AUDITOR GENERAL
WILLIAM O. MONROE, CPA

PUBLIC SERVICE COMMISSION CASE MANAGEMENT SYSTEM

INFORMATION TECHNOLOGY AUDIT

Summary

Pursuant to Florida law[1,2], the Public Service Commission (Commission) serves as a state regulatory agency and consists of five commissioners. The Commission regulates or oversees various operations of the telecommunications, electric, gas, and water and wastewater industries. The Commission promulgates rules governing utility operations, hears and settles complaints, issues written orders similar to court orders, and enforces state laws affecting the utility industries.

Matters to be brought before the Commission for regulatory or oversight decisions are organized and tracked by docket (case). Once a docket is established, the activities relating to the docket are tracked in the Case Management System (CMS). Our audit focused on evaluating selected Commission information technology (IT) functions and determining the effectiveness of general and CMS application controls.

Although we did not identify any significant control deficiencies within the CMS application, certain general control deficiencies were noted which, if uncorrected, could, over time, jeopardize the reliability of the system. Specifically:

- ***We noted instances where the Commission had not established an appropriate segregation of duties among IT functions, increasing the risk of erroneous or unauthorized modification or destruction of data.***
- ***Deficiencies existed in the Commission's IT security administration, increasing the risk that access to IT resources were not appropriately controlled.***
- ***The Commission had not established an adequate information system development methodology, increasing the risk of changes to programs and data outside of management's authorization.***
- ***We noted instances where the Commission had not adequately utilized sufficient security control features to protect CMS information resources and also noted aspects of the Commission's business continuity/disaster recovery plan that needed improvement.***

[1] Section 350.01(1), Florida Statutes
[2] Section 350.011, Florida Statutes

Background:

Matters which are to be addressed by the Commission or which otherwise involve the exercise of the Commission's authority are identified and recorded and a case (informally referred to as a docket) is opened. All documents associated with a specific matter are identified by the same docket number.

Once a docket is established, the activities relating to the docket are tracked in CMS. The system tracks such items as the date the docket was opened, the type of docket, its current status, staff assigned, events scheduled to occur, documents filed, utilities involved, and names and addresses of parties of record and interested persons. CMS plays a major role in tracking mission-critical events and is the primary tool used by Commission management and staff to keep dockets on specific timelines in accordance with appropriate statutes and rules.[3,4]

The Commission's Bureau of Records and Hearing Services is the primary user responsible for the maintenance of CMS information. CMS was custom-developed by Commission staff within the Bureau of Information Processing (BIP). CMS is a multi-user interactive application written using Microsoft FoxPro and operated on the Commission's Novell local area network.

Finding No. 1:

We noted instances where the Commission had not established an appropriate segregation of duties among IT functions, increasing the risk of erroneous or unauthorized modification or destruction of data.

An important aspect of good management controls is a division of roles and responsibilities to prevent the possibility for a single individual to subvert a critical process. In the information technology area, a division of roles should generally be maintained between information system use, network management, system administration, systems development and maintenance, and security administration. In the area of program change control, the organization should segregate duties such that programmers are not responsible for moving programs into production and do not have update access to production libraries or data. Segregation of duties can be enforced through proper system access controls by which access privileges are limited to those individuals who require the access to accomplish their job duties and employees are restricted from performing incompatible functions. Where an appropriate segregation of duties does not exist, compensating controls, such as monitoring the activities of the individuals, should be in place in order to mitigate the risk of errors or fraud occurring and being concealed.

Our audit disclosed the following:

- The Commission had assigned "Supervisor Equivalent" (Administrator) access rights to six individuals within the Bureau of Information Processing which provided unlimited access. These individuals, referred to by the Commission as network supervisors, also functioned as security administrators, programmers, network administrators, or tape librarians. In addition, there were no monitoring activities in place for the actions of these individuals. In response to our audit inquiries, the Commission indicated that monitoring the actions of

[3] Chapters 350, 364, 366, 367, and 368, Florida Statutes
[4] Chapters 25 and 28, Florida Administrative Code

these individuals would be the responsibility of the Commission's new Information Security Officer (ISO) hired during our audit field work.

- Three application programmers had update access as a user to CMS production data. Additionally, these individuals were among the six network supervisors noted above.
- For program changes, two CMS application programmers performed the functions of system analysis, code design, and the movement of changes into production. There was no independent review or approval prior to the modified programs being moved into the production environment.

The absence of segregation of duties, along with the lack of monitoring, increased the risk that erroneous or fraudulent transactions could be processed, that improper program changes could be implemented and not be detected, and that computer resources could be damaged or destroyed.

Recommendation:

The Commission should review the existing security administration and application programming functions and implement a segregation of duties wherever practicable. In particular, the Commission should limit programmer access to the production environment to reduce the risk of erroneous or fraudulent transactions being initiated. Where an appropriate segregation of duties is not established, the Commission should carefully monitor the activities of the affected individuals.

Finding No. 2:

Deficiencies existed in the Commission's IT security administration, increasing the risk that access to IT resources were not appropriately controlled.

Senior management should establish a structure to implement the security program throughout the entity. The effectiveness of the security program is affected by the way in which responsibility for overseeing its implementation is assigned. A central management approach is key to ensuring that the various activities associated with managing risks are carried out. Additionally, effective IT security administration includes, among other things, a standardized process for documenting requests for system access, a formal approval procedure outlining the data or system owner who is responsible for granting the access privileges, and periodic review of the appropriateness of employee access privileges.

Our audit disclosed certain aspects of the Commission's IT security administration that needed improvement. Specifically:

- The Commission had delegated security administration responsibilities to six individuals; however, there was not a centralized management structure for the security administration function to ensure that the various activities and procedures associated with managing risks were carried out. In response to our audit inquiries, the Commission indicated that its new ISO will provide centralized management for the security administration function.

- CMS user access authorizations were e-mailed to one of the security supervisors from CMS group owners. However, these e-mails were not maintained as documentation of the user's access authorization and approval. In response to our audit inquiries, the Commission indicated that the e-mails regarding the CMS access rights are now being kept on file.
- The Commission did not have a control process in place to periodically review and confirm the appropriateness of access rights.

Without an established security management structure and clearly assigned security responsibilities for overseeing its implementation, there is an increased risk that activities and procedures will not be in place to appropriately manage risks related to unauthorized access. Additionally, the absence of periodic reviews of user access rights increases the risk that unauthorized access to information resources may not be prevented or detected.

Recommendation:

The Commission should establish a central management for security administration with appropriate procedures to ensure user access is appropriately requested, authorized, and documented. Furthermore, the Commission should periodically review user access rights, and when necessary, make appropriate changes to ensure access privileges remain accurate and current.

Finding No. 3:

The Commission had not established an adequate information system development methodology, increasing the risk of changes to programs and data outside of management's authorization.

Controls over systems development and modification activities are intended to ensure that new systems and system changes are suitably approved, designed, tested, and implemented.

Our audit disclosed deficiencies in the Commission's information system development methodology as follows:

- The Commission had prepared standard operating procedures[5] for managing program modifications in the areas of scope/impact determination, approval requirements for requested program modifications, and the logging of approved program modifications. However, documentation was not maintained to demonstrate that these procedures were being followed.
- The Commission's standard operating procedures for managing program changes did not address control of program modifications progressing through the design, programming, testing, final approval, and implementation phases.
- Functional specifications were not prepared as a basis for user approval and for programmers to code program changes.

[5] SOP 1412, In-house Applications Services

- A record of program modifications moved into production was not maintained.
- Tests of program code changes were performed in the test environment; however, tests dependent on data were performed in the CMS production environment, which could jeopardize "live" data.

Without establishing and documenting policies and procedures controlling system development for CMS modifications, the risk is increased that erroneous or unauthorized program modifications will be placed into production and that information could be inappropriately modified or destroyed.

Recommendation:

The Commission should enhance its standard operating procedures to manage all aspects of the program change process to ensure that all CMS modifications are properly documented, authorized, designed, tested, and implemented.

Finding No. 4:

We noted instances where the Commission had not adequately utilized sufficient security control features to protect CMS information resources and also noted aspects of the Commission's business continuity/disaster recovery plan that needed improvement.

Controls should be in place to protect data and programs from unauthorized access and to restore those programs and data and resume operations in the event of a disruption.

During our audit, we identified certain deficiencies in certain security control features and the Commission's business continuity/disaster recovery plan. Specific details of these deficiencies are not disclosed in this report to avoid any possibility of compromising Commission information. However, the appropriate Commission personnel have been notified of the deficiencies.

Without adequate security and business continuity controls in place, the risk is increased that CMS's information resources may be subject to improper modification or undue disruption.

Recommendation:

The Commission should implement the appropriate controls over security and business continuity to ensure the continued integrity and availability of CMS data and computer resources.

Other Matters:

The United States Congress passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[6], primarily as a way to allow individuals to carry health insurance from employer to employer. However, the law also addresses privacy and reporting requirements for electronic data interchange, privacy, and information security standards for personal health information.

The Commission indicated that the Director of the Division of the Commission Clerk and Administrative Services (CCA) had been assigned the responsibility of determining the effect of HIPAA on the Commission's internal systems. In addition to the CCA Director's research, Human Resources and BIP staff within CCA were consulted on the issue. The Commission indicated that the issue may have been informally discussed with Commission legal staff; however, no formal legal opinion was requested. The Commission staff responsible for

[6] Public Law 104-191

reviewing the effect of HIPAA attended meetings with the State Technology Office and other State agency security officers to gain an understanding of HIPAA requirements. Based upon this understanding, informal reviews were performed and it was determined that no information in CMS would be affected by HIPAA regulations.

Scope, Objectives, and Methodology:

The scope of this audit focused on evaluating selected IT functions applicable to CMS during the period August 2002 through January 2003. Our objectives were to determine the effectiveness of selected general and application controls relating to CMS, and to determine the Commission's awareness of HIPAA legislation and what actions, if any, had been taken concerning this legislation.

In conducting this audit, we interviewed appropriate Commission personnel, observed processes and procedures, and performed various other audit procedures to test selected controls.

Authority:

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our audit.

William O. Monroe, CPA
Auditor General

Commission Response:

In a response letter dated April 3, 2003, the Executive Director generally concurred with our audit findings and recommendations. The Executive Director's response can be viewed in its entirety on the Auditor General Web site.

THIS PAGE INTENTIONALLY LEFT BLANK

We conducted our audit in accordance with applicable standards contained in *Government Auditing Standards* issued by the Comptroller General of the United States. This audit was conducted by Cathy Jones, CISA, and supervised by Shelly Posey, CISA. Please contact Jon Ingram, CPA*, CISA, Audit Manager, with any questions regarding this report. He may be reached via e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other Auditor General reports can be obtained on our Web site (www.state.fl.us/audgen); by telephone at (850) 487-9024; or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

*Regulated by State of Florida

STATE OF FLORIDA

COMMISSIONERS:
LILA A. JABER, CHAIRMAN
J. TERRY DEASON
BRAULIO L. BAEZ
RUDOLPH "RUDY" BRADLEY
CHARLES. M. DAVIDSON

EXECUTIVE DIRECTOR
MARY ANDREWS BANE
(850) 413-6055

Public Service Commission

April 3, 2003

Mr. William O. Monroe, CPA
Auditor General
111 West Madison Street
G74 Claude Pepper Building
Tallahassee, Florida 32399-1450

Dear Mr. Monroe:

Pursuant to Section 11.45(4)(d), Florida Statutes, enclosed is the Commission's response to the preliminary and tentative findings and recommendations from your Information Technology Audit of the Public Service Commission's Case Management System, for the period August 2002 through January 2003.

We appreciate the professional and constructive approach your team brought to the audit process, and feel that the report will provide a valuable tool to improve our administration of this system. If you have questions or require additional information, please contact the Commission's Inspector General, Mr. Steve Stolting, at 413-6338.

Sincerely,

Mary Andrews Bane

Mary Andrews Bane
Executive Director

MAB/ba

Enclosure

cc: Chairman Lila A. Jaber
Ms. Blanca Bayó, Director, Commission Clerk and Administrative Services
Mr. Steve Stolting, Inspector General

Agency Response
PUBLIC SERVICE COMMISSION
CASE MANAGEMENT SYSTEM
INFORMATION TECHNOLOGY AUDIT

Finding No. 1:
We noted instances where the Commission had not established an appropriate segregation of duties among IT functions, increasing the risk of erroneous or unauthorized modification or destruction of data.

Recommendation:
The Commission should review the existing security administration and application programming functions and implement a segregation of duties wherever practicable. In particular, the Commission should limit programmer access to the production environment to reduce the risk of erroneous or fraudulent transactions being initiated. Where an appropriate segregation of duties is not established, the Commission should carefully monitor the activities of the affected individuals.

Response:
We concur with this finding, and procedures will be implemented for the Information Security Officer (ISO) to review existing security administration and application programming functions using Bindview software, which profiles access rights. This information will be used to segregate duties where practicable. Where duties cannot be segregated, new procedures and software will improve monitoring, including required notification to the application owner and ISO of any changes, and maintenance of required documentation for any changes requested and made. In addition, the ISO is evaluating software such as LT Audit+, which would create an automated audit trail of any modifications to program code and databases to ensure that unauthorized changes are detected.

Finding No. 2:
Deficiencies existed in the Commission's IT security administration, increasing the risk that access to IT resources were not appropriately controlled.

Recommendation:
The Commission should establish a central management for security administration with appropriate procedures to ensure user access is appropriately requested, authorized, and documented. Furthermore, the Commission should periodically review user access rights, and when necessary, make appropriate changes to ensure access privileges remain accurate and current.

Response:
We concur with this finding, and as of November 2002, the Commission established centralized management for security administration by designating Mr. Chris Church as the Information

Security Officer (ISO). The ISO will review and amend procedures to ensure that changes in user access are appropriately requested, authorized and documented. Implementation of the software and procedures outlined in our response to Finding 1 will also improve the capability of the Commission to ensure user access is periodically reviewed. Additional new procedures will include automated notification to the ISO of personnel changes that would affect access rights, including hires, terminations, and reassignments.

Finding No. 3:
The Commission had not established an adequate information system development methodology, increasing the risk of changes to programs and data outside of management's authorization.

Recommendation:
The Commission should enhance its standard operating procedures to manage all aspects of the program change process to ensure that all CMS modifications are properly documented, authorized, designed, tested, and implemented.

Response:
We concur with this finding, and procedures for control and tracking of program changes, including those discussed in our response to Finding 1, will be formalized in the standard operating procedures.

Finding No. 4:
We noted instances where the Commission had not adequately utilized sufficient security control features to protect CMS information resources and also noted aspects of the Commission's business continuity/disaster recovery plan that needed improvement.

Recommendation: The Commission should implement the appropriate controls over security and business continuity to ensure the continued integrity and availability of CMS data and computer resources.

Response:
We concur with this finding and the Commission is already moving forward with several projects in this area, purchasing required materials and modifying internal procedures to prevent improper modification or undue disruption of the CMS data and computer resources.