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

February 27, 2010

Mr. Joaquin C. Flores
General Manager
Guam Power Authority
1911 Route 16
Harmon, Guam 96913

Dear Mr. Flores:

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, 2009 (on which we have issued our report dated February 27, 2010), 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, 2009 that we wish to bring to your attention.

We have also issued a separate report to the Consolidated Commission on Utilities, also dated February 27, 2010, 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 Public Accountability - 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

SECTION I –DEFICIENCIES

We identified, and have included below, deficiencies involving the Authority's internal control over financial reporting as of September 30, 2009 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. Fourteen profiles created for test purposes are classified to the Attribute of *PROD in the List of Library. Employees under these profiles, who are responsible for test data, could intentionally or accidentally change the data in the production environment. The data integrity of the production environment could be negatively impacted.

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

   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. Segregation of Duties in System Maintenance

   Condition: Programmers are allowed to modify code and to migrate the codes in the production environment and as such, programmers can manipulate production data. The Authority advised that this is necessary because programmers require access in cases when another programmer is not available. Currently, GPA Computer Services only has one position designated to allow, modify 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.

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

   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 and activity logs monthly. This could assist in detecting manipulation of system codes and application systems.

3. Enhancement to Network Security

   Condition: There is a lack of control over network activities. Without appropriate levels of control, a greater chance may exist of incurring data integrity and confidentiality issues. For example, hackers may be able to gain access to the Authority's network and view or modify sensitive information.

   Recommendation: A firewall should be installed to restrict access from outside parties and to monitor network activities. Network violation reports should be regularly reviewed. Also, network vulnerability testing and/or network penetration testing should be performed annually.

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. 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 cease interest capitalization on projects that are not actively undergoing activities to prepare them for use.

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

   Condition: Of nine assets tested, we noted the following.

   - HT1000,VHF 5 Watts 2 Channel (asset no. 2719238) could not be located due to the lack of an identification number.
   - Roadrunner 2 W2MB 860 Telx (asset no. 2733363) was traded-in for a new set of handheld roadrunners, but the asset was not removed from the fixed asset listing.

   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 regularly update subsidiary ledgers. A prenumbered asset retirement form should be utilized to account for asset disposals and to facilitate communication with Accounting to allow the update of the subsidiary ledger.

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

3. Incorrect Late Charges

   Condition: A new residential customer account receivable contains incorrect late charges assessed in September 2009 for $59,139. The error was discovered by GPA during manual checking of bills for unusual amounts prior to mailing. The error was corrected on October 8, 2009. As a result, receivable and late charge revenues were overstated as of September 30, 2009. This error occurred in the Utiligy system and appears to affect some new accounts in the initial months billing. The errors are either discovered during the manual checking of bills or through customer complaints.

SECTION II – OTHER MATTERS, CONTINUED

3. Incorrect Late Charges, Continued

   Recommendation: Although this system error does not appear to have caused significant errors in the financial statements (total recorded late charges as of September 30, 2009 approximated $375,000), GPA should continue to work with the consultant to determine the cause and find a resolution. This should improve efficiency as less time will be required on manual correcting procedures.

4. Reconciliation of Customer Deposits and Review of Related Accrued Interest

   Condition: At September 30, 2009, customer deposit subsidiary details contain negative balances that should have a zero balance. Furthermore, no regular review of related accrued interest occurs.

   Recommendation: Customer deposit accounts should be regularly reviewed.

5. 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" and miscellaneous accrued account is not regularly reviewed to clear transactions from the account.

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

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

6. Synchronization of Work Order Status

   Condition: The work order status between the J.D. Edwards ("JDE") and the Utiligy systems is not synchronized. Further, customer information in Utiligy contains work orders that have already been cancelled. This is due to an Utiligy system limitation that prohibits GPA from cancelling created work orders. Specifically, we noted that an open work order was not closed for a meter change out made in 2008. As a result, the meter had no monthly usage but incurred monthly service charges.

   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 assist in avoiding an accumulation of work orders to be corrected and to improve the completeness of billings.

7. Monitoring of Temporary Streetlights

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

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

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

SECTION II – OTHER MATTERS, CONTINUED

8. Defective Fuel Auto Gauges

Condition: Auto gauges are devices used to record fuel consumption and issuance. 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.

9 Internal Reporting

Condition: Claims and collections reported by Engineering on a quarterly basis do not reconcile with amounts reported by Accounting.

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

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

10. Meter Reading Exception Reports

Condition: Of twenty-five meter reading exception reports tested, we noted the following:

- Six reports contained items that are not within the exception criteria. This results in inefficiency in the meter reviewing process;
- One report contained an exception that was not corrected on the same billing period, and
- For all the tested exception reports, there is no evidence that the hash totals are used to verify the completeness of the exception listings. Further, the hash totals are not accurate. There is also no evidence of a review of the results of the exception investigations.

Exception reports should be designed to ensure that the effectiveness and efficiency of the reports are facilitated. If the exception report reflects exceptions within the criteria, this would give more time for personnel involved in verifying these exceptions to concentrate on actual exceptions and the review process can be facilitated.

Recommendation: The Authority should consider revising the process to allow maximum efficiency and to allow for the timeliness of investigations and the correction of actual usage exceptions.

SECTION II – OTHER MATTERS, CONTINUED

11. Review of Defective Meters

    Condition: One account registering low consumption was only back billed for actual consumption on the fifth month. The low consumption was due to a meter without a seal.

    Recommendation: GPA should review meter status on a monthly basis and ensure that meters are sealed. Accounts registering low-consumption should be reviewed for a possibility of defective meters after two consecutive months of registering as low-consumption. This practice would assist in limiting and avoid accumulation of unbilled charges.

12. OS 400 Computer System Value Setting Best Practices

    Condition: Currently, the Authority has not activated the security setting of "QINACTITV" in the AS400 system. This setting requires a user to re-sign in after a pre-determined time of inactivity. The best practice setting is 30 minutes. However, we recognize that certain jobs take longer than 45 minutes to complete. Therefore, the Authority could activate the security setting with a higher value of 70 minutes, to coincide with the setting of "**QDSCJOBITV" (**the system ends a disconnected job after 70 minutes**).**

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

13. 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 should be documented. The AS/400 user profiles listing dated October 13, 2009 contained two terminated employees.

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

    Recommendation: The Authority should verify the status of these employees and immediately remove them if appropriate. 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.

14. 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.

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

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

SECTION II – OTHER MATTERS, CONTINUED

15. 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.

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

    Recommendation: The Authority should follow existing policies and procedures or amend then, if appropriate.

16. Inappropriate Access to Sensitive System Commands

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

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

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

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.

APPENDIX II

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.