will be housed at a remote site for the backup of data.

- **Updated College Response May 21, 2008:** *We agree.* A *new data backup hard drive system has been purchased. The local backup is currently housed in the Palmer A building in the same room as the servers it supports in order to facilitate the backup process (takes approximately twenty (20) hours to complete a single back up of all servers). This room has an intrusion alarm and an emergency power source. A second mirrored data backup hard drive system has been installed on the east side of the campus in Hamilton Center where it is being tested and validated. As soon as the testing is completed it will be re-located to the CFRDC site in Tampa, thus providing a remote site to store back up data. IT staff will meet with CFRDC staff on September 9, 2008, to establish a target date to relocate the second mirrored data backup hard drive system from Hamilton Center to the CFRDC site.*

- **Update July 2, 2009:** The data backup hard drive system described in the above college response has been placed at the CFRDC in Tampa and back ups are done daily to this server.

- **April 18, 2007, Internal Audit Report:** The College has two (2) vendors that can access specific servers as long as the servers are on. These vendors are College Boards for Admissions (Recruitment Plus) and Lloyd Air Conditioner. Recruitment Plus is a critical system and contains a large amount of applicant personal data. There is no review of the log-ins for either of these vendors. We recommend the College implement a process to review the log-ins for unauthorized access or unusual activity.

  - ***College Response April 18, 2007****: We agree. We will work with Admissions, Physical Plant, and the vendors in order to develop and implement the appropriate procedures needed to review/monitor these logins by September 2007.*

  - **Update May 21, 2008:** Per IT personnel, access to Recruitment Plus is monitored by the Admissions Department and they assume that if they are not contacted by Admissions then there was no unauthorized access. There is no formal process that documents that this is being done and the findings and resolutions that follow. There is also no monitoring of the access from Lloyd Air Conditioner. Per IT personnel, the server they access is dedicated to HVAC controls with no connection to the rest of the College network; therefore, the server is not monitored for unauthorized access.

  - ***Updated College Response May 21, 2008:*** *We agree that the current procedure needs refinement. Effective September 5, 2008, the procedure was changed as follows: The Recruitment Plus vendor can only access the software when IT grants them access. IT now requires designated Admissions' staff to submit a help desk ticket requesting temporary access. The ticket must include the start and end date of this access. IT has also modified the way Boyd's A/C logins to the HVAC controls*

server. Designated Physical Plant staff must submit a help desk ticket requesting server access for Boyd's A/C for a specific start and end date of the access. This procedure is now documented in draft form on IT Operating Standards and Procedures web pages at http://www.ncf.edu/it/policies-forms--procedures/it-security-regulations/it-access-by-non_employees

- **Update July 2, 2009:** Per the CIO**, t**hese procedures are in place and working effectively. The IT Operating Standards and Procedures on the website detail these procedures and identify the two vendors that have access to the NCF servers. There are specific procedures for each vendor on how access is gained and monitored.

- **April 18, 2007, Internal Audit Report:** While a disaster recovery site is identified for the Banner system at the Central Florida Regional Data Center (CFRDC), the College does not have well defined, written disaster recovery procedures. The College should finalize development of contingency plans so that all personnel will be aware of their responsibilities in the event of an emergency that precludes the continuation of existing EDP operations. We suggest this plan include, but not be limited to, the following: location of, and access to, off-site storage; a listing of all data files that would have to be obtained from the off-site storage location; identification of a back-up location with similar or compatible equipment for emergency processing; responsibilities of various personnel in an emergency; and priority of critical applications and reporting requirements during the emergency period.

  - ***College Response April 18, 2007****: We agree. While administrative data recovery and disaster contingency are provided for in our contract with the CFRDC, we have not developed detailed written plans for carrying out or testing those procedures. We will work with the CFRDC over the next several months to rectify that and develop comprehensive written procedures by December 2007. We will also review a number of disaster recovery options for onsite campus operations and critical data for implementation in the same timeframe.*

  - **Update May 21, 2008:** There have been no further actions taken on this finding.

  - ***Updated College Response May 21, 2008:*** *We agree that we have not been able to complete these tasks to date. IT has scheduled a meeting with the CFRDC staff in Tampa on September 9, 2008, to obtain their assistance in developing a written protocol for disaster recovery and testing. Now that the College has acquired a backup system to support campus based servers, a disaster recovery plan will be prepared for this system as well. IT expects to have the written procedures completed and in place by the October 31, 2008.*

  - **Update July 2, 2009:** A detailed disaster recovery plan has been implemented and has been reviewed by CPAA in the audit procedures noted above. The college has also conducted various recovery tests with the CFRDC and the NWRDC which have also been reviewed during our audit testing above.

- **April 18, 2007, Internal Audit Report:** Data recovery testing is not being performed to ensure server data information backed up by the college's IT Department can be restored from back up tapes. This should be performed at least annually for critical systems of the college to ensure data can be restored in the event of a disaster.

  - ***College Response May 18, 2007****: We agree in part. The data backup at the CFRDC is restored into two test databases periodically and we have accessed both of these databases to confirm that saved and restored data is accurate and available when needed. We have not performed this type of testing for data backed up on campus from shared drives or servers used for additional administrative systems. In order to provide these functions for on campus operations, we need to have additional hardware such as servers and drivers for which we have made new budget requests. With the additional budget for new hardware, we should be able to have improved campus back up and recovery processes in place by the end of this calendar year.*

  - **Update May 21, 2008:** Data recovery testing of Banner is being performed several times a year by the IT Department to ensure server data information is backed up and can be restored from back up tapes. Currently, this process is not being documented to provide evidence of test.

  - ***Updated College Response May 21, 2008:*** *We agree. Effective September 1, 2008, IT will require that all requests for restoration of the production database into test instances be documented on help desk tickets. The procedure also requires that conversion of the production database into test instances be accomplished at least once a year.*

  - **Update July 2, 2009:** During our audit procedures noted above we noted all recovery testing is now documented and supported by verification of the testing completed. This testing documentation also documents the initials of the person responsible for the testing area denoting the test was successfully performed.

- **April 18, 2007, Internal Audit Report:** Per Florida Statues section 282-318-1984, the "Security of Data and Information Technology Resources Act" requires each IT Department head to be responsible for assuring an adequate level of security for all data information technology resources. The State University System has issued a Standard Practice entitled "Security" requiring each College to establish an Information Security Manager. This person is to perform an IT risk analysis and certify compliance annually. The College has not yet complied with this requirement.

  - ***College Response May 18, 2007****: We agree. NCF's CIO has appointed Jeff Smith as our Information Security Manager. Ramon Padilla of the SUS IRM organization was informed of this appointment in April 2007, and Jeff Smith has attended his first meeting of the state group. Jeff is committed to working with the IRM and performing all the steps needed to ensure compliance.*

- ❖ **Update May 21, 2008:** While the College has now designated an Information Security Manager, there has not been any testing or analysis completed or submitted to the Board of Trustees.

- ❖ ***Updated College Response May 21, 2008:*** *We agree. IT has reviewed several risk self assessment instruments and will have completed the first annual self assessment by late September 2008. Self assessment findings will be reviewed at the next Technology Advisory Committee meeting, tentatively scheduled for September 26, 2008. Assessment findings will also be reported annually to the Board of Trustees' Audit Committee.*

- ❖ **Update July 2, 2009:** IT has incorporated a risk assessment in the disaster recovery plan noting physical, internal and external security risks, as well as environmental risks to the system. There is also a section for preventative measures that are either in place or can be implemented to mitigate the risks.

- **April 18, 2007, Internal Audit Report:** Several attempts were made to obtain a Statement of Auditing Standards (SAS) 70 audit report of the CFRDC data center. A SAS 70 report is generated as a result of a critical review of processes that should be requested of the data center. This should be provided to the College so they can perform their due diligence of the CFRDC's system of internal controls and ensure data is safeguarded, disaster recovery plans are in place and weaknesses in control systems are addressed in a timely manner. After discussions with College personnel, USF Internal Audit Department, the Auditor General, and the Director of the CFRDC, it was concluded that no formal review of the data center has been performed. Due to the unavailability of a SAS 70 report and because the evaluation of a third party service provider's internal controls is outside the scope of services we are providing the College, we have no basis on which to comment on the procedures and controls CFRDC has in place over the College's Banner data system.

  - ❖ ***College Response April 18, 2007****: We agree. During attempts by our external auditor to gather this information from the CFRDC, this situation was communicated as a possible gap in the CFRDC's audit standards. We believe that the state auditors and CFRDC management will take steps in the next few months to address this. We will also follow up with CFRDC management to determine what progress has been made by September 2007.*

  - ❖ **Update May 21, 2008:** To date, there has been no known formal review of the CFRDC, but there has been an operation audit conducted by the Auditor General of the NWRDC. There were two (2) findings which are documented in Auditor General Report No 2007-129, finding Nos. 4 and 5.

  - ❖ ***Updated College Response May 21, 2008:*** *We agree. Although CFRDC has determined that it is not subject to SAS 70 audits, the College will consult with USF and CFRDC management to confirm the data center's system of internal controls and to ensure data are safeguarded, disaster recovery plans are in place and weaknesses*

in control systems are addressed in a timely manner. We will strive to receive written confirmation from USF regarding this matter.

- **Update July 2, 2009:** Management had requested audits reports for audits that were conducted at the CFRDC but was informed that these are confidential and only available to the Auditor General for their review. This confidentiality is per Florida Statutes in order to maintain the integrity and security of the information systems. Management did confirm that audits are done within regulations and the Auditor General has recently reviewed the IT area.

Based on the above review of prior year findings it appears all items have been addressed and cleared. Policies and procedures have been implemented and continue to work effectively. A few areas are still in the process of being finalized but are in process and almost completed.

REGISTRAR OFFICE: ENROLLMENT

A review of the policies and procedures related to student enrollment was performed to determine the following:

- Admittance of students is done within College guidelines;
- Proper documentation is being maintained in student files;
- Admission fees are being accurately charged and properly posted to student accounts;
- Applicant information is properly entered into the Recruitment Plus database;
- Policies for denied students are being followed.

Procedures Performed

Selected ten (10) students who applied for the Fall 2008 and Spring 2009, semesters and performed the following procedures:

- Inquired of management and staff regarding processes for admission of students;
- Reviewed student files to ensure proper documentation is being maintained;
- Determined that admission fee was correctly charged to student accounts in Banner and received prior to evaluation;
- Compared student name and application status from the applicant listing to information listed in the Recruitment Plus database;
- Ensured that all application requirements were checked as complete in the Recruitment Plus database.
- Verified that the application decision listed in the Recruitment Plus database agreed with the decision in the applicant listing that was mailed to the applicant.

Findings

No findings were noted during our review.

REGISTRAR OFFICE: TUITION

An understanding of the registration process related to student tuition was obtained and testing was done to determine:

- Tuition fees are being accurately posted to student accounts;
- Receipt of tuition fees are being accurately posted to student accounts and general ledger.

Procedures Performed

Selected ten (10) students registered for classes during the Fall 2008 and Spring 2009, semesters and performed the following procedures:

- Obtained student files for the semester being tested;
- Reviewed student file for signed contract stating registered courses for the applicable semester;
- Verified registered courses per the signed contract agree to registered courses per Banner;
- Determined proper documentation exists supporting receipt of tuition fees;
- Tuition receipts collected for the day are properly reported on the "Daily Receipt Report" which documents the total receipts, the bank deposit, and has initials of a preparer and reviewer;
- Total receipts reported on the "Daily Receipt Report" agree to the deposit slip and monies deposited in the bank account;
- Receipt is properly posted to student account in a timely manner, if applicable;
- Bank account reconciliations are prepared and properly reviewed.

Findings

No findings were noted during our review.

RESEARCH PROGRAMS: GRANT REVIEW

An understanding of procedures related to state and local grants was obtained and testing was done to determine:

- Grant applications and contracts have proper authorization from college management;
- Approval was obtained and dates on record are accurate;
- Expenses being paid are within grant covenants;
- Expenses paid are not over budgeted amounts.

Procedures Performed

- Reviewed contracts to ensure procedures for application are being followed;
- Reviewed contracts to determine proper approval was received and funding amounts established;

- Selected ten (10) disbursements made during the period July 1, 2008 through May 31, 2009, and verified proper documentation for grant expense, where applicable;
- Verified above disbursements were proper expenses within the grant covenants.

Findings

No findings were noted during our review.

We would like to take this opportunity to thank you for the courtesies which were extended to us during the course of the engagement. The cooperation received from your staff was greatly appreciated.