Deloitte & Touche LLP
361 South Marine Corps Drive
Tamuning, GU 96913-3911
USA
Tel: (671)646-3884
Fax: (671)649-4932
www.deloitte.com

March 31, 2009

Consolidated Commission on Utilities (CCU)

Dear Members of the Commission:

In planning and performing our audit of the financial statements of Guam Power Authority (the "Authority" or "GPA") as of and for the year ended September 30, 2008 (on which we have issued our report dated March 31, 2009), in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, we considered the Authority's internal control over financial reporting as a basis for designing audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Authority's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the Authority's internal control over financial reporting.

Our consideration of internal control over financial reporting was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control over financial reporting. However, in connection with our audit, we identified, and included in the attached Appendix I, deficiencies related to the Authority's internal control over financial reporting and other matters as of September 30, 2008 that we wish to bring to your attention.

We have also issued a separate report to the Commission and management, also dated March 31, 2009, which includes certain matters involving the Authority's internal control over financial reporting that we consider to be a material weakness *or* significant deficiencies under standards established by the American Institute of Certified Public Accountants.

The definition of a deficiency is also set forth in the attached Appendix I.

A description of the responsibility of management for establishing and maintaining internal control over financial reporting and of the objectives of and inherent limitations of internal control over financial reporting, is set forth in the attached Appendix II and should be read in conjunction with this report.

This report is intended solely for the information and use of the Consolidated Commission on Utilities, management, others within the organization, the Office of the Public Auditor of Guam and the Federal cognizant agency and is not intended to be and should not be used by anyone other than these specified parties.

We will be pleased to discuss the attached comments with you and, if desired, to assist you in implementing any of the suggestions.

We wish to thank the staff and management of the Authority for their cooperation and assistance during the course of this engagement.

Very truly yours,

Deloitte & Touche LLP

APPENDIX I

SECTION I –DEFICIENCIES

We identified, and have included below, deficiencies involving the Authority's internal control over financial reporting as of September 30, 2008 that we wish to bring to your attention:

1. Segregation of the Information Technology (IT) Production and Testing Environments

   Condition: IT testing and production environments should be separated. Seven profiles that are created for testing purposes are classified to the Attribute of *PROD in the List of Library. Employees under these profiles, who are responsible for testing data, could intentionally or accidentally change the data in the production environment. The data integrity of the production environment could be affected.

   Recommendation: The Authority should review the incompatible settings and delete those libraries, if no longer needed. If they are still needed, the attribute should be changed from *PROD to *TEST.

2. Access to the IT Production Environment

   Condition: Access to data and the ability to make changes to the production environment should not be granted to the same individual. The Authority's programmers are granted access to production data. The system programmers, including GWA and AMX users, are also responsible for developing changes to the interface and migration of these modifications to the production environment. As such, segregation of duties may be compromised. Inappropriate segregation of duties could reduce the likelihood of detecting unauthorized transactions or errors; programmers could perform changes in production without responsibility and accountability being established and therefore data integrity could be threatened; and version control over scripts/files could be compromised. Access to the production environment should be limited to users and administrators who need it in order to perform their daily tasks.

   Recommendation: Formal segregation of duties should be defined and applied in respect to the process of making changes and moving updated versions to production. In addition, activity logs should be reviewed on a periodic basis. The Authority has noted that currently this segregation of duties cannot be achieved, since a single Computer System Analyst needs access to production data in order to fulfill his job requirements. However, we reiterate the importance of segregation of duties within the IT environment and recommend the Authority consider other methods to mitigate potential risks.

3. Segregation of Duties in System Maintenance

   Condition: Programmers are allowed to modify code and migrate the codes in the production environment and as such, programmers can manipulate production data. The Authority noted that this is necessary because programmers need access in cases when another programmer is not available. Currently, GPA Computer Services only has one position designated to allow, modify code and migrate code from one environment to another on the IBM platform, which is the Computer Systems Analyst II. To maintain segregation of duties, end users do not have access nor do they have authorization to perform such function(s). As such, it appears the control at the end-user level is sufficient. However, a segregation of duties issue still exists at the Computer System Analyst II level.

SECTION I – DEFICIENCIES, CONTINUED

3. Segregation of Duties in System Maintenance, Continued

Recommendation: Although we are mindful of restrictions that the Authority is facing due to limited IT resources, the Authority should strengthen its detective controls to mitigate risk exposure when personnel have the ability to perform incompatible duties. For example, an individual, other than the programmers, (e.g. CIS consultant, the Acting Manager of Computer Systems, the Chief Financial Officer or Computer Operations Supervisor) may be assigned to review code modification logs and activities logs monthly. This could assist in detecting manipulation of system codes and application systems.

SECTION II – OTHER MATTERS

Our observations concerning other matters related to operations, compliance with laws and regulations, and best practices involving internal control over financial reporting that we wish to bring to your attention are as follows:

1. Review of Payroll Deductions

Condition: Six employees hired after March 31, 1986, have been erroneously exempted from Medicare deductions.

Recommendation: The Authority should independently review, on a quarterly basis, required employee deductions.

2. Allowance for Funds Used During Construction (AFUDC)

Condition: The Authority's interest capitalization policy is not in accordance with generally accepted accounting principles. The policy has not been approved by the Public Utilities Commission (PUC). In addition, the Authority does not have a policy for cessation of interest capitalization for construction in progress projects that are on hold.

Prior Year Status: This condition is reiterative of conditions identified in our prior year audit of GPA.

Recommendation: The Authority should submit its interest capitalization policy to the PUC for approval. GPA should consider ceasing interest capitalization on projects that are not actively undergoing activities to prepare them for use.

3. Monitoring of Fixed Assets and Maintenance of Fixed Asset Register

Condition: Of fourteen assets tested, we noted the following:

- Model Hardware 9335 (asset no. 2727351) with Computer Service has been salvaged but not yet removed from the fixed asset register,

- Kronos 55 and accessories (asset no. 2728062) are still being depreciated although they are no longer in use, having been replaced by the JDE Payroll Module.

Recommendation: The Authority should regularly update of the fixed asset subsidiary ledgers and should perform periodic inventories to verify the status and existence of assets.

SECTION II – OTHER MATTERS, CONTINUED

4. Inventory Obsolescence Policy

Condition: The Authority does not produce inventory aging reports to assist in the identification of obsolete inventory and the establishment of inventory obsolescence reserves. Furthermore, there is no established policy governing a periodic assessment of inventory valuation to ensure that inventories are carried at the lower of cost or market.

Prior Year Status: This condition is reiterative of conditions identified in our prior year audit of GPA.

Recommendation: Regular preparation and review of an inventory aging report should identify potential inventory valuation issues and serve as an independent check that slow-moving items are evaluated for obsolescence.

5. Retirement of Fixed Assets

Condition: Pre-numbered documents are not sent to accounting to record fixed assets retired by departments.

Prior Year Status: This condition is reiterative of conditions identified in our prior year audit of GPA.

Recommendation: The Authority should adopt a pre-numbered document to be completed by end-users for all retired fixed assets.

6. Synchronization of Work Order Status

Condition: The work order status between the J.D. Edwards ("JDE") and the Utiligy systems is not synchronized.

Prior Year Status: This condition is reiterative of conditions identified in our prior year audit of GPA.

Recommendation: The Authority should implement a process to regularly update the work order status between Utiligy and JDE. This would avoid an accumulation of work orders to be corrected and improve completeness of billings.

7. Prepayments and Payroll Clearing Accounts

Condition: The Authority's prepaid parts account is not reconciled against outstanding bank letters of credit. Furthermore, a "deferred clearing" account is not regularly reviewed to clear transactions from the account.

Recommendation: A regular review of prepaid parts and deferred clearing accounts should occur to clear transactions and to minimize error accumulations.

SECTION II – OTHER MATTERS, CONTINUED

8. Bid Deposits

Condition: Bid deposit accounts are not regularly reviewed to reflect actual refundable balances.

Recommendation: The bid deposit account should be regularly reviewed and deposits for closed bid transactions should be adjusted to recognize income in the correct accounting period.

9. Accounts for Disconnection

Condition: Billings for accounts that are due for disconnection are not subjected to meter exception report reviews.

Recommendation: All billings should be reviewed for obvious errors before they are sent to customers.

10. Monitoring of Temporary Streetlights

Condition: Accounts receivable includes receivables for work orders for temporary streetlights that have not been closed out.

Recommendation: The customer service and accounting departments should regularly coordinate as to the status of work orders pertaining to these accounts.

11. Defective Fuel Auto Gauges

Condition: Auto gauges are devices used to record consumption and issuance of fuel. In four of ten fuel inventory observation locations, the auto gauges were defective.

Prior Year Status: This condition is reiterative of conditions identified in our prior year audit of GPA.

Recommendation: Auto gauges should be maintained so that movements of fuel are monitored to minimize losses.

12. Reconciliation of Accounts with Guam Waterworks Authority (GWA)

Condition: GWA is disputing charges from GPA for certain joint use costs.

Recommendation: Since GPA and GWA have the same governing body, disputed charges should be referred to the CCU for resolution.

13. OS 400 Computer System Value Setting Best Practices

Condition: Currently, four of the Authority's security settings in its OS 400 environment differ from those settings that are considered best practices. However, management has concluded that three of the four settings are necessary for proper system functionality.

Recommendation: The Authority should consider changing the remaining setting to the more stringent method which is a best practice.

SECTION II – OTHER MATTERS, CONTINUED

14. Computer System User Profiles

Condition: Computer user profiles (IDs) for terminated employees should be promptly deleted. System users having more than one user ID should be for specific business purposes and approval be properly documented. The AS/400 user profiles listing dated December 1, 2008 contained seven terminated employees, based on human resource records.

Recommendation: The Authority should verify the status of these employees and immediately remove them if they are indeed terminated employees. Additionally, procedures should be established to review a list of existing user profiles on a regular basis together with the HR department to detect invalid users.

15. Assignment of Users to the Appropriate Class

Condition: Computer system users should be granted access to appropriate user classes. Some users were granted access to incorrect user classes and were assigned inappropriate special authorities.

Recommendation: The Authority should review incorrect settings and make necessary corrections.

16 Termination Procedures

Condition: Per GPA operating standard procedure, SP108, Section V, the payroll division is to notify computer services of any employee termination for system access removal. However, based on the Computer Operation Supervisor, verbal notification or an email from any of the following parties is sufficient to delete a user account: 1) Acting Manager of Computer Service, 2) HR department or 3) Division supervisors.

Recommendation: The Authority should follow existing policies and procedures.

17. Inappropriate Access to Sensitive System Commands

Condition: Use of sensitive commands should be restricted. We noted that the "public authority" to several sensitive system commands is set to *USE, which should be set to *EXCLUDE. These system commands were properly set to *EXCLUDE previously, but they appeared to have been reset during a recent upgrade.

Recommendation: The "public authority" should be set as *EXCLUDE. For cases where further access is required, management should assess the appropriateness of the assignment.

18. Internal Reporting

Condition: Claims and collections reported by Engineering on a quarterly basis, as part of reporting requirements of certain projects, does not reconcile with the amounts reported by Accounting.

Recommendation: A quarterly reconciliation of the claims and collection balances between Engineering and Accounting would assist in monitoring of differences.

SECTION II – OTHER MATTERS, CONTINUED

19. Wire Transfer

Conditions: A wire transfer of $1.5 million took seven business days to be credited by the receiving bank.

Recommendation: GPA should request an explanation for the delay in receiving credit for the $1.5 million bank transfer.

SECTION III – DEFINITIONS

The definition of a deficiency that is established in AU 325, *Communicating Internal Control Related Matters Identified in an Audit*, is as follows:

A *deficiency* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A deficiency in design exists when (a) a control necessary to meet the control objective is missing or (b) an existing control is not properly designed so that, even if the control operates as designed, the control objective would not be met. A deficiency in operation exists when (a) a properly designed control does not operate as designed, or (b) the person performing the control does not possess the necessary authority or competence to perform the control effectively.

MANAGEMENT'S RESPONSIBILITY FOR, AND THE OBJECTIVES AND LIMITATIONS OF, INTERNAL CONTROL OVER FINANCIAL REPORTING

The following comments concerning management's responsibility for internal control over financial reporting and the objectives and inherent limitations of internal control over financial reporting are adapted from auditing standards generally accepted in the United States of America.

Management's Responsibility

The Authority's management is responsible for the overall accuracy of the financial statements and their conformity with generally accepted accounting principles. In this regard, management is also responsible for establishing and maintaining effective internal control over financial reporting.

Objectives of Internal Control over Financial Reporting

Internal control over financial reporting is a process affected by those charged with governance, management, and other personnel and designed to provide reasonable assurance about the achievement of the entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations. Internal control over the safeguarding of assets against unauthorized acquisition, use, or disposition may include controls related to financial reporting and operations objectives. Generally, controls that are relevant to an audit of financial statements are those that pertain to the entity's objective of reliable financial reporting (i.e., the preparation of reliable financial statements that are fairly presented in conformity with generally accepted accounting principles).

Inherent Limitations of Internal Control over Financial Reporting

Because of the inherent limitations of internal control over financial reporting, including the possibility of collusion or improper management override of controls, material misstatements due to error or fraud may not be prevented or detected on a timely basis. Also, projections of any evaluation of the effectiveness of the internal control over financial reporting to future periods are subject to the risk that the controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.