

March 31, 2006

Consolidated Commission on Utilities (CCU):

In planning and performing our audit of the financial statements of Guam Power Authority (GPA) for the year ended September 30, 2005, on which we have issued our report dated March 31, 2006, we developed the following recommendations concerning matters related to its internal control. Our recommendations are summarized below:

Finding No. 1 – Revenue Reconciliation

Criteria: Internal revenue reports should be monitored and significant variances should be investigated.

Condition: There is a difference of 4,541,299 KWH between the summary of KWH usage as generated in the proof of revenue report and the KWH sales recorded in the general ledger. Specifically, the following differences were noted:

Customer Category	KWH Usage per Proof of Revenue	KWH Sales per Books	Difference
Residential	505,219,034	503,165,147	2,053,887
Small General Demand	199,605,051	198,896,154	708,897
Small Demand	101,772,264	101,170,046	602,218
Others	510,844,314	509,668,017	1,176,297

Cause: We did not see any evidence of review to ensure that a comparison of the two reports occurs.

Effect: Revenues and receivables may be immaterially misstated.

Recommendation: We recommend that GPA monitor and research significant variances between the proof of revenue report and revenue billed.

Finding No. 2 – Reconciliation of Fuel Consumption

Criteria: Differences in fuel consumption recorded in accounting and actual fuel consumption reported by Generation should be investigated.

Condition: There were differences of approximately \$600 thousand in fuel consumption as recorded in GPA's accounting records versus consumption recorded through meters in the Generation department.

Cause: We understand that differences arose from the fact that the Accounting department records the consumption based on fuel inventories and Generation reports the fuel consumption based on the usage as recorded by meters in the Generation Plant.

Finding No. 2 – Reconciliation of Fuel Consumption, Continued

Effect: There is no impact on the financial statements, but there could be unauthorized usage of fuel.

Recommendation: We recommend that GPA monitor and research significant variances in fuel usage recorded by Accounting versus Generation.

Finding No. 3 – Allowance for Funds Used During Construction (AFUDC)

Criteria: For regulated entities, the capitalized interest policy should be approved by the regulator.

Condition: GPA's interest capitalization policy has not been approved by the Public Utilities Commission (PUC).

Cause: GPA has not submitted its interest capitalization policy to the PUC for its approval.

Effect: There is no financial statement effect as a result of this condition; however, AFUDC calculations may be questioned.

Recommendation: GPA should submit its capitalization policy to the PUC for approval.

Finding No. 4 – Accounting for Federal Grants

Criteria: Federal grant expenditures should be properly accounted for in accordance with Government Accounting Standards Board Statement (GASB) #33.

Condition: Grant expenditures were not recorded as receivables and capital contributions. Federal reimbursements received were recorded as a reduction of construction work in progress.

Cause: There appears to be a lack of understanding of how to account for federal grant expenditures and related reimbursements.

Effect: Receivables, contributed capital and construction in progress were misstated before adjustment.

Recommendation: Federal grant expenditures should be recorded in accordance with GASB #33.

Finding No. 5 - Testing of Disaster Recovery Plan/Business Continuity Plan

Criteria: A formal Disaster Recovery Plan and/or a Business Continuity Plan should be in place.

Condition: A current Disaster Recovery Plan (DRP) and/or a Business Continuity Plan (BCP) relating to the Information System's Operations were not available for our review. GPA has DRPs for Electrical Transmission and Distribution recovery in the event of a disaster.

Cause: It appears that GPA has not yet formalized the documentation of the above plans.

Effect: Without a DRP/BCP, the business system and its technical functions could be exposed to the risk of an extended amount of down time. In the event of a disaster, employees may not be aware of procedures to restore the information system to its original operation.

In addition, regular testing of the DRP and BCP is required to ensure that the plans remain current and consistent with the critical business processes. The absence of testing of the plans may potentially delay the restoration of critical business processes and the information system, which may result in operational problems and financial losses.

Finding No. 5 - Testing of Disaster Recovery Plan/Business Continuity Plan, Continued

Recommendation: We recommend that management perform a business impact analysis to ensure that DRP's encompass the existing computing environment, and to test the plans on a periodic basis.

Some possible options to consider (but not restricted to) for the testing are:

- The testing scenario should change from test to test;
- Conduct surprise tests when possible, taking into account financial and safety implications;
- The restoration of off-site data should be tested;
- Vendor (if any) performance should be included in the testing of recovery plans;
- Test objectives and criteria should be formally developed and published;
- Test planning assumptions should be developed and published;
- Test results are formally critiqued and the results published; and
- Identify and document plan inadequacies; test results should be promptly reported.

Finding No. 6 - Assignment of Users to Appropriate User Classes and Special Authorities

Criteria: Computer system users should only be granted access to the appropriate user classes.

Condition: Some users were granted access to incorrect user classes and assigned inappropriate Special Authorities. The following User Classes that have inappropriate assignments include:

1. *SECOFR
2. *PGMR
3. *USER

Special Authority Settings

User Class	Current Special Authority Settings	Recommended Special Authority Setting	Management Response
*PGMR	*SPLCTL, *JOBCTL, *ALLOBJ, *SERVICE, *SAVSYS, *IOSYSCFG	Remove: *ALLOBJ	
*USER	*SPLCTL, *JOBCTL, *ALLOBJ, *SERVICE, *SAVSYS, *IOSYSCFG	Remove: *SPLCTL, *JOBCTL, *ALLOBJ, *SERVICE, *SAVSYS, *IOSYSCFG Recommended Setting for *USER = *NONE	

Limited Capability Settings

User Class	Current Limited Capability Settings	Recommended Limited Capability Setting	Management Response
*USER	*YES, *NO, *PARTIAL	*YES	

Finding No. 6 - Assignment of Users to Appropriate User Classes and Special Authorities, Continued

Condition, Continued:

User Class Assignment

User Class	Current Users Inappropriately Assigned to User Class	Recommended User Assignment to User Class	Management Response
*SECOFR	JOHNPC JINKYS JDETRAIN JAMES1 CRACEQ CHARLENEB ROBERTG JOEC HANSOM DMRJMT03 ADMIN TONY TESSIEF PAT1 PATD JIMP3 BROOKF	<p>Remove *SECOFR Users Listed on the Left and place them in the following User Classes</p> <p>*PGMR = For individuals listed providing programming functions, implementation functions, and/or consulting functions.</p> <p>*SYSOPR = For individuals listed on the left providing Computer Operations functions (other than the *SECOFR Jim Pinaula).</p>	

Cause: There is a lack of review of the assignment of user classes to certain individuals.

Effect: It is inappropriate to assign user's rights through Special Authorities and User Classes to allow access to secure AS/400 tools and information. The following issues for each assignment are as follows:

- Special Authorities: To control security and grant proper access rights, users placed into User Classes should only be allowed certain Special Authorities. By granting authorities to the class, the Security Officer is reducing the risk of inappropriate access to sensitive data, programs and parameter settings. By removing the *ALLOBJ authority from the *PGMR class, the production applications are always separated from the programmer's AS/400 working environment. Therefore, this setting will mitigate the risk of programmers accessing production applications. By removing all special authorities from the *USER class and replacing the special authority setting to *NONE, risk of users accessing sensitive data will be reduced.
- Limited Capability: The Limit Capabilities parameter can be used to prevent users from modifying their current library, attention key program and initial menu and program as well as to limit their ability to execute system commands. All *USER class' limited capability should be set to *YES. *YES is the most restrictive control as it prevents users from changing any of their initial program, menu and library settings as well as restricting them from entering system commands.
- User Class Assignments: Primary concentration for user class assignments focus on the *SECOFR user class. This is the highest level of security for the AS/400 and should be restricted to the System Manager, Security Administrator and Backup Security Administrator. Users with this status have access to all resources on the AS/400 and distributing access over many people increased the risk of system integrity and failure.

Finding No. 6 - Assignment of Users to Appropriate User Classes and Special Authorities, Continued

Recommendation: In general, Special Authorities should be granted with strict controls to reduce the risk of inappropriate access to sensitive information based upon the users skills and needs. *ALLOBJ and *AUDIT should be restricted to the Security Officer and the Department Administrator only. For Limited Capability, all users in the *USER class should have limited capability set only to *YES.

For User Class Assignments, all users should be placed into classes that grant appropriate access. For instance, all end users should be placed in the *USER class and all programmers should be placed in the *PGMR user class. Only the Security Officer and Department Administrator (and if applicable, the Assistant Security Officer) should be placed into the *SECOFR class.

User classes such as *PGMR, *SYSOPR and *SECADM are currently not being utilized. To better secure the AS/400, place programmers, system operators and if needed security administrators in proper user classes to reduce the risk of inappropriate access.

Finding No. 7 - Access to Production

Criteria: Access and making changes to the production environment should not be granted to the same individual.

Condition: The programmers are granted access to the production data. They were all granted access to the following objects through the User Class *SECOFR and the *ALLOBJ authority.

The system programmers are also responsible for developing changes to the interface and migration of these modifications to the production environment. Therefore segregation of duties is compromised.

Cause: There appears to be inappropriate assignment of access to certain individuals.

Effect: 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.

Recommendation: In general, programmers should not have access to production. This access should be limited to users and administrators who need it in order to perform their daily tasks. We recommend that formal segregation of duties be defined and applied in respect of the process of making changes and moving updated versions to production, in addition, activities log should be reviewed on a periodic basis.

Finding No. 8 - Inappropriate Audit and History Log Settings

Criteria: Monitoring commands settings should be activated appropriately.

Condition: The Audit Control (QAUDCTL) has been set to *NONE.

Cause: There appears to be a need to review settings of appropriate commands.

Effect: When QAUDCTL is set to *NONE, the ability for the Security Officer to audit user attempts to access secure data and/or delete sensitive data cannot be recorded.

Recommendations: Management should require all system audit functions to be adequately set to record and review all attempts by users to access/delete sensitive and secure data. The system settings should be as follows:

Finding No. 8 - Inappropriate Audit and History Log Settings, Continued

Recommendations, Continued:

Audit Function	Current Settings	Recommended Setting	Management Response
QAUDCTL	*NONE	*AUDLVL	
QAUDLVL	*SECURITY *DELETE *CREATE *OBJMGT *SAVRST	Add to Current Settings: *AUTFAIL	

Audit reports should be reviewed regularly by both the Security Officer and Department Manger and signed to acknowledge review was performed. If exceptions are found, such should be reported to security management and procedures should be performed to maintain system security and integrity. After review of reports, they should be stored in a secured location.

Finding No. 9 - Public Object Authority Assignment

Criteria: Sensitive commands should have proper settings.

Condition: We noted two instances where the *PUBLIC user was assigned an inappropriate Object Authority for two Objects.

Cause: The access settings to these sensitive commands do not appear to have been reviewed.

Effect: The improper access granted to the *PUBLIC user for sensitive objects increases the risk of users changes and or deleting the object. The following is a list of objects where the *PUBLIC user has inappropriate object authority.

Object	Current *PUBLIC Object Authority	Recommended *PUBLIC Object Authority	Management Response
#SUELIB	*CHANGE	*USE	
#DFULIB	*CHANGE	*USE	

Recommendation: Management should consider changing the current *PUBLIC Object Authority from *CHANGE to *USE for Objects #SUELIB and #DFULIB.

Finding No. 10 - Inappropriate Access to Sensitive System Commands

Criteria: Use of sensitive commands should be restricted.

Condition: We noted that the “public authority” to the list of sensitive system commands set to *USE (see Appendix 1).

Cause: It seems that the access settings to these sensitive commands do not appear to have been reviewed.

Effect: The commands as listed in appendix 1 are sensitive system commands which should be restricted to *PUBLIC, that is, *PUBLIC should be having *EXCLUDE access to minimize unauthorised operations performed on the system.

Finding No. 10 - Inappropriate Access to Sensitive System Commands, Continued

Recommendation: Management should ensure that the *PUBLIC are assigned *EXCLUDE access to these commands. For cases where further access is required, management should assess the appropriateness of the assignment.

Finding No. 11: - Computer System User Profiles

Criteria:

Computer user profiles (IDs) for terminated employees should be promptly deleted. No system users should have more than one user ID.

Condition:

We reviewed the user profiles listing dated February 16, 2005, and noted that:

- a) Some users may no longer be employees, but their user ID was still active.
- b) Some users have redundant user IDs.

Cause:

It appears that user access is not regularly reviewed.

Effect:

The existence of redundant user profiles increases the risk of unauthorized access to the system without being detected promptly.

Recommendation:

We recommend that management review user profiles to determine whether they are still in use or required for operation and if the user profile belongs to a current employee.

Additionally, procedures should be established to review user profiles on a regular basis (semi-annually) to detect and remove redundant profiles.

Auditee Response:

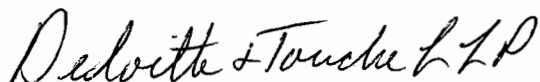
- a) In the process of being renewed and corrected.
- b) This is based on GPA's discretion. There are certain situations that require more than one user profile.

* * * * *

This report is intended solely for the information and use of the Consolidated Commission on Utilities, the management of Guam Power Authority and the Office of the Public Auditor of Guam.

We wish to express our appreciation for the cooperation of the staff and management of GPA during the course of our audit. We would be available to discuss any questions that you may have concerning the above comments at your convenience.

Very truly yours,



APPENDIX 1

COMMAND	DESCRIPTION	PUBLIC AUTHORITY
ADDAUTLE	Add Authorisation List Entry.	*USE
CHGAUTLE	Change Authorisation List Entry.	*USE
CHGDSTPWD	Change Dedicated Service Tools Password.	*USE
CHGDTA	Change Database File (Using DFU).	*USE
CHGOBJOWN	Change Object Ownership.	*USE
CHGUSRPRF	Change User Profile.	*USE
CLRLIB	Clear Library.	*USE
CLROUTQ	Clear Output Queue.	*USE
CRTAUTL	Create Authorisation List.	*USE
CRTCLPGM	Create Control Language Program.	*USE
CRTLIB	Create Library	*USE
CRTOUTQ	Create Output Queue	*USE
CRTUSRPRF	Create User Profile	*USE
DLTAUTHLR	Delete Authority Holder	*USE
DLTAUTL	Delete Authorisation List	*USE
DLTDFUPGM	Delete DFU Program	*USE
DLTLIB	Delete Library	*USE
DLTPGM	Delete Program	*USE
DLTUSRPRF	Delete User Profile	*USE
EDTAUTL	Edit Authorisation List	*USE
EDTOBJAUT	Edit Object Authority	*USE
GRTOBJAUT	Grant Object Authority	*USE
RMVAUTLE	Remove Authorisation List Entry	*USE
RVKOBJAUT	Revoke Object Authority	*USE
SAVSYS	Save System	*USE
STRDFU	Start DFU	*USE
STRSEU	Start SEU	*CHANGE
UPDDTA	Update Data (using DFU)	*USE
VRYCFG	Vary Controller Description on or off	*USE
WRKSYSSTS	Work with System Status	*USE
WRKUSRPRF	Work with User Profile	*USE