



STATE OF FLORIDA
DIVISION OF EMERGENCY MANAGEMENT

Ron DeSantis
Governor

Jared Moskowitz
Director

May 7, 2019

Jared Moskowitz, Director
Florida Division of Emergency Management
2555 Shumard Oak Boulevard
Tallahassee, Florida, 32399-2100

Re: **Auditor General Report No. 2019-049**
Information Technology Operational Audit
Florida Public Assistance System (FloridaPA.org)

Dear Director Moskowitz:

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 let me know.

Regards,


Susan Cureton
Inspector General

Attachment

CC: Kevin Guthrie, Deputy Director
Melinda Miguel, Chief Inspector General
Joint Legislative Auditing Committee

**Florida Division of Emergency Management
Six-month Follow-up to the
Auditor General Report No. 2019-049**

Pursuant to Section 20.055(6)(h), Florida Statutes, the Office of Inspector General for the Florida Division of Emergency Management (FDEM) conducted a six-month follow-up to the Auditor General's Information Technology Operational Audit of FDEM, Report Number 2019-049. The final report was issued in November 2018, and contained nine findings with nine recommendations. The following is a summary of the findings and recommendations, along with FDEM Management's six-month status responses.

Finding 1: Policies and Procedures

The Division had not established written policies and procedures related to FloridaPA.org configuration management and had not completed, approved, and implemented a written plan or procedures to support the Division's Public Assistance Program and assist with the reconciliation processes between FloridaPA.org and other systems. A similar finding was noted in our report No. 2016-102.

Recommendation: We recommend that Division management establish and implement written policies and procedures for FloridaPA.org configuration management and complete, approve, and implement the draft plan and procedures to support the Division's PA Program including workflow and reconciliation processes.

FDEM Response: The Division concurs with the recommendation. The Division's Bureau of Recovery will establish and implement the written policies and procedures for the www.FloridaPA.org configuration management, as well as formalize the draft procedure for the Public Assistance Program including workflows, and reconciliation processes.

FDEM Six-Month Status Response: The Bureau of Recovery has drafted an updated policies and procedures for FloridaPA.org configuration management. The Bureau has engaged the Division's standardized operating system to formalize the procedures.

Finding 2: Access Authorization Documentation

Access authorization documentation for some nonapplicant users with access to FloridaPA.org was missing, incomplete, or did not match the access granted. Similar findings were noted in prior audits of the Division, most recently in our report No. 2016-102.

Recommendation: We again recommend that Division management maintain complete and accurate documentation demonstrating management's authorization of FloridaPA.org nonapplicant user access privileges.

FDEM Response: The Division concurs with the recommendation. The Division's Bureau of Recovery will coordinate with the Division's Information Technology Section to maintain complete and accurate documentation, in the form of user access forms, demonstrating authorization and access privileges to nonapplicant users.

FDEM Six-Month Status Response: The Bureau of Recovery has drafted an updated policies and procedures for FloridaPA.org access, which includes procedures on access authorization documentation. The procedures document internal controls within the Bureau of Recovery to ensure that the authorization forms are appropriately maintained. Forms will be maintained by the person who has authorized access, in FloridaPA, and within the Admin and Plans Unit. The Bureau has engaged the Division's standardized operating system to formalize the procedures.

Finding 3: Inappropriate Access Privileges

Some FloridaPA.org security groups did not promote an appropriate separation of duties and the access privileges for some Division employees and software contractor employees did not restrict users to only those functions appropriate and necessary for their assigned job duties. Similar findings were noted in prior audits of the Division, most recently in our report No. 2016-102.

Recommendation: We again recommend that Division management redefine the access privileges provided by the security groups 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 and ensure that incompatible job duties are appropriately separated.

FDEM Response: The Division concurs with the recommendation. The Division's Bureau of Recovery will coordinate with the Division's Information Technology Section to redefine access privileges by limiting the user access privileges provided by security group. The Division's Bureau of Recovery will re-evaluate user access and privilege against position duties to ensure appropriate access and ensure separation of duties.

FDEM Six-Month Status Response: The Bureau of Recovery has drafted an updated policies and procedures for FloridaPA.org access authorization, which includes access privilege definitions. The Bureau has engaged the Division's standardized operating system to formalize the procedures. The Bureau is still working on ensuring all current users adhere to the access privilege groups.

Finding 4: Timely Deactivation of Access Privileges

As similarly noted in prior audits, the Division did not timely deactivate the FloridaPA.org accounts for some former employees.

Recommendation: We again recommend that Division management ensure that the FloridaPA.org user access privileges for former employees are timely deactivated upon a user's separation from Division employment

FDEM Response: The Division concurs with the recommendation. The Division's Bureau of Recovery will coordinate with the Division's Information Technology Section to document and timely revoke access privileges for former employees in accordance with existing policy.

FDEM Six-Month Status Response: The Bureau of Recovery has drafted an updated policies and procedures for FloridaPA.org access authorization, which includes procedures on deactivation of access privileges. The procedures document internal controls to ensure that access is revoked timely. The Bureau has engaged the Division's standardized operating system to formalize the procedures.

Finding 5: Periodic Reviews of User Access Privileges

The Division had not performed periodic reviews of FloridaPA.org nonapplicant user access privileges to ensure that access privileges assigned were authorized and appropriate. Similar findings were noted in prior audits of the Division, most recently in our report No. 2016-102

Recommendation: We again recommend that Division management perform periodic reviews of FloridaPA.org nonapplicant user access privileges to verify that the access privileges are authorized and appropriate

FDEM Response: The Division concurs with the recommendation. The Division's Bureau of Recovery will establish written policies and procedures for periodic reviews of www.FloridaPA.org nonapplicant user access privileges to verify that the access privileges are authorized and appropriate. These procedures will include when the reviews will be performed, delineate personnel responsibility, and provide documentation guidelines.

FDEM Six-Month Status Response: The Bureau of Recovery has drafted an updated policies and procedures for FloridaPA.org access authorization, which includes periodic reviews of user access privileges to ensure access is appropriate. This review will be performed on a quarterly basis. The Bureau has engaged the Division's standardized operating system to formalize the procedures.

Finding 6: Security Awareness Training

Security awareness training processes need improvement to ensure all new employees receive training within 14 days of their hire date and documentation of training completed is maintained. Similar findings were noted in prior audits of the Division, most recently in our report No. 2016-102.

Recommendation: We recommend that Division management ensure that employees timely receive security awareness training and that documentation of the security awareness training is maintained to demonstrate compliance with Division policies.

FDEM Response: The Division concurs with the recommendation. The Division's Information Technology Section will ensure that employees receive security training, as well as document and maintain that documentation showing that the training took place in accordance with existing Division policy.

FDEM Six-Month Status Response: The Division regularly conducts New Employee Cybersecurity training. The Division has and will continue to ensure that new employees

receive cybersecurity training, as well as document and maintain that documentation showing that the training took place in accordance with existing Division policy.

Finding 7: Background Screening

As similarly noted in prior audits, background screenings for employees in positions of special trust in Information Technology Management were not always performed.

Recommendation: We recommend that Division management ensure that all employees occupying a position of special trust undergo a level 2 background screening as a condition of employment and continued employment.

FDEM Response: The Division concurs with the recommendation. The Division's Information Technology Section will coordinate with the Division's Human Resources Section to ensure that all Division personnel in positions of special trust undergo a level 2 background screenings. The Division has already undergone measures identifying employees in those positions and ensuring the appropriate background check is performed.

FDEM Six-Month Status Response: Employees in the Information Technology and Management (ITM) Bureau in positions of special trust have had the appropriate Level 2 background screenings and new employees within the ITM Bureau in positions of special trust are required to complete the Level 2 background screening as a condition of employment.

Finding 8: Records Retention

Contrary to the State of Florida General Records Schedule GS1-SL for State and Local Government Agencies retention requirements, the Division did not retain relevant FloridaPA.org access control records related to the deactivation of access privileges. A similar finding was noted in our report No. 2016-102.

Recommendation: We again recommend that Division management ensure that relevant FloridaPA.org access control records are retained as required by the General Records Schedule.

FDEM Response: The Division concurs with the recommendation. The Division's Bureau of Recovery and Division's Information Technology Section will ensure compliance with the Division's existing record retention policy and develop procedures to include the method and responsibility of maintaining access control records.

FDEM Six-Month Status Response: The Bureau of Recovery has drafted an updated policies and procedures for FloridaPA.org authorization access, which includes guidelines on retention of access forms. Forms will be maintained by the user, the Admin and Plans Unit, as well as uploaded to FloridaPA. The Bureau has engaged the Division's standardized operating system to formalize the procedures.

Finding 9: Security Controls – Transmission of Data and Logging and Monitoring

Certain security controls related to the transmission of data and logging and monitoring continue to need improvement to ensure the confidentiality, integrity, and availability of FloridaPA.org data and Division IT resources.

Recommendation: We recommend that Division management improve certain security controls related to the transmission of data and logging and monitoring 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 concurs with the recommendation. The Division's Information Technology Section and Bureau of Recovery will coordinate to improve certain security controls related to the transmission of data and logging and monitoring for FloridaPA.org and related IT resources to ensure the continued confidentiality, integrity, and availability of FloridaPA.org data and related IT resources

FDEM Six-Month Status Response: Protection of confidential and exempt data has been addressed in the Division's IT System Access and Use policy (SOP-ITM-003). It is also addressed during new employee cybersecurity training.