STATE OF FLORIDA

DIVISION OF EMERGENCY MANAGEMENT

RICK SCOTT
Governor

BRYAN W. KOON
Director

February 15, 2017

Bryan Koon, Director
Division of Emergency Management
2555 Shumard Oak Boulevard
Tallahassee, Florida, 32399-2100

Re: **Auditor General Report No. 2016-102**
State of Florida – Information Technology Operational Audit
Florida Public Assistance System (FloridaPA.org)
Six-Month Follow-up

Dear Director Koon:

As required by Section 20.055(6)(h), Florida Statutes, the six month status report for the subject audit is attached. The report details the implementation or current status of each recommendation.

If you have any questions, please call me at 815-4151

Sincerely,

Ronnie Atkins,
Deputy Inspector General

RA: ac

Enclosure

CC: Jonathan Lord, Deputy Director
Wes Maul, Chief of Staff
Kathy Dubose, Staff Director
Joint Legislative Auditing Committee
JLAC@leg.state.fl.use
Melinda Miguel, Chief Inspector General

Florida Division of Emergency Management
6-month Follow-up to the
Office of Auditor General
State of Florida – Information Technology Operational Audit
Florida Public Assistance (FloridaPA.org) Report #: 2016-102

Finding No. 1: IT Policies and Procedures

Our audit procedures disclosed that the Division had not established written policies or procedures related to FloridaPA.org configuration management and FloridaPA.org access security administration. Specifically, we found that:

- The Division had not established written policies or procedures to ensure that FloridaPA.org program changes or data changes made by the Division's software contractor were properly requested and reviewed. Without written configuration management policies or procedures to ensure FloridaPA.org program changes or data change requests are properly communicated to the software contractor and reviewed by Division staff once implemented by the software contractor, the risk is increased that erroneous or unauthorized application program changes or data changes may be moved into the FloridaPA.org production environment without timely detection.

- The Division had not established written procedures for administering and assigning access privileges to users of FloridaPA.org. Written procedures would enhance the Division's ability to ensure that user access privileges granted to individuals are authorized by management, appropriate for the accomplishment of assigned job duties, and commensurate with management's direction may be limited. A similar finding was noted in previous audits of the Division, most recently our report No. 2009-086.

Recommendation:

Division management should establish written policies and procedures for FloridaPA.org configuration management and FloridaPA.org access security administration.

FDEM Response:

The Division concurred with the recommendation. The Division's IT Section and Bureau of Recovery will coordinate to establish written policies and procedures for FloridaPA.org configuration management and FloridaPA.org access security administration.

6-month Follow-up Response:

The IT Section implemented controls for FloridaPA.org configuration management and FloridaPA.org access security administration. The IT Section has written Access and Security procedures that are in draft form awaiting formal adoption.

Completion Date: June 2017 (Partially Complete)

Finding No. 2: Periodic Reviews of User Access Privileges

Our audit procedures disclosed that the Division had not performed periodic reviews of FloridaPA.org nonapplicant user access privileges. Without periodic reviews of FloridaPA.org nonapplicant user access privileges, the risk is increased that unauthorized and inappropriate access privileges may exist and not be timely detected. A similar finding was noted in our report No. 2009-086.

Recommendation:

Division management should perform periodic reviews of FloridaPA.org nonapplicant user access privileges to verify that the access privileges are authorized and appropriate.

FDEM Response:

The Division concurred with the recommendation. The Division's IT Section and Bureau of Recovery will coordinate to establish written policies and procedures for periodic reviews of FloridaPA.org nonapplicant user access privileges to verify that the access privileges are authorized and appropriate.

6-month Follow-up Response:

The Bureau of Recovery and the IT Section are working with MB3, the IT consultant, to develop programmatic reminders in FloridaPA.org that will prompt subgrantees and Bureau of Recovery staff to review and update access privileges on a regular basis. At this time, the Subgrantee and Public Assistance Coordinators are reminded to review and update their access privileges on a quarterly basis. Approximately 6 months ago, the Bureau of Recovery conducted a review of all access privileges listed in FloridaPA.org and made the necessary corrections to ensure accuracy.

Completion Date: June 2017 (Partially Complete)

Finding No. 3: Appropriateness of Access Privileges

Our audit procedures disclosed some access controls related to FloridaPA.org system administration and security administration access privileges and to FloridaPA.org user groups that need improvement.

FloridaPA.org System Administration and Security Administration. Our examination of system administration and security administration access privileges for ten Division employees and eight contractors disclosed that some inappropriate and unnecessary system administration and security administration access privileges existed within FloridaPA.org. Specifically, we found that:

- Seven of the ten Division employees were FloridaPA.org users who had access privileges to both FloridaPA.org system administration and security administration functions that allowed the employees to make changes to FloridaPA.org, such as FloridaPA.org system administration parameter setting changes and access privileges changes.
- The remaining three of the ten employees included in our examination were security administrators who had access privileges to FloridaPA.org system administration functions that allowed the employees to make changes to FloridaPA.org system administration parameter setting changes and perform user functions (i.e., end-user functions).
- The eight contractors had access privileges to FloridaPA.org security administration functions that allowed the contractors to make assigned access privileges changes.

Each of these access privileges were inappropriate and unnecessary for the employees' or contactors' assigned job duties.

FloridaPA.org User Groups. FloridaPA.org user groups (user groups) were used to group and control access privileges to FloridaPA.org and were assigned to users based on their job duties. Our examination of assigned user groups disclosed that some users were assigned user groups that included access privileges that were appropriate and necessary for the users to perform their assigned job duties. However, the same user groups also included other access privileges that granted users the ability to perform functions that were inappropriate and unnecessary for the users' assigned job duties. For example, some Division employees (i.e., users) were granted access to perform supervisory and planning functions that were inappropriate and unnecessary for the employees' assigned job duties.

Division management indicated that changes in processes and related job duties were the primary causes of the inappropriate and unnecessary access privileges noted above. In addition, the Division's lack of periodic reviews of nonapplicant user access privileges as noted in Finding 2 may have contributed to the existence of these inappropriate or unnecessary access privileges. The existence of inappropriate and unnecessary access privileges increases the risk that unauthorized modification, loss, or disclosure of data and IT resources may occur. A similar finding was noted in our report No. 2009-086.

Recommendation:

Division management should limit user access privileges to FloridaPA.org to promote an appropriate separation of duties and restrict users to only those functions necessary for the users' assigned job duties.

FDEM Response:

The Division concurred. The Division's IT Section and Bureau of Recovery will coordinate to establish written policies and procedures to limit user access privileges to FloridaPA.org to promote an appropriate separation of duties and restrict users to only those functions necessary for the users' assigned job duties.

6-month Follow-up Response:

The Division's IT Section and Bureau of Recovery are working with MB3, the consultant, to update the workflows in FloridaPA.org. With these updates user groups will be assigned by job description, (i.e. Grants Specialist, PAC, Planner, Appeals, etc.) Once complete the Bureau of Recovery will ensure job descriptions are updated to reflect required actions in FloridaPA.org.

Completion Date: August 2017 (Incomplete)

Finding No. 4: Employee Access Deactivation

Our audit procedures disclosed that the Division did not timely deactivate the FloridaPA.org accounts for some former and transferred employees. Specifically, for eight former or transferred employees' FloridaPA.org accounts we reviewed, we found that:

- As of August 21, 2015, FloridaPA.org accounts for four former employees remained active for time periods ranging from 84 to 259 days after the employees separated from Division employment. Although the accounts were not timely deactivated, we noted that these former employees' FloridaPA.org accounts had not been used subsequent to the dates of employment separation.
- The Division did not deactivate the FloridaPA.org accounts for two former employees and one transferred employee until time periods ranging from 5 to 192 days had elapsed after the employees' dates of employment separation or transfer. Notwithstanding the untimely deactivation, the FloridaPA.org accounts of the former and transferred employees had not been used subsequent to the dates of employment separation or transfer.

Without timely deactivation of former and transferred employee FloridaPA.org accounts, the risk is increased that the accounts may be misused by the former or transferred employees or others. A similar finding was noted in our report No. 2009-086.

Recommendation:

Division management should ensure that the FloridaPA.org accounts of former and transferred employees are timely deactivated.

FDEM Response:

The Division concurred with the recommendation. The Division's IT Section and Bureau of Recovery will coordinate to establish written policies and procedures to ensure that the FloridaPA.org accounts of former and transferred employees are timely deactivated.

6-month Follow-up Response:

The Bureau of Recovery submits a FOCUS ticket at the time of separation or relocation requesting access to FloridaPA.org be deactivated for that former employee. In the event FOCUS is not operational, an email to the IT Section will be sent upon separation/relocation.

Completion Date: Complete

Finding No. 5: Positions of Special Trust

We found that the Division had not established procedures for the performance of background screenings for newly hired employees in positions of special trust or periodic background screenings of current employees in positions of special trust. Additionally, the Division had not designated IT positions that have system, database, developer, network, or other administrative capabilities related to FloridaPA.org as positions of special trust. Absent documented background screening procedures and the appropriate designation of applicable IT positions as positions of special trust the risk is increased that persons with inappropriate backgrounds may be employed or remain employed in positions of special trust and may gain access to confidential or sensitive data and IT resources. A similar finding was noted in previous audits of the Division, most recently in our report No. 2009-086.

Recommendation:

Division management should establish procedures for the designation of positions of special trust and the performance of background screenings for new hires, as well as periodic background screenings for employees in positions of special trust.

FDEM Response:

The Division concurred with the finding. The Division's IT Section and Bureau of Recovery will coordinate to establish procedures for the designation of positions of special trust and the performance of background screenings for new hires, as well as periodic background screenings for employees in positions of special trust.

6-month Follow-up Response:

The IT Section has drafted its Access procedure that addresses the Special Trust finding. The Access procedure is awaiting adoption.

Completion Date: April 2017 (Partially Complete)

Finding No. 6: Access Authorization Documentation

Our audit procedures disclosed that the Division's access authorization documentation for some employees and contractors with access to FloridaPA.org was missing, incomplete, or inaccurate. Specifically, we found that:

- For two of the nine employees and contractors included in our audit test, the access authorization forms showing supervisory approval were missing. For the remaining seven employees and contractors, four forms were incomplete as the forms did not have appropriate approvals.
- For four of the nine employees and contractors included in our audit test, help desk tickets supporting the approved access privileges were missing. Of the remaining five employees and contractors, four help desk tickets were incomplete or inaccurate as the tickets did not identify or match the user access privileges granted.

Division management attributed the lack of access authorization documentation to the high employee turnover rate within the Division and large decreases in staffing. The lack of complete and accurate access authorization forms limits management's assurances that access privileges are authorized and appropriately assigned. A similar finding was noted in our report No. 2009-086 and in Finding Number 2014-042 noted in our report No. 2015-166.

Recommendation:

Division management should maintain complete and accurate documentation demonstrating management's authorization of FloridaPA.org user access.

FDEM Response:

The Division concurred with the finding. The Division's IT Section and Bureau of Recovery will coordinate to establish procedures to maintain complete and accurate documentation demonstrating management's authorization of FloridaPA.org user access.

6-month Follow-up Response:

The Division has implemented documentation demonstrating management's authorization of FloridaPA.org user access.

Completion Date: Complete

Finding No. 7: Security Awareness Training

Although new employees received some security awareness training during new employee orientation, the Division had not implemented and maintained a comprehensive security awareness training program to facilitate all Division employees' ongoing education and training on security responsibilities, including password protection and usage, copyright issues, malicious software and virus threats, workstation and personal mobile device controls, and the handling of sensitive and confidential information. A comprehensive security awareness training program enhances Division employee awareness of the importance of information handled and their responsibilities for maintaining the confidentiality, integrity, and availability of Division data and IT resources. A similar finding was noted in prior audits of the Division, most recently our report No. 2009-086.

Recommendation:

Division management should implement and maintain a comprehensive security awareness training program to ensure that all Division employees are aware of the importance of the information handled and their responsibilities for maintaining the confidentiality, integrity, and availability of Division data and IT resources.

FDEM Response:

The Division concurred with the finding. The Division's IT Section will implement and maintain a comprehensive security awareness training program to ensure that all Division employees are aware of the importance of the information handled and their responsibilities for maintaining the confidentiality, integrity, and availability of Division data and IT resources.

6-month Follow-up Response:

The IT Section has implemented a comprehensive security awareness training program to ensure that all Division employees are aware of the importance of the information handled and their responsibilities for maintaining the confidentiality, integrity, and availability of Division data and IT resources. The IT Section has also hired an Information Security Manager and has developed draft IT security procedures.

Completion Date: Complete

Finding No. 8: Retention of Access Control Records

State of Florida, General Records Schedule GS1-SL for State and Local Government Agencies (General Records Schedule) provides that access control records must be retained for one anniversary year after superseded or after the employee separates from employment. Contrary to the requirements of the General Records Schedule, the Division did not retain relevant FloridaPA.org access control records related to the deactivation of employee access privileges. Without adequate retention of relevant FloridaPA.org access control records, the risk is increased that the Division may not have sufficient documentation to assist in future investigations of security incidents, should they occur.

Recommendation:

Division management should ensure that relevant FloridaPA.org access control records are retained as required by the General Records Schedule.

FDEM Response:

The Division's IT Section and Bureau of Recovery will coordinate to establish written policies and procedures to ensure that relevant FloridaPA.org access control records are retained as required by the General Records Schedule.

6-month Follow-up Response:

The IT Section Access procedure addresses record retention and is awaiting adoption.

Completion Date: April 2017 (Partially Complete)

Finding No. 9: Security Controls – Protection of Confidential and Exempt Data, User Authentication, Logging and Monitoring, and Other Security Controls

We are not disclosing specific details of the issues in this report to avoid the possibility of compromising FloridaPA.org data and IT resources. However, we have notified appropriate Division management of the specific issues. Without adequate security controls related to the protection of confidential and exempt data, user authentication, logging and monitoring, and other security controls for FloridaPA.org and related IT resources, the risk is increased that the confidentiality, integrity, and availability of FloridaPA.org data and related IT resources may be compromised. Similar findings related to logging and monitoring and other security controls were noted in our report No. 2009-086 and findings related to the protection of confidential and exempt data and user authentication were also communicated to Division management in connection with that report.

Recommendation:

Division management should improve certain security controls related to the protection of confidential and exempt data, user authentication, logging and monitoring, and other security controls for FloridaPA.org and related IT resources to ensure the continued confidentiality, integrity, and availability of FloridaPA.org data and related IT resources.

FDEM Response:

The Division concurred with the finding. The Division's IT Section and Bureau of Recovery will coordinate to improve certain security controls related to the protection of confidential and exempt data, user authentication, logging and monitoring, and other security controls for FloridaPA.org and related IT resources to ensure the continued confidentiality, integrity, and availability of FloridaPA.org data and related IT resources.

6-month Follow-up Response:

The Systems Security Policy has been drafted and is awaiting the adoption.

Completion Date: April 2017 (Partially Complete)

Finding No. 10: NEMIS Upload

During the period of our audit, Federal public assistance program data, including payment approvals and payment amounts, from the National Emergency Management Information System (NEMIS) was uploaded to FloridaPA.org on a daily basis, Monday through Friday. Although the Division had daily reports of the uploaded data counts and the error counts, the Division had not established procedures to ensure that all data was processed, error data was resolved, and reconciliations were performed between FloridaPA.org and NEMIS to promote the completeness and accuracy of FloridaPA.org payment approvals and payment amounts.

Without effective procedures related to the processing, error data resolution, and reconciliation of payment approvals and payment amounts in FloridaPA.org, the risk is increased that payment approvals and payment amounts may not be completely and accurately processed in FloridaPA.org and may result in inaccurate information being used by Division staff. A similar finding was noted in our report No. 2009-086.

Recommendation:

Division management should establish procedures to ensure that all payment approval and payment amount data is processed, error data is resolved, and reconciliations are performed in FloridaPA.org to promote the completeness, accuracy, and availability of FloridaPA.org data.

FDEM Response:

The Division concurred with the recommendation. The Division's IT Section and Bureau of Recovery will coordinate to establish procedures to ensure that all payment approval and payment amount data is processed, error data is resolved, and reconciliations are performed in FloridaPA.org to promote the completeness, accuracy, and availability of FloridaPA.org data.

6-month Follow-up Response:

The Division's IT Section and Bureau of Recovery are coordinating and working with the IT consultant to establish procedures to ensure that all payment approval and payment amount data is processed, error data is resolved, and reconciliations are performed in FloridaPA.org to promote the completeness, accuracy, and availability of FloridaPA.org data.

Completion Date: August 2017 (Incomplete)