Board of Directors Meeting

February 14, 2008

Approve Annual Financial Report **Item IV.A.**

Recommended Action:	Accept the 2007 Annual Financial Report and the accompanying Management Letter.
Issue:	FY 0607 Completed Financial Audit Report
Program:	None
Budget Impact:	None
Strategic Plan Goal:	None

Background: Attached is a copy of the FY 2006-07 Annual Financial Report which includes the Audit Report and Management Letter. The Board is asked to review and accept this report.

ıe report focuses on both the JWB as a whole (government-wide) and the major individual funds in order to allow the user to address relevant questions, widen comparisons, and enhance accountability. The sections are as follows: *MD&A* (Management Discussion and Analysis); *Basic Financial Statements* (Government-wide and Fund specific) along with the Notes to the Financial Statements; and *Other required supplementary information.*

The firm of Cherry, Bekaert and Holland, LLP completed the audit. The Annual Financial Report has been prepared consistent with applicable state statutes and the reporting standards of the Government Accounting Standards. This certifies the accuracy and integrity of the fiscal policies and procedures of the Juvenile Welfare Board during FY 0607.

Cherry, Bekaert and Holland have no Management Letter recommendations to report.

CHERRY BEKAERT & HOLLAND
CERTIFIED PUBLIC ACCOUNTANTS & CONSULTANTS

Cherry, Bekaert & Holland, L.L.P.
The Firm of Choice.

www.cbh.com

601 South Harbour Island Boulevard
Suite 200
Tampa, Florida 33602
phone 813.251.1010
fax 813.251.9235

February 6, 2008

Dear Members of the Board of the
Juvenile Welfare Board of Pinellas County:

In planning and performing our audit of the financial statements of the governmental activities, the business-type activities, each major fund, and the aggregate remaining fund information of the Juvenile Welfare Board of Pinellas County, Florida ("JWB"), as of and for the year ended September 30, 2007, which collectively comprise JWB's basic financial statements, we considered its internal control in order to determine our auditing procedures for the purpose of expressing our opinions on the basic financial statements and not to provide assurance on internal control.

During our audit we became aware of matters that present opportunities for strengthening internal control and other matters. We will review the status of these comments during our next audit engagement.

CURRENT YEAR'S OBSERVATIONS AND RECOMMENDATIONS

Purchasing Cards

Observation: We noted that audit documentation for approving temporary increases in individual purchasing card limit could be strengthened and there were a significant number of employees that used a purchasing card.

Recommendation: We recommend that appropriate audit documentation be maintained to indicate approval of increases in individual purchasing card limits. We also recommend that JWB evaluate the number of employees that use purchasing cards to determine if purchasing card use may be excessive.

Management's Response: Management concurs with this recommendation. An audit trail was immediately instituted at the time of this finding. An evaluation of the number of employees and purchasing card usage was presented to the Finance Committee on January 31st. It was determined that JWB will reduce the degree of risk by reducing the number of staff holding purchasing cards. They will be reviewed and distributed only to essential staff under day to day management and control of Senior Managers.

Board Minutes

Observation: We noted that the board minutes are not officially signed by the secretary indicating final approval of the minutes by the board of directors.

Recommendation: We recommend that board minutes by signed by the secretary upon approval of the minutes by the board of directors.

Management's Response: Management concurs with this recommendation. Beginning October, 2007, JWB Board Meeting minutes will be signed by the Board Secretary.

Information Technology

Training

Observation: We noted that security awareness training provided to employees was limited.

Recommendation: We recommend that JWB consider providing IT security awareness training to employees when initially hired and conduct training once a year thereafter. Training can reduce the risk that information security may be compromised. Training materials for desktop and laptop users typically contains acceptable use policy and information relating to desktop security, log-on requirements and password administration guidelines. Training should also address social engineering and the policies and procedures that protect against social engineering attacks. We also recommend that employees sign-off on IT security policies on an annual basis. A similar recommendation was made in the year ended September 30, 2006.

Management's Response: Management concurs with this recommendation. As part of the orientation process since 2001, security training is provided to all new staff. Security training is provided to all new staff as part of the orientation process. Ongoing training was conducted in January 2008 which included issues such as desktop security, log-on requirements, password administration guidelines, social engineering, etc. Staff signed in, received an attendance certificate following the session, and a copy was sent to HR. All staff was required to attend the security training; an additional session was held for managers to reinforce the need for support for policy enforcement. IT security awareness training will be conducted once a year and IT security policies will have employee sign-off on an annual basis.

Access

Observation: It appears that information system owners do not periodically review access authorization and rights. This may increase the risk of fraud, misuse, and excessive privileges.

Recommendation: We recommend that JWB perform a review of access authorization and rights at least annually. Information system owners should also sign-off on each user to certify that each user's level of access is current and accurately reflects the appropriate level of segregation of duties. A similar recommendation was made in the year ended September 30, 2006.

Management's Response: Management concurs with this recommendation. Access rights for systems are reviewed annually by the owners of some systems. Users of all the JWB network resources are reviewed each time a staff change occurs; Contract Managers are tasked to review access rights of SAMIS users during the annual site visit process; Great Plains access rights are controlled by Finance and access to that resource is dependent upon a user being set up in Active Directories. The Active Directories accounts of staff that terminate employment from JWB are locked following notification from the department director. Vendor and temporary staff accounts are set up with limited access rights including hours of the day. Vendor accounts are closed until access is requested. IT will implement an annual sign-off on each user certifying that each user's level of access is current and accurately reflects the appropriate level of segregation of duties

Computer Terminal Security

Observation: Computer terminals are not automatically locked or logged off after a period of inactivity. This situation allows the opportunity for the computer to be used in an unauthorized manner.

Recommendation: We recommend that computer terminals be locked, logged off, or password protected by a screensaver after a period of inactivity of ten to fifteen minutes. A similar recommendation was made in the year ended September 30, 2006.

Management's Response: Management concurs with this recommendation. The Finance department implemented a logoff after five minutes of inactivity in January 2007. The fifteen minute threshold agency wide logoff was implemented on January 25, 2008.

Password Controls

Observation: Currently password controls for the financial application are weak. This reduces the accountability of the password in authenticating an individual user logging on to a user account by increasing the risk that the password could be guessed.

Recommendation: We commend that best practices be followed for passwords which require passwords have a minimum length of 6 to 8 characters and expire at least every 90 days. A history of 24 previous passwords should be maintained to prevent the same password from being used in the same year. User accounts should be locked after 3 to 5 unsuccessful log-on attempts. A screensaver password should protect all desktops after a period of inactivity of 10-15 minutes.

Management's Response: Management concurs with this recommendation. The Great Plains security is controlled by Password which is linked to a specific fiscal activity level. In order for the Great Plains security to allow for a password to change every 90 days, the database will need to be updated to SQL 2005 in order to work with the network active directory. This will allow Great Plains to coincide with the JWB network User ID/Password security policy. Staff met on January 30th and the IT Director is currently moving forward with this project.

The above items have been discussed with the appropriate individuals. We would be glad to further discuss this letter with you at your convenience.

Very truly yours,

CHERRY, BEKAERT & HOLLAND, L.L.P.

Troy Y. Manning
Partner

TYM/ker