2009-086

STATE OF FLORIDA

DEPARTMENT OF COMMUNITY AFFAIRS

"Dedicated to making Florida a better place to call home"

CHARLIE CRIST
Governor

THOMAS G. PELHAM
Secretary

MEMORANDUM

TO: Thomas G. Pelham, Secretary

FROM: Candie M. Fuller, Inspector General

SUBJECT: Audit Follow-up

DATE: July 29, 2009

In accordance with Section 20.055 (5) (g), Florida Statutes, a report of the most recent audit relating to Department of Community Affairs and Division of Emergency Management issued by the Florida Auditor General is attached. The report includes a brief summary of the audit findings, recommendations, and agency response, with status of corrective actions at this time.

Please let me know if you would like additional information regarding this follow-up report.

Attachment

cc: Joint Legislative Auditing Committee

JLAC
Rec'd 8/4/2009

2555 SHUMARD OAK BOULEVARD ♦ TALLAHASSEE, FL 32399-2100
850-488-8466 (p) ♦ 850-921-0781 (f) ♦ Website: www.dca.state.fl.us

♦ COMMUNITY PLANNING 850-488-2356 (p) 850-488-3309 (f) ♦ FLORIDA COMMUNITIES TRUST 850-922-2207 (p) 850-921-1747 (f) ♦
♦ HOUSING AND COMMUNITY DEVELOPMENT 850-488-7956 (p) 850-922-5623 (f) ♦

FOLLOW-UP OF AUDIT REPORTS ISSUED BY THE AUDITOR GENERAL OR OPPAGA				
AUDITING ENTITY	REPORT NUMBER	PERIOD COVERED	SUMMARY OF FINDINGS AND RECOMMENDATIONS	SUMMARY OF CORRECTIVE ACTIONS TAKEN
Auditor General	2009-086	May 2008 – July 2008	**Finding No.1:** Department and Division security policies and procedures had not been fully developed or approved and were not sufficiently comprehensive. **Recommendation:** The Department and Division should work together to fully develop, officially approve, and implement, as applicable, current and appropriate policies, procedures, and controls, including access authorization and removal and incident monitoring and response, designation of positions of special trust, and associated background checks. Additionally, the Department and Division should promote ongoing security awareness to ensure that all employees are aware of the importance of information handled and their responsibilities for maintaining its confidentiality, integrity, and availability.	**Department response:** The Department has approved a comprehensive Information Security Policy. Information Security awareness training was conducted May/June 2009. Follow-up security training will be offered Nov/Dec. 2009. Positions of special trust have been identified and request for background checks are currently being conducted. It is anticipated these should be completed by August 30, 2009. **Division response:** DCA has a appointed a Department Security Manager and has implemented a comprehensive security policy and procedure and additionally has sponsored department wide security awareness training.
			Finding No.2: Neither the Department nor the Division had an Information Systems Development Methodology (ISDM) to govern the	**Department response:** The Department has an Information System Development Methodology (ISDM) document. The

			development, maintenance, operation, and disposition of systems. In addition, existing change management practices needed improvement. **Recommendation:** The Department and Division should establish an ISDM to govern the management of application systems and supporting IT infrastructure. As a part of the effort, the Department and Division should implement a configuration management process that documents changes to the information system and network, including current software patches.	Department has implemented a change management process for network configuration changes to include server patch management. **Division response:** DCA does have an ISDM document, and has also instituted configuration management that governs system information and current software patches. DCA still needs to investigate change management at the application level and should have procedures in place by the end of this calendar year.
			Finding No.3: The Division's management of FloridaPA System access privileges needed improvement. **Recommendation:** The Division should develop application security documentation, including policies and procedures for granting access, and maintain access request forms that document the access privileges requested, approved, and granted. The Division should also periodically review access privileges, monitor access activity, and investigate access violations. In addition, the Division	**Division response:** DEM now has in place a system where any new non-applicant user requesting access must first go through an approval process to gain access (with appropriate documentation and logging of access privileges granted). FloridaPA.org has also been upgraded so as to allow the creation of user groups (13 different group levels have been created to date), with assigned access privileges to the individual applicant determined by which group that individual is a member of (groups are used to limit access privileges and are based on needs and potential security threats posed by members of the group). A Planning Manager at the FRO has approval authority over new non-applicant users who request

			should ensure that access privileges of former employees are timely removed, restrict system administrator functions to staff responsible for controlling system access, assign employee access privileges at the individual level, and restrict user access to the payment approval process to allow for an appropriate separation of duties. Furthermore, the Division should pursue correcting the FloridaPA software so that the access levels correctly correspond to employee job responsibilities.	access. Additionally, in support of an immediate order (on the employee's separation date) to suspend the access privileges of former employees, DEM now utilizes quarterly audits of non-applicant users to ensure that access privileges of former employees have been removed.
			Finding No.4: Certain Division security controls protecting the FloridaPA System date and IT resources needed improvement. **Recommendation:** The Division should improve appropriate security controls to ensure the continued confidentiality, integrity, and availability of Division data and IT resources.	**Division response:** Security control improvements to date have focused on the access issue noted above, and corrective actions taken are likewise listed above under Finding 3.
			Finding No.5: The Division did not maintain a complete log of user activity in the FloridaPA System. **Recommendation:** The Division should establish sufficient transaction	**Division response:** FloridaPA.org now allows administrators and applicants to monitor the specifics of data changes (what was changed, when it was changed & who performed the change) on the applicant's summary

			history logging and reporting capabilities in the FloridaPA System to provide a complete record of changes to data, including the person who made the change and the data that was changed.	page under the "history" Tab.
			Finding No.6: The Division had not developed FloridaPA System nonapplicant user documentation. **Recommendation:** The Division should create and maintain user manuals for nonapplicant users and establish periodic review process to ensure that the user manuals are updated as appropriate to reflect relevant system modifications.	**Division response:** DEM has made a state user guide available upon logging into the FloridaPA.org system. This user guide may be downloaded in its entirety, or may be accessed through a new window in the user's current web-browser session.
			Finding No.7: The Division did not timely address processing errors occurring during the data upload process between the National Emergency Management Information System (NEMIS) and the FloridaPA System. **Recommendation:** The Division should monitor the daily upload process between NEMIS and FloridaPA and investigate and correct as necessary all processing errors in a timely manner.	**Division response:** FloridaPA.org has been upgraded to provide an alert to data fields that did not migrate over from NEMIS during the most recent daily data synchronization. Any such alerts are automatically written into an Excel file which allows the administrator to more easily diagnose the problem. Currently, this report is checked daily by the Office Automation Analyst at the Lake Mary FRO.