REPORT NO. 2010-197
JUNE 2010

PUBLIC SERVICE COMMISSION

CASE MANAGEMENT SYSTEM

Information Technology Operational Audit

For the Period
December 2009 Through March 2010
and Selected Actions from January 1, 2009,
and Through April 23, 2010

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

PUBLIC SERVICE COMMISSION AND EXECUTIVE DIRECTOR

Pursuant to Section 350.01, Florida Statutes, the Commission consists of five Commissioners who serve four-year terms. Commissioners are appointed by the Governor and confirmed by the Senate pursuant to Section 350.031, Florida Statutes. The Executive Director is employed by the Commission and serves at the pleasure of the Commission. Commissioners and Executive Directors who served during the audit period are listed below:

Nancy Argenziano, Chair from January 2, 2010
Lisa Polak Edgar
Nathan A. Skop
David E. Klement, from October 22, 2009
Ben A. "Steve" Stevens III, from January 2, 2010
Matthew M. Carter II, Chair to January 1, 2010
Katrina J. McMurrian, to October 5, 2009

Timothy J. Devlin, Executive Director from January 25, 2010
Dr. Mary Andrews Bane, Executive Director to December 31, 2009

The audit team leader was Chris Gohlke, CPA, CISA, and the audit was supervised by Shelly Posey, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, by e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

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

PUBLIC SERVICE COMMISSION

Case Management System

SUMMARY

Matters to be brought before the Public Service Commission (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 information technology (IT) controls applicable to CMS for the period December 2009 through March 2010 and selected actions from January 1, 2009, and through April 23, 2010. We also determined the status of corrective actions regarding prior audit findings disclosed in our report No. 03-176 that were applicable to the scope of this audit. The results of our audit are summarized below:

Case Management System and Related IT Controls

Finding No. 1: Certain Commission user identification and authentication controls needed improvement with regard to uniquely identifying system users and protecting the confidentiality of user passwords.

Finding No. 2: The Commission's procedures governing the management of IT access privileges needed improvement. Additionally, some employees had unnecessary or inappropriate network or CMS access privileges.

Finding No. 3: The Commission had not performed adequate background checks of employees with sensitive IT responsibilities and access privileges

Finding No. 4: The Commission's program change control procedures and process for CMS needed improvement.

Finding No. 5: The Commission had not established a security awareness training program to facilitate employee education and training on information security responsibilities.

Finding No. 6: Certain Commission network security controls and IT disaster recovery plan provisions needed improvement.

Additional Matter

Finding No. 7: The Commission disabled the text messaging functions of BlackBerries (smartphones used by some Commission employees), other than standard e-mail. As of April 23, 2010, the Commission was in the process of revising its Administrative Procedures Manual for the use of these communication technologies.

BACKGROUND

The Commission regulates or oversees various operations of the telecommunications, electric, natural gas, and water and wastewater industries in the State. The Commission exercises regulatory authority over utilities through rate regulation; competitive market oversight; and monitoring of safety, reliability, and service.

Matters which are to be decided 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. CMS captures and maintains information used to assist in the

Commission's decision-making processes such as the date the docket was opened, the type of docket, the current status of the docket, staff assigned, events scheduled to occur, documents filed, utilities involved, and names and addresses of parties of record and interested persons. The Commission's Office of Commission Clerk is the primary user responsible for the maintenance of CMS information. CMS, a multiuser interactive system operated on the Commission's local area network, was custom developed by Commission staff within the Office of Information Technology Services (OITS).

FINDINGS AND RECOMMENDATIONS

Case Management System and Related IT Controls

Finding No. 1: User Identification and Authentication Controls

Access controls involve the use of computer hardware and software to prevent or detect unauthorized access by requiring users to input user identifications (IDs), passwords, or other forms of identification and authentication that are linked to predetermined access privileges. The unique identification and authentication of system users allows management to affix responsibility for system activity to an individual employee. The effectiveness of password-based authentication is dependent on controls that protect the confidentiality of the passwords, such as password length and complexity requirements, lockouts for invalid access attempts, and requirements for passwords to be changed on regular intervals and not be reused.

Our audit disclosed that some user IDs and passwords for network administration and CMS functions were being shared by multiple users, limiting the Commission's ability to assign responsibility for system activities. Specifically:

- Seven employees shared the user ID and password for restoring backups.
- The three network storage platform administrators shared a user ID and password.
- The three firewall administrators shared a user ID and password.
- Three employees shared one user ID and password with update access privileges to CMS. These employees also had their own individual user IDs for accessing CMS.

The Commission developed a network password policy covering requirements for password length, complexity requirements, and inactivity timeouts. However, the policy did not address requirements for account lockouts when users exceed a maximum number of invalid access attempts, limitations on password reuse, or minimum required password change intervals. The risk of password compromise and unauthorized access would be further reduced if such requirements were included in the password policy. In response to audit inquiry, the Commission updated its network password policy to include the above-mentioned items.

Our audit also disclosed that the network password policy applied only to network accounts and not to other hardware and software with authentication controls independent of the network. The lack of password policies for other hardware and software increases the risk that security controls intended by management may not be implemented.

Additionally, as similarly noted in our report No. 03-176, the Commission's password policy required passwords to be changed only every 180 days. Our review also noted that this policy was not being enforced by the network for 29 field users and 22 local users. If passwords are not periodically changed, the risk is increased that the passwords will be discovered by unauthorized users who may gain access to the Commission's data or other IT resources. In response to audit inquiry, the Commission implemented enforcement of the 180-day password change setting for all

but 9 of the field users and all but 1 of the local users. The risk of password compromise would be further reduced if passwords were required to be changed on a more frequent basis and if the change requirement were enforced for all Commission users.

Our audit also disclosed that some additional password control parameters required in the Commission's password policy were not software-enforced. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the Commission's data and IT resources. However, we have notified appropriate Commission management of the specific issues.

Recommendation: The Commission should continue its efforts to improve user identification and authentication controls. Specifically, the Commission should assign each system user a unique user ID, expand the scope of its network password policy, and enforce the policy for all users.

Finding No. 2: Management of Access Privileges

Effective access controls include measures that limit user access privileges to only what is needed in the performance of assigned job duties. Appropriately restricted access privileges help protect IT resources from unauthorized disclosure, modification, and destruction. Periodic reviews of access privileges help management ensure access privileges remain appropriate. Effective management of system access privileges also includes provisions to timely remove employee access privileges when employment terminations occur. Prompt action is necessary to ensure that a former employee's access privileges are not misused by the former employee or others.

Our audit disclosed that the Commission's procedures governing the management of IT access privileges needed improvement. Specifically:

- As similarly noted in our report No. 03-176, the Commission had not developed written procedures defining the process and documentation requirements for authorizing, granting, and removing access privileges for both the network and CMS. Additionally, the Commission had not developed written procedures for periodically reviewing access privileges for CMS.
- Various provisions of the Commission's network access procedures were inaccurate. For example, the procedures referenced positions that no longer existed, software that was no longer used, and services that were no longer offered.

As indicated by the issues discussed in the following paragraphs, the lack of comprehensive and accurate written procedures for managing IT access privileges increases the risk that system access will not be restricted in a consistent manner pursuant to management's expectations.

Our audit disclosed that some employees had unnecessary access privileges to CMS or access privileges that had not been authorized by the functional owner, increasing the risk of unauthorized disclosure, modification, or destruction of CMS data. Specifically:

- As similarly noted in our report No. 03-176, three OITS employees had update access privileges to CMS that were not necessary for their job duties as described in their formal job descriptions.
- The CMS update access privileges of four users had not been authorized by the functional owner. In response to audit inquiry, the functional owner indicated that, although she had not authorized the access privileges, the privileges were appropriate for all four users.

We also reviewed the access privileges for the network and CMS for all 50 former Commission employees who terminated employment during the period January 1, 2009, through December 4, 2009. Our review noted a former employee whose network access privileges were not removed for 38 days after termination. Upon audit inquiry,

Commission management removed the former employee's access privileges. Under these conditions, the risk was increased that the access privileges could be misused by the former employee or others.

Recommendation: The Commission should establish more comprehensive procedures for managing network and CMS access privileges and address inaccuracies in the network access procedures. Additionally, the Commission should remove all unnecessary or inappropriate access privileges and ensure that all access privileges have been authorized in writing by the functional owner.

Finding No. 3: Background Checks

Periodic background checks, including fingerprinting and a criminal history check through the Florida Department of Law Enforcement (FDLE) and the Federal Bureau of Investigations (FBI), help ensure that employees hired for positions requiring special trust do not have criminal records.

The Commission's Administrative Procedures Manual indicated that the Executive Director had designated all Commission employee positions as special trust. We selected eight employees within OITS with security administration responsibilities and noted that none had been fingerprinted or subjected to criminal history checks by the FBI and only two had been checked by FDLE. Each of the eight employees had been assigned sensitive IT responsibilities and granted elevated access privileges that indicated a need for them to be subject to background checks. In response to audit inquiry, Commission management indicated that the remaining six had been hired prior to the implementation of the background check procedure. Commission management also stated that they were investigating performing recurring background checks including fingerprinting and criminal history checks by FDLE and the FBI for all OITS employees. Without appropriate background checks, the risk is increased that a person with an inappropriate background could be employed in a position with sensitive responsibilities and be provided access privileges that could lead to misuse of critical resources.

Recommendation: The Commission should ensure that all employees in sensitive positions have undergone appropriate background checks. Additionally, the Commission should reperform background checks on a periodic basis.

Finding No. 4: Program Change Controls

Effective controls over application program changes include documentation, review, and approval requirements that are intended to ensure that only authorized and properly functioning program changes are implemented. Effective program change controls also include provisions for an appropriate separation of duties by ensuring that a group or persons independent of the application programmers approve program changes and control the movement of programs into production.

As similarly noted in our report No. 03-176, the Commission had not developed a comprehensive systems development life cycle methodology to govern the development and modification of application systems. Although the Commission had developed Standard Operating Procedure 1412, In-House Application Services, which included requirements for CMS systems development and modifications, the Procedure did not address the following:

- Documentation requirements,
- Mechanisms to ensure an appropriate separation of incompatible duties, and
- Requirements for the development of functional specifications.

We additionally noted that the Commission did not have a process in place to automatically record all program changes moved into production. The lack of such a process increases the risk that unauthorized changes could be moved into production without timely detection by management.

The above-described issues precluded the Commission from demonstrating, upon audit inquiry, that it followed an appropriate program change control process with regard to CMS. In response to audit inquiry, Commission management informed us that, in most cases, the development, review, testing, and movement of program changes to production were performed by the same person. This lack of separation of duties increased the risk that unauthorized program changes could be moved into production.

Recommendation: The Commission should establish a comprehensive systems development life cycle methodology that includes the above-noted change control procedures and process to promote the ongoing integrity of CMS.

Finding No. 5: Security Awareness Training

A comprehensive security awareness training program apprises new employees of, and reemphasizes to current employees, the importance of preserving the confidentiality, integrity, and availability of data and IT resources entrusted to them. The Commission had not established a security awareness training program to facilitate all employees' ongoing education and training on information security responsibilities. The lack of a comprehensive security awareness training program increases the risk that employees may inadvertently compromise information security while performing their assigned duties.

Recommendation: The Commission should promote security awareness through a comprehensive training program to ensure that all employees are aware of the importance of information in their possession and their responsibilities for maintaining its confidentiality, integrity, and availability.

Finding No. 6: Network Security Controls and IT Disaster Recovery Planning Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain Commission network security controls and provisions of IT disaster recovery planning that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the Commission's data and IT resources. However, we have notified appropriate Commission management of the specific issues. Without adequate network security controls and IT disaster recovery planning, the confidentiality, integrity, and availability of data and IT resources may be compromised, increasing the risk that Commission data and IT resources may be subject to improper disclosure, modification, or destruction.

Recommendation: The Commission should implement the appropriate network security controls and IT disaster recovery plan provisions to ensure the continued confidentiality, integrity, and availability of Commission data and IT resources.

Additional Matter

Finding No. 7: Communication Technologies

In an e-mail dated September 10, 2009, the Executive Director informed Commission staff that the text messaging functions of BlackBerries (smartphones used by some Commission employees), other than standard e-mail, had been disabled pending completion of an internal review of the use of these communication technologies within the Commission. As of April 23, 2010, the Commission was in the process of revising its Administrative Procedures Manual to address these technologies.

Recommendation: The Commission should continue its efforts to revise its Administrative Procedures Manual to provide the necessary guidance for these communication devices to Commission staff.

PRIOR AUDIT FINDINGS

Except as discussed in the preceding paragraphs, the Commission had taken corrective actions for findings applicable to the scope of this audit included in our report No. 03-176.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of this IT operational audit were to determine the effectiveness of selected IT controls applicable to CMS in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, and reliability of data; and the safeguarding of IT resources. An additional objective was to determine the extent to which the Commission corrected, or was in the process of correcting, deficiencies disclosed in our report No. 03-176 that were applicable to the scope of this audit.

The scope of our audit focused on evaluating selected IT controls applicable to CMS during the period December 2009 through March 2010 and selected actions from January 1, 2009, and through April 23, 2010.

In conducting our audit, we:

- Interviewed Commission personnel.
- Obtained an understanding of the Commission including the purpose, goals, and compliance requirements; basic data and business processing flows; IT organizational structure and management; and the interaction of CMS.
- Obtained an understanding of CMS, including the computing platforms and related software.

- Obtained an understanding of logical access paths to CMS and CMS data and tested whether logical access controls ensured that access privileges to the network, CMS, and associated data files, software, and databases were restricted to authorized users.
- Evaluated the effectiveness of wireless and other perimeter controls.
- Evaluated Commission policies and procedures that provide for security administration and systems development and modification.
- Observed selected controls over the design, testing, approval, and implementation of system program modifications.
- Evaluated the adequacy of the Commission's Business Continuity Plan and Disaster Recovery Plan, including backup procedures and tape handling.
- Observed, and tested the effectiveness of selected CMS input, processing, and output controls.
- Obtained an understanding of Commission controls to ensure that messages sent via mobile device text messaging were captured as part of the public record.

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 IT operational audit.

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

In a letter dated June 2, 2010, the Executive Director provided responses to our preliminary and tentative findings. This letter is included at the end of this report as EXHIBIT A.

EXHIBIT A
MANAGEMENT'S RESPONSE

STATE OF FLORIDA

Public Service Commission

June 2, 2010

Mr. David W. Martin
Auditor General
G74 Claude Pepper Building
111 W. Madison Street
Tallahassee, Florida 32399-0850

Dear Mr. Martin:

We are pleased to respond to the preliminary and tentative audit findings and recommendations of your information technology operational audit of the Public Service Commission Case Management System. As required by Section 11.45(4) (d), Florida Statutes, our response is as follows:

Finding No. 1: User Identification and Authentication Controls

Recommendation: The Commission should continue its efforts to improve user identification and authentication controls. Specifically, the Commission should assign each system user a unique user ID, expand the scope of its network password policy, and enforce the policy for all users.

Response: We agree that when feasible network administration tasks should be performed by staff utilizing unique and identifiable login credentials. We will implement unique login credentials for each system which supports this functionality.

For hardware and software with independent authentication controls the PSC agrees to implement a written password policy similar to our network password policy. When feasible, the password policy will be enforced with automated software controls. Not all hardware and software with independent authentication controls has a mechanism to enforce the written policy.

While PSC management continues to believe that a 180 day password expiration best balances our needs for security while minimizing the impact of more frequent password changes on Commission staff, Commission management agrees to consider a reduced interval for password changes and will incorporate any changes determined necessary in the password policy.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Mr. David W. Martin
Page 2
June 2, 2010

Finding No. 2: *Management of Access Privileges*

Recommendation: The Commission should establish more comprehensive procedures for managing network and CMS access privileges and address inaccuracies in the network access procedures. Additionally, the Commission should remove all unnecessary or inappropriate access privileges and ensure that all access privileges have been authorized in writing by the functional owner.

Response: We agree and will continue to refine our written procedures to address inaccuracies and document the assignment and removal of network and CMS access privileges by the functional owner. This will include regularly scheduled reviews of assigned access privileges and appropriate adjustments to ensure that only authorized users have access to resources.

Finding No. 3: Background Checks

Recommendation: The Commission should ensure that all employees in sensitive positions have undergone appropriate background checks. Additionally, the Commission should perform background checks on a periodic basis.

Response: We agree and have obtained the necessary authorizations from law enforcement to perform such checks for all information technology staff. In addition, we are currently developing Commission policies to conduct background checks and require rechecks every three years.

Finding No. 4: Program Change Controls

Recommendation: The Commission should establish a comprehensive systems development life cycle methodology that includes the above-noted change control procedures and process to promote the ongoing integrity of CMS

Response: We agree and will implement a systems development life cycle methodology which includes the change control procedures noted in the finding.

Finding No. 5: *Security Awareness Training*

Recommendation: The Commission should promote security awareness through a comprehensive training program to ensure that all employees are aware of the importance of information in their possession and their responsibilities for maintaining its confidentiality, integrity, and availability.

Response: We agree and have implemented annual training classes for all staff.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Mr. David W. Martin
Page 3
June 2, 2010

Finding No. 6: Network Security Controls and IT Disaster Recovery Planning Controls

Recommendation: The Commission should implement the appropriate network security controls and IT disaster recovery plan provisions to ensure the continued confidentiality, integrity, and availability of Commission data and IT resources.

Response: We agree and will implement network security controls and IT disaster recovery plan provisions to address the cited finding issues.

Finding No. 7: Communication Technologies

Recommendation: The Commission should continue its efforts to revise its Administrative Procedures Manual to provide the necessary guidance for these communication devices to Commission staff.

Response: We agree and have developed revised procedures which should be adopted within the near future. In the interim, all functionality of these devices other than standard e-mail remains effectively disabled.

We appreciate the efforts of you and your staff to assist the Commission in improving our information technology operations and will work diligently to implement the recommended measures. If you require further information, please contact our Inspector General, Steve Stolting, at 413-6338.

Sincerely,

Timothy J. Devlin
Executive Director

TJD:ld

cc: Chairman Nancy Argenziano
Mr. Steven J. Stolting