STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2016-102
March 2016

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 Director of the Division is appointed by and serves at the pleasure of the Governor. Bryan Koon served as the Director of the Division during the period of our audit.

The team leader was Andrew Denny, CISA, and the audit was supervised by Tina Greene, CPA, CISA.

Please address inquiries regarding this report to Arthur Hart, CPA, Audit Manager, by e-mail at arthart@aud.state.fl.us or by telephone at (850) 412-2923.

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

www.myflorida.com/audgen

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. 2009-086 and Finding Number 2014-042 noted in our report No. 2015-166. Our audit disclosed the following areas in FloridaPA.org IT controls and operational processes that need improvement:

Finding 1: The Division had not established written policies or procedures related to FloridaPA.org configuration management and FloridaPA.org access security administration to ensure that FloridaPA.org program changes or data change requests were properly communicated to the Division's software contractor and reviewed by Division staff once implemented by the software contractor and that user access privileges granted to individuals were authorized by management, appropriate for the accomplishment of assigned job duties, and commensurate with management's direction. A similar finding related to FloridaPA.org access security administration procedures was noted in previous audits of the Division, most recently in our report No. 2009-086.

Finding 2: The Division had not performed periodic reviews of FloridaPA.org nonapplicant user access privileges to ensure that the access privileges assigned were authorized and appropriate. A similar finding was noted in our report No. 2009-086.

Finding 3: The access privileges for some Division employees and contractors and FloridaPA.org user groups did not promote an appropriate separation of duties and did not restrict users to only those functions appropriate and necessary for their assigned job duties, thus increasing 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.

Finding 4: As similarly noted in our report No. 2009-086, the Division did not timely deactivate the FloridaPA.org accounts for some former and transferred employees, thus increasing the risk that the FloridaPA.org accounts may be misused by the former or transferred employees or others.

Finding 5: The Division had not established procedures for the performance of background screenings of newly hired employees in positions of special trust or periodic background screenings of current employees in positions of special trust and also had not designated IT positions that have system, database, developer, network, or other administrative capabilities related to FloridaPA.org as positions of special trust to reduce the risk 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.

Finding 6: As similarly noted in our report No. 2009-086 and Finding Number 2014-042 noted in our report No. 2015-166, access authorization documentation for some employees and contractors with

access to FloridaPA.org was missing, incomplete, or inaccurate, thus limiting management's assurances that access privileges were authorized and appropriately assigned.

Finding 7: 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 and the handling of sensitive and confidential information. A similar finding was noted in prior audits of the Division, most recently in our report No. 2009-086.

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 employee access privileges, thus increasing the risk that the Division may not have sufficient documentation to assist in future investigations of security incidents, should they occur.

Finding 9: Certain security controls related to protection of confidential and exempt data, user authentication, logging and monitoring, and other security controls for FloridaPA.org and related IT resources continue to need improvement to ensure the continued confidentiality, integrity, and availability of FloridaPA.org data and related IT resources.

Finding 10: 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 the National Emergency Management Information System (NEMIS) to promote the completeness and accuracy of FloridaPA.org payment approvals and payment amounts. A similar finding was noted in our report No. 2009-086.

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 ensures that Florida is prepared to respond to emergencies, recover from them, and mitigate their impacts. The Division is responsible for the State Emergency Response Team (SERT) which is composed of various intergovernmental entities, volunteers, and the private sector. The Division is also responsible for coordination with the efforts of the Federal Government (Federal Emergency Management Agency [FEMA]), 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 National Emergency Management Information System (NEMIS) is a system used by FEMA and the states. 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, NEMIS interfaces Federal public assistance program data, including payment approvals and payment amounts, to the Florida Public Assistance System (FloridaPA.org).

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

FloridaPA.org is a Web-based portal used to manage the Disaster Grants – Florida Public Assistance programs relating to disaster relief and recovery. The Agency for State Technology - Southwood Data Center provides technical infrastructure support to the Division, including the server and network connections used by FloridaPA.org. The Division's software contractor provides application design and support services for FloridaPA.org. FloridaPA.org is used by applicant and nonapplicant users. Applicant users include State agencies, local governments, and not-for-profit organizations, whereas nonapplicant users include Division employees and contractors.

FINDINGS AND RECOMMENDATIONS

Finding 1: IT Policies and Procedures

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

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.

Finding 2: Periodic Reviews of User Access Privileges

Agency for Enterprise Information Technology (AEIT) rules[2] provide that agency information owners shall review access rights (privileges) periodically based on risk, access account change activity, and error

[2] AEIT Rule 71A-1.007(2), Florida Administrative Code. Effective July 1, 2014, Chapter 2014-221, Laws of Florida, created the Agency for State Technology (AST) within the Department of Management Services and authorized a type two transfer of all records; property; administrative authority; and administrative rules in Chapters 71A-1 and 71A-2, Florida Administrative Code, of the AEIT to the AST.

rate. Periodic reviews of user access privileges help ensure that only authorized users have access and that the access provided to each user remains appropriate.

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.

Finding 3: Appropriateness of 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 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.

Finding 4: Employee Access Deactivation

AEIT rules[3] provide that access authorization shall be promptly removed when the user's employment is terminated or access to the information resource is no longer required. Prompt action is necessary to ensure that former or transferred employees or others do not misuse the former or transferred employees' access privileges.

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.

Finding 5: Positions of Special Trust

State law[4] requires each agency to designate those positions that, because of the special trust or responsibility or sensitive location, require security background investigations (i.e., background screenings). All persons and employees in such positions must undergo background screening in

[3] AEIT Rule 71A-1.007(6), Florida Administrative Code.

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

accordance with State law[5] using level 2 screening standards, which include fingerprinting, as a condition of employment and continued employment. AEIT rules[6] 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 high as 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.

Finding 6: Access Authorization Documentation

AEIT rules[7] provide that agency information owners shall be responsible for authorizing access to information. 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.

We requested access authorization documentation for nine employees and contractors with update access privileges to FloridaPA.org as of June 29, 2015, to determine whether the access privileges granted to FloridaPA.org were appropriately authorized and documented. The access authorization documentation requested consisted of forms showing supervisory approval and help desk tickets supporting approved access privileges. 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.

[5] Chapter 435, Florida Statutes.

[6] AEIT Rule 71A-1.004(1), Florida Administrative Code.

[7] AEIT Rule 71A-1.007(1), Florida Administrative Code.

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.

Finding 7: 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. AEIT rules[8] require the agency Information Security Manager to implement and maintain the agency information security awareness program and provide that, at a minimum, agency workers are to receive annual 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.

Finding 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*.

[8] AEIT Rule 71A-1.008(1) and (2), Florida Administrative Code.

Finding 9: Security Controls – Protection of Confidential and Exempt Data, User Authentication, Logging and Monitoring, and Other Security Controls

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 protection of confidential and exempt data, user authentication, logging and monitoring, and other security controls 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 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.

Finding 10: NEMIS Upload

Business process controls are the automated and manual controls applied to business transaction flows and relate to the completeness, accuracy, and availability of data during application processing. Completeness controls for the uploading of data provide reasonable assurance that all transactions that occurred are input (uploaded) into the system; that the system accepts valid transactions and rejects invalid transactions; and that rejected transactions are identified, corrected, and reprocessed.

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.

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. 2009-086 and Finding Number 2014-042 noted in our report No. 2015-166.

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 June 2015 through October 2015 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 2014 through June 2015 and selected actions through October 7, 2015. The audit included selected business process application controls over transaction data processing and output and selected application-level general controls applicable to FloridaPA.org that related to the deficiencies disclosed in our report No. 2009-086 and Finding Number 2014-042 noted in our report No. 2015-166. The audit also included selected application-level general controls related to security management. The overall objectives of the audit were:

- To determine the effectiveness of selected IT controls in achieving management's control objectives in the categories 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, deficiencies disclosed in our report No. 2009-086 and Finding Number 2014-042 noted in our report No. 2015-166.
- 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 system 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 system 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 system 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.
- Obtained an understanding of the IT computing platform for FloridaPA.org including identification of the applicable hardware, operating system and version, database management system and version, and security software and version related to FloridaPA.org.
- Obtained an understanding of FloridaPA.org configuration management processes, including identification of policies and procedures for FloridaPA.org change control, as well as patch management controls, and a description of the Division's system development lifecycle methodology.
- Evaluated the effectiveness of selected application security management controls, including security awareness training and protection of confidential and exempt data, and other security-related personnel policies.
- Evaluated the effectiveness of selected FloridaPA.org configuration management controls, including patch management. Specifically, we reviewed four program change requests that were authorized during the period July 1, 2014, through June 30, 2015, to determine whether selected FloridaPA.org program changes were appropriately authorized and documented in accordance with the Division's policies and procedures.
- Evaluated the effectiveness of selected logging and monitoring controls related to FloridaPA.org.
- Evaluated the effectiveness of selected processing and output controls related to FloridaPA.org.
- Obtained an understanding of the procedures for account management processes for authorizing, creating, modifying, and revoking FloridaPA.org accounts.
- Obtained an understanding of the FloridaPA.org periodic review process for access appropriateness.

- Obtained an understanding of the procedures for password management processes for FloridaPA.org that include guidance for password assignments, password changes, password resets, and handling of lost or compromised passwords.
- Evaluated the effectiveness of selected access controls to ensure that the access privileges granted to FloridaPA.org were appropriately authorized and documented. Specifically, we reviewed access authorization documentation for nine employees and contractors with update access privileges to FloridaPA.org as of June 29, 2015, to determine whether access privileges granted to FloridaPA.org were appropriately authorized and documented.
- Evaluated the effectiveness of selected FloridaPA.org access controls related to access privileges, including system administration and security administration functions, and periodic review procedures for access appropriateness. Specifically, we reviewed:
    - The ability to grant FloridaPA.org access privileges for ten employees and eight contractors as of June 29, 2015.
    - The effectiveness of the removal of FloridaPA.org accounts as of August 21, 2015, for eight former or transferred employees.
- Evaluated the effectiveness of selected FloridaPA.org user authentication controls.
- 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

MANAGEMENT'S RESPONSE

STATE OF FLORIDA
DIVISION OF EMERGENCY MANAGEMENT

RICK SCOTT
Governor

BRYAN W. KOON
Director

February 22, 2016

Ms. Sherrill F. Norman
Claude Pepper Building, Suite G74
111 West Madison Street
Tallahassee Florida 32399-2100

Dear Ms. Norman:

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

If you have any questions or need additional assistance, please contact Ronnie Atkins, Deputy Inspector General at (850) 922-1611 or ronnie.atkins@em.myflorida.com.

Sincerely,

Bryan W. Koon, Director

BWK/ra

Enclosure

C: Ronnie Atkins, Deputy Inspector General

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

Tel: 850-413-9969 • Fax: 850-488-1016
www.FloridaDisaster.org

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

FINDINGS AND RECOMMENDATIONS

Finding 1: IT Policies and Procedures

Finding 1: The Division had not established written policies or procedures related to FloridaPA.org configuration management and FloridaPA.org access security administration to ensure that FloridaPA.org program changes or data change requests were properly communicated to the Division's software contractor and reviewed by Division staff once implemented by the software contractor and that user access privileges granted to individuals were authorized by management, appropriate for the accomplishment of assigned job duties, and commensurate with management's direction. A similar finding related to FloridaPA.org access security administration procedures was noted in previous audits of the Division, most recently in 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.

State Agency Response and Corrective Action Plan: We concur 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.

Estimated Corrective Action Date: August 15, 2016

Agency Contact and Telephone Number: Kevin Smith (850) 922-2289 and Evan Rosenberg (850) 528-7526

Finding 2: Periodic Reviews of User Access Privileges

Finding 2: The Division had not performed periodic reviews of FloridaPA.org nonapplicant user access privileges to ensure that the access privileges assigned were authorized and appropriate. 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.

State Agency Response and Corrective Action Plan: We concur 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.

Estimated Corrective Action Date: August 15, 2016

Agency Contact and Telephone Number: Kevin Smith (850) 922-2289 and Evan Rosenberg (850) 528-7526

Finding 3: Appropriateness of Access Privileges

Finding 3: The access privileges for some Division employees and contractors and FloridaPA.org user groups did not promote an appropriate separation of duties and did not restrict users to only those functions appropriate and necessary for their assigned job duties, thus increasing 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.

State Agency Response and Corrective Action Plan: We concur with the recommendation. 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.

Estimated Corrective Action Date: August 15, 2016

Agency Contact and Telephone Number: Kevin Smith (850) 922-2289 and Evan Rosenberg (850) 528-7526

Finding 4: Employee Access Deactivation

Finding 4: As similarly noted in our report No. 2009-086, the Division did not timely deactivate the FloridaPA.org accounts for some former and transferred employees, thus increasing the risk that the FloridaPA.org accounts may be misused by the former or transferred employees or others.

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

State Agency Response and Corrective Action Plan: We concur 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.

Estimated Corrective Action Date: August 15, 2016

Agency Contact and Telephone Number: Kevin Smith (850) 922-2289 and Evan Rosenberg (850) 528-7526

Finding 5: Positions of Special Trust

Finding 5: The Division had not established procedures for the performance of background screenings of newly hired employees in positions of special trust or periodic background screenings of current employees in positions of special trust and also had not designated IT positions that have system, database, developer, network, or other administrative capabilities related to FloridaPA.org as positions of special trust to reduce the risk 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.

State Agency Response and Corrective Action Plan: We concur with the recommendation. 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.

Estimated Corrective Action Date: August 15, 2016

Agency Contact and Telephone Number: Kevin Smith (850) 922-2289 and Evan Rosenberg (850) 528-7526

Finding 6: Access Authorization Documentation

Finding 6: As similarly noted in our report No. 2009-086 and Finding Number 2014-042 noted in our report No. 2015-166, access authorization documentation for some employees and contractors with access to FloridaPA.org was missing, incomplete, or inaccurate, thus limiting management's assurances that access privileges were authorized and appropriately assigned.

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

State Agency Response and Corrective Action Plan: We concur with the recommendation. 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.

Estimated Corrective Action Date: August 15, 2016

Agency Contact and Telephone Number: Kevin Smith (850) 922-2289 and Evan Rosenberg (850) 528-7526

Finding 7: Security Awareness Training

Finding 7: 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 and the handling of sensitive and confidential information. A similar finding was noted in prior audits of the Division, most recently in 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.

State Agency Response and Corrective Action Plan: We concur with the recommendation. 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.

Estimated Corrective Action Date: August 15, 2016

Agency Contact and Telephone Number: Kevin Smith (850) 922-2289

Finding 8: Retention of Access Control Records

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 employee access privileges, thus increasing the risk 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*.

State Agency Response and Corrective Action Plan: We concur with the recommendation. 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*.

Estimated Corrective Action Date: August 15, 2016

Agency Contact and Telephone Number: Kevin Smith (850) 922-2289 and Evan Rosenberg (850) 528-7526

Finding 9: Security Controls - Protection of Confidential and Exempt Data, User Authentication, Logging and Monitoring, and Other Security Controls

Finding 9: Certain security controls related to protection of confidential and exempt data, user authentication, logging and monitoring, and other security controls for FloridaPA.org and related IT resources continue to need improvement to ensure the continued confidentiality, integrity, and availability of FloridaPA.org data and related IT resources.

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.

State Agency Response and Corrective Action Plan: We concur with the recommendation. 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.

Estimated Corrective Action Date: August 15, 2016

Agency Contact and Telephone Number: Kevin Smith (850) 922-2289

Finding 10: NEMIS Upload

Finding 10: 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 the National Emergency Management Information System (NEMIS) to promote the completeness and accuracy of FloridaPA.org payment approvals and payment amounts. 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.

State Agency Response and Corrective Action Plan: We concur 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.

Estimated Corrective Action Date: August 15, 2016

Agency Contact and Telephone Number: Kevin Smith (850) 922-2289 and Evan Rosenberg (850) 528-7526