STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2019-049
November 2018

DIVISION OF EMERGENCY MANAGEMENT

Florida Public Assistance System
(FloridaPA.org)

Sherrill F. Norman, CPA
Auditor General

Director of the Division of Emergency Management

Section 14.2016, Florida Statutes, establishes the Division of Emergency Management within the Executive Office of the Governor. The head of the Division is the Director who is appointed by and serves at the pleasure of the Governor. During the period of our audit, the following individuals served as the Division Director:

Wes Maul	From October 1, 2017
Bryan Koon	Through October 26, 2017

The team leader was Wayne Revell, CISA, and the audit was supervised by Hilda S. Morgan, CPA, CISA.

Please address inquiries regarding this report to Brenda Shiner, CISA, Audit Manager, by e-mail at brendashiner@aud.state.fl.us or by telephone at (850) 412-2946.

This report and other reports prepared by the Auditor General are available at:

FLAuditor.gov

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 • 111 West Madison Street • Tallahassee, FL 32399-1450 • (850) 412-2722

DIVISION OF EMERGENCY MANAGEMENT

Florida Public Assistance System (FloridaPA.org)

SUMMARY

This operational audit of the Division of Emergency Management (Division) focused on evaluating selected information technology (IT) controls applicable to the Florida Public Assistance System (FloridaPA.org) and included a follow-up on the findings included in our report No. 2016-102. Our audit disclosed the following:

Finding 1: 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.

Finding 2: 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.

Finding 3: 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.

Finding 4: As similarly noted in prior audits, the Division did not timely deactivate the FloridaPA.org accounts for some former employees.

Finding 5: 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.

Finding 6: 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.

Finding 7: As similarly noted in prior audits, background screenings for employees in positions of special trust in Information Technology Management were not always performed.

Finding 8: 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.

Finding 9: 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.

BACKGROUND

Pursuant to State law,[1] the Division of Emergency Management (Division) is established within the Executive Office of the Governor as a separate budget entity and is responsible for maintaining a comprehensive Statewide program of emergency management. The Division:

- Plans for and responds to both natural and man-made disasters.
- Prepares and implements a Statewide Comprehensive Emergency Management Plan.
- Conducts damage assessment surveys and advises the Governor on whether to declare an emergency and seek Federal relief funds.
- Maintains a primary Emergency Operations Center, which serves as the communications and command center for reporting emergencies and coordinating State response activities.
- Is responsible for the State Emergency Response Team (SERT) which is composed of various intergovernmental entities, volunteers, and the private sector.
- Serves as the State's liaison between the Federal Emergency Management Agency (FEMA) and other public and private agencies and is responsible for coordinating FEMA efforts with other departments and agencies of State Government, county and municipal governments and school boards, and private agencies that have a role in emergency management.

The Emergency Management Mission Integrated Environment (EMMIE), formerly the National Emergency Management Information System (NEMIS), provides automated support for joint FEMA and State critical functions such as: managing infrastructure projects and grants, providing individual and family grants, and conducting preliminary damage assessments. On a daily basis, Monday through Friday, EMMIE interfaces Federal Public Assistance Program data, including payment approvals and payment amounts, to the Florida Public Assistance System (FloridaPA.org).

FloridaPA.org is a Web-based portal used to manage the Disaster Grants – Florida Public Assistance programs relating to disaster relief and recovery. Both applicant users, such as State agencies, local governments, and not-for-profit organizations, and nonapplicant users, such as Division employees and contractors, utilize FloridaPA.org. The Division's FloridaPA.org software contractor remotely provides application support to the Division through software patches and database administration functions for FloridaPA.org.

FINDINGS AND RECOMMENDATIONS

Finding 1: Policies and Procedures

Effective controls include the establishment of policies and procedures that describe management's expectations for controlling an organization's operations. Documented policies and procedures help ensure that management directives are clearly communicated, understood, accepted, and followed by all staff.

[1] Sections 14.2016 and 252.35(1), Florida Statutes.

Our audit procedures disclosed that, as of August 7, 2018, 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 and procedures related to the Public Assistance (PA) Program and selected reconciliation processes. 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. A similar finding was noted in our report No. 2016-102.
- The Division drafted but management had not approved and implemented the *PA Grant Management Plan* (*Plan*) that describes the basic policies and procedures to support the PA Program. The *Plan* provides the Division's Bureau of Recovery direction for completing workflows within the PA Program's account, project, and finance areas including workflows associated with the interface and reconciliation between FloridaPA.org and EMMIE and workflows associated with the single payment reconciliation and account reconciliation between FloridaPA.org and the Florida Accounting Information Resource Subsystem (FLAIR). Approving and implementing the *Plan* increases management's assurance that the PA Program workflows will be appropriately completed in accordance with management's directives.
- The Division began drafting a job aid document with procedures to help ensure that all data is processed, error data is resolved, and reconciliations are performed between the EMMIE and FloridaPA.org. However, this draft document had not been completed, approved, and implemented. Without effective procedures related to the processing, error data resolution, and reconciliation of 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. Similar findings were noted in prior audits of the Division, most recently 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.

Finding 2: Access Authorization Documentation

AST rules[2] provide that agency information owners are responsible for establishing and authorizing the types of privileges and access rights appropriate to system users. Effective access authorization practices include, among other things, the use of access authorization forms to document the user access privileges that management has authorized. Additionally, appropriately maintained access authorization documentation facilitates the complete and accurate assignment of user access privileges.

As part of our audit, we requested access authorization documentation for 11 of the 99 nonapplicant users with active access privileges to FloridaPA.org as of February 28, 2018, to determine whether FloridaPA.org access privileges granted to nonapplicant users were appropriately authorized and documented. The access authorization documentation requested consisted of *IT Systems Access* forms

[2] AST Rule 74-2.003(5)(g)6., Florida Administrative Code.

or, alternatively, Help Desk tickets showing supervisory approval and approved access groups. Our audit procedures disclosed that the Division's access authorization documentation for 10 of the 11 nonapplicant users reviewed was missing, incomplete, or inaccurate. Specifically, we found that:

- An *IT Systems Access* form, a Help Desk ticket, or other form of authorization documentation was not available for 4 of the 10 users. Therefore, Division records did not evidence supervisor authorization of user access or what, if any, access groups should have been assigned to a user.
- For the 6 users for whom a Help Desk ticket was available, the access groups noted on all 6 Help Desk tickets did not match the access groups granted and 4 of the 6 Help Desk tickets were missing supervisor approvals.

The lack of complete and accurate access authorization documentation limits management's assurance that access privileges are authorized and appropriately assigned. 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.

Finding 3: Inappropriate Access Privileges

Effective access controls include measures that restrict user access privileges to data and IT resources to only those functions that promote an appropriate separation of duties and are appropriate and necessary for the user's assigned job duties. Appropriately restricted access privileges help protect data and IT resources from unauthorized modification, loss, or disclosure.

Our audit procedures disclosed some users had unnecessary and inappropriate FloridaPA.org access privileges. As part of our audit procedures to evaluate the appropriateness of access privileges, we noted that three security groups that provide system administration or security administration functions were not appropriately defined. Specifically, two security groups provided system administration, security administration, and update to numerous end-user functions, and one security group provided security administration and update to numerous end-user functions, thereby combining access privileges that should be separated.

We performed additional audit procedures to evaluate the appropriateness of access privileges as of February 23, 2018, for the 11 Division employees and the 12 software contractor employees assigned one or more of the FloridaPA.org access groups described above that allowed a combination of system administration, security administration, and end-user update access privileges to numerous FloridaPA.org screens. Our evaluation disclosed that, in addition to the incompatible functions provided by the security groups, some users had inappropriate access privileges for their job duties. Specifically, we found that:

- For 2 of the 3 Division employees assigned the security group for security administration functions, neither the security administration access privileges nor the end-user update access privileges were needed for the employees' job duties.
- For 5 of the 9 Division employees assigned the security group for system administration functions, the system administration, security administration, and end-user update access privileges were not necessary based on the employees' job duties. While another 2 of the 9 Division employees,

1 of whom was also assigned the security group for security administration functions, required security administration and end-user update access privileges, the employees did not require system administration access privileges. The other 2 Division employees required system administration access privileges; however, they did not need security administration or end-user update access privileges.

- Based on the software contractor's responsibilities, the security administration and end-user update access privileges were inappropriate for 11 of the 12 software contractor employees assigned the security group for system administration functions.

The existence of inappropriate and unnecessary access privileges increases the risk that unauthorized modification, loss, or disclosure of data and IT resources may occur. 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.

Finding 4: Timely Deactivation of Access Privileges

Agency for State Technology (AST) rules[3] require agency control measures that ensure IT access is removed when an IT resource is no longer required. Prompt action to deactivate access privileges when a user separates from employment or access to the information is no longer required is necessary to help prevent the misuse of the access privileges.

As part of our audit procedures, we selected Division records for 5 of the 44 Division employees who separated from Division employment during the period July 1, 2017, through February 10, 2018, to evaluate whether the former employees' FloridaPA.org user access privileges were timely deactivated. Our audit procedures disclosed that the FloridaPA.org user access privileges for 3 of the 5 former employees remained active for periods ranging from 6 to 117 days after the employees separated from Division employment. Although the accounts were not timely deactivated, Division records indicated that the FloridaPA.org user access privileges for these 3 former employees had not been used subsequent to the respective dates of employment separation. In response to our audit inquiry, Division management indicated that supervisors did not always notify the Help Desk to ensure tickets to deactivate user accounts were created when employees separated from the Division. Similar findings were noted in prior audits of the Division, most recently in our report No. 2016-102.

Timely deactivation of FloridaPA.org user access privileges upon an employee's separation from Division employment reduces the risk that FloridaPA.org access privileges may be misused by the former employee or others.

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.

[3] AST Rule 74-2.003(1)(a)8., Florida Administrative Code.

Finding 5: Periodic Reviews of User Access Privileges

AST rules[4] provide that agency information owners are to review access rights (privileges) periodically based on assessed risk. Periodic reviews of user access privileges help ensure that only authorized users have access and that the access provided to each user remains appropriate.

In prior audits of the Division, most recently in our report No. 2016-102, we noted that the Division had not performed periodic reviews of FloridaPA.org nonapplicant user (Division employees and contractors) access privileges. Our follow-up procedures disclosed that, although the Division had a procedure in place requiring Division managers or supervisors to perform an annual review of access privileges for all nonapplicant users under their supervision, reviews of access privileges only occurred for selected individuals who had events such as separation from the Division, changes in position, or newly assigned managers or supervisors.

The periodic performance of a complete review of all FloridaPA.org nonapplicant user access privileges would increase management's assurance that the access privileges assigned to FloridaPA.org nonapplicant users are authorized and remain appropriate.

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.

Finding 6: Security Awareness Training

AST rules[5] require each agency to establish a program that includes, at a minimum, security awareness training within 30 days of employment and annually, and on-going education and reinforcement of security practices.

In report No. 2016-102, we noted that 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. As part of our follow-up procedures, we examined Division policies and procedures and noted that Division policies[6] now require authorized users to receive information security awareness training within 14 days of starting employment with the Division and prior to accessing confidential information. We evaluated security awareness training rosters to determine whether the six employees hired during the period of January 1, 2018, through February 28, 2018, had attended security awareness training within 14 days of their initial employment hire dates. Our audit procedures disclosed that, contrary to Division policies, security awareness training was not conducted until 28 days after one employee's initial employment date and, although we requested, the Division could not locate documentation of security awareness training for two other employees.

Timely security awareness training and reinforcement of security practices through this training, help to protect the confidentiality, integrity, and availability of Division data. Similar findings were noted in prior audits of the Division, most recently in our report No. 2016-102.

[4] AST Rule 74-2.003(1)(a)6., Florida Administrative Code.

[5] AST Rule 74-2.003(3)(b)(c), Florida Administrative Code.

[6] Division Policy SOP-ITM-003, *IT Systems Access and Use Policy*, implemented November 20, 2017.

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.

Finding 7: Background Screening

State law[7] requires each agency to designate those positions that, because of the special trust or responsibility or sensitive location, require security background investigations. State law[8] also provides that all persons and employees in such positions must undergo background screenings in accordance with State law[9] using level 2 screening standards,[10] including fingerprinting, as a condition of employment and continued employment. AST rules[11] advise agency heads to designate IT positions that have system, database, developer, network, or other administrative capabilities for systems, applications, or servers with risk categorization of moderate or higher as positions of special trust.

In report No. 2016-102, we reported that the Division had not established procedures for the performance of background screenings for employees hired in positions of special trust. We also reported that 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. As part of our follow-up procedures, we examined Division policies and procedures and noted that Division policies[12] now provide that certain employees in Information Technology Management (ITM) are in positions of special trust and are subject to a level 2 background screening, including fingerprinting, as a condition of employment.

We examined Division records for the 20 ITM employees in positions of special trust as of March 22, 2018, and found that the Division had not performed level 2 background screenings for 15 of the 20 employees. In response to our audit inquiry, Division management indicated that, although the level 2 background screening requirement was implemented in September 2016, Division management did not interpret State law to require level 2 background screenings for employees who occupied positions of special trust prior to the positions being designated as such and the Division had not designated any of the positions within ITM as positions of special trust until 2017.

Notwithstanding Division management's response, since July 1, 2012, State law has required that all employees who serve in positions of special trust be subject to level 2 background screenings as a condition of employment and continued employment. The Division, as a matter of best practices, should implement level 2 background screenings of all employees in positions of special trust to remain consistent with the intent of State law. Performing level 2 background screenings for all employees in positions of special trust provides management assurance that only those individuals with appropriate backgrounds are granted access to Division data and IT resources.

---

[7] Section 110.1127(2)(a), Florida Statutes.

[8] Section 110.1127(2)(a), Florida Statutes.

[9] Section 435.04(1)(a), Florida Statutes.

[10] Pursuant to Section 435.04, Florida Statutes, level 2 background screenings are to include, but need not be limited to, fingerprinting for Statewide criminal history records checks through the Department of Law Enforcement, national criminal history records checks through the Federal Bureau of Investigation, and may include local criminal records checks through local law enforcement agencies.

[11] AST Rule 74-2.002(1)(f)9., Florida Administrative Code.

[12] Division Policy SOP-ITM-003, *IT Systems Access and Use Policy*, implemented November 20, 2017.

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.

Finding 8: Records Retention

State of Florida, *General Records Schedule GS1-SL for State and Local Government Agencies* (*General Records Schedule*) provides that access control records for employees, contractors, or subscribers must be retained for 1 year after superseded or access rights are deactivated. However, the Division did not always retain relevant FloridaPA.org access control records related to the deactivation of access privileges for 1 year. 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. 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*.

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

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed certain security controls related to the transmission of data and logging and monitoring for FloridaPA.org and related IT resources continue to need improvement. 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 transmission of data and logging and monitoring 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 were noted in prior audits of the Division, most recently in our report No. 2016-102.

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.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Division had taken corrective actions for the applicable findings included in our report No. 2016-102.

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 from February 2018 through July 2018 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 the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected IT controls applicable to FloridaPA.org during the period July 2017 through June 2018 and selected actions subsequent thereto. The audit included selected business process application controls over transaction data input, processing, output, and interfaces; and selected application-level general controls over security management, logical access, user identification and authentication, change management, and logging and monitoring. The overall objectives of the audit were:

- To determine the effectiveness of selected IT controls in achieving management's control objectives of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.
- To determine whether management had corrected, or was in the process of correcting, all deficiencies disclosed in our audit report No. 2016-102.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for the IT systems and controls included within the scope of the audit, deficiencies in management's internal controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT systems and controls included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding of the IT systems and controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting this audit, we:

- Interviewed Division personnel and reviewed FloridaPA.org-related documentation to obtain an understanding of:
  - FloridaPA.org background information including the purpose and goals involving financial, operations, and compliance requirements.
  - FloridaPA.org data and business process flows including key sources of data input, key application transactions and processes, and key types of application data output, including interfaces.
  - The FloridaPA.org computing platform, including applicable hardware, operating system, database management system, and security software.
- Evaluated FloridaPA.org transaction data input and processing controls related to claims payment processing and reconciliations. Specifically, we evaluated the review and approval process for public assistance claims to determine whether the claims were appropriately reviewed and approved prior to processing, claim dates were validated, and errors and irregularities were detected, reported, and corrected.
- Evaluated FloridaPA.org transaction data output controls related to claims reporting to determine whether controls were in place to reasonably assure claim data is timely reported and accounted for, key workflow dates are captured, and approvals for claims are accurately processed including historical data.
- Evaluated FloridaPA.org interface controls related to EMMIE to determine whether controls were in place to reasonably assure that the interfaces were processed accurately, completely, and timely, and rejected interface data was isolated, analyzed, and corrected timely.
- Evaluated FloridaPA.org interface controls related to FLAIR. Specifically, we reviewed the single payment and account level reconciliation process between FloridaPA.org and FLAIR.
- Evaluated the logging and monitoring controls related to FloridaPA.org to determine whether application transactions and access security changes were logged and monitored.
- Evaluated application security management controls including the security awareness program, documented security policies and procedures, and background screenings for positions designated as positions of special trust. Specifically, we examined:
  - Security awareness training documentation to determine whether security awareness training was timely provided to the six Division employees hired during the period January 1, 2018, through February 28, 2018.
  - Background screening documentation to determine whether background screenings had been performed for the 20 ITM employees in positions of special trust as of March 22, 2018.
- Evaluated selected FloridaPA.org application access controls. Specifically, we evaluated:
  - The appropriateness of access authorization documentation as of February 28, 2018, for 11 of the 99 FloridaPA.org nonapplicant users.
  - Whether access records related to the deactivation of user access privileges are retained for 1 year in accordance with the *General Records Schedule*.
  - Whether periodic access reviews were performed to ensure the continued appropriateness of access privileges assigned.

- The appropriateness of access for the 11 Division employees and the 12 software contractor employees as of February 23, 2018, assigned one or more of the three high risk access groups allowing system administration, security administration, and end-user update functions.
- The appropriateness of access for the 26 Division employees as of February 23, 2018, assigned selected end-user access privileges to FloridaPA.org.
- The FloridaPA.org user access accounts as of February 23, 2018, for 5 of the 44 Division employees who separated from Division employment during the period July 1, 2017, through February 10, 2018, to determine whether user access privileges were timely deactivated for the former employees.

- Evaluated FloridaPA.org authentication and identification controls as of April 13, 2018, and June 29, 2018, and e-mail encryption processes as of June 11, 2018.
- Evaluated FloridaPA.org application configuration management policies and procedures to ensure that FloridaPA.org application changes from the software contractor are authorized and reviewed.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. 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.

Sherrill F. Norman, CPA
Auditor General

STATE OF FLORIDA

DIVISION OF EMERGENCY MANAGEMENT

RICK SCOTT
Governor

WESLEY MAUL
Director

November 05, 2018

Ms. Sherrill F. Norman
Claude Denson Pepper Building, Suite G74
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

Enclosed is the Florida Division of Emergency Management's response to the preliminary and tentative findings and recommendations for the Auditor General's operational audit of the Florida Public Assistance System (www.FloridaPA.org).

If you have any questions or need additional assistance, please contact Susan Cureton, Deputy Inspector General at (850)-815-4151 or susan.cureton@em.myflorida.com .

Sincerely,

Wesley Maul
Director

DIVISION HEADQUARTERS
2555 Shumard Oak Blvd
Tallahassee, FL 32399-2100

Tel: 850-815-4000
www.FloridaDisaster.org

STATE LOGISTICS RESPONSE CENTER
2702 Directors Row
Orlando, FL 32809-5631

FINDINGS AND RECOMMENDATIONS

Finding 1: Policies and Procedures

Finding 1: 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.

State Agency Response and Corrective Action Plan:

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.

Estimated Corrective Action Date: May 06, 2019

Agency Contact: Joseph Oglesby (850)-815-4134

Finding 2: Access Authorization Documentation

Finding 2: 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.

State Agency Response and Corrective Action Plan:

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.

Estimated Corrective Action Date: January 07, 2019

Agency Contact: Richard Butgereit (850)-815-4701 & Joseph Oglesby (850)-815-4134

Finding 3: Inappropriate Access Privileges

Finding 3: 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.

State Agency Response and Corrective Action Plan:

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.

Estimated Corrective Action Date: May 06, 2019

Agency Contact: Richard Butgereit (850)-815-4701 & Joseph Oglesby (850)-815-4134

Finding 4: Timely Deactivation of Access Privileges

Finding 4: 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.

State Agency Response and Corrective Action Plan:

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.

Estimated Corrective Action Date: January 07, 2019

Agency Contact: Richard Butgereit (850)-815-4701 & Joseph Oglesby (850)-815-4134

Finding 5: Periodic Reviews of User Access Privileges

Finding 5: 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.

State Agency Response and Corrective Action Plan:

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.

Estimated Corrective Action Date: May 06, 2019

Agency Contact: Richard Butgereit (850)-815-4701 & Joseph Oglesby (850)-815-4134

Finding 6: Security Awareness Training

Finding 6: 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.

State Agency Response and Corrective Action Plan:

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.

Estimated Corrective Action Date: January 07, 2019

Agency Contact: Richard Butgereit (850)-815-4701

Finding 7: Background Screening

Finding 7: 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.

State Agency Response and Corrective Action Plan:

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.

Estimated Corrective Action Date: January 07,2019

Agency Contact: Richard Butgereit (850)-815-4701

Finding 8: Records Retention

Finding 8: 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.

State Agency Response and Corrective Action Plan:

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.

Estimated Corrective Action Date: May 06, 2019

Agency Contact: Richard Butgereit (850)-815-4701 & Joseph Oglesby (850)-815-4134

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

Finding 9: 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.

State Agency Response and Corrective Action Plan:

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.

Estimated Corrective Action Date: May 06, 2019

Agency Contact: Richard Butgereit (850)-815-4701 & Joseph Oglesby (850)-815-4134