REPORT NO. 2009-086
JANUARY 2009

DEPARTMENT OF COMMUNITY AFFAIRS

DIVISION OF EMERGENCY MANAGEMENT
FLORIDA PUBLIC ASSISTANCE SYSTEM

Information Technology Operational Audit

May 2008 Through July 2008
and Selected Actions Through September 2008

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

SECRETARY OF THE DEPARTMENT OF COMMUNITY AFFAIRS

Pursuant to Section 20.18(1), Florida Statutes, the Secretary of the Department of Community Affairs is appointed by the Governor, subject to confirmation by the Senate. Thomas G. Pelham served as Secretary during the audit period.

DIRECTOR OF THE DIVISION OF EMERGENCY MANAGEMENT

Pursuant to Section 20.18(2)(a), Florida Statutes, the Division of Emergency Management is a separate budget entity and is not subject to control, supervision, or direction by the Department of Community Affairs in any manner. The Director of the Division is appointed by the Governor and is the agency head of the Division for all purposes. W. Craig Fugate served as Director during the audit period.

The audit team leader was William Tuck, CISA, and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, by e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other audit reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 487-9024; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF COMMUNITY AFFAIRS

Division of Emergency Management
Florida Public Assistance System

SUMMARY

The Florida Public Assistance (FloridaPA) System is a Web-based portal used by the Division of Emergency Management (Division) to manage public assistance relating to disaster relief and recovery. The Department of Community Affairs (Department) provides information technology (IT) infrastructure and support services, including server and network support, for the FloridaPA System.

Our audit focused on evaluating the effectiveness of selected IT controls applicable to the FloridaPA System for the period May 2008 through July 2008 and selected actions through September 2008. The results of our audit are summarized below:

Finding No. 1: Department and Division security policies and procedures had not been fully developed or approved and were not sufficiently comprehensive.

Finding No. 2: Neither the Department nor the Division had an Information Systems Development Methodology (ISDM) to govern the development, maintenance, operation, and disposition of systems. In addition, existing change management practices needed improvement.

Finding No. 3: The Division's management of FloridaPA System access privileges needed improvement.

Finding No. 4: Certain Division security controls protecting the FloridaPA System data and IT resources needed improvement.

Finding No. 5: The Division did not maintain a complete log of user activity in the FloridaPA System.

Finding No. 6: The Division had not developed FloridaPA System nonapplicant user documentation.

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.

BACKGROUND

Effective July 1, 2006, Chapter 2006-70, Laws of Florida, established the Division as a unit of the Department that is a separate budget entity and not subject to control, supervision, or direction by the Department in any manner. The Division is responsible for maintaining a comprehensive Statewide program of emergency management and provides programs and services to assist communities in preparing for and responding to natural and man-made disasters. The Division was required by law to enter into a service agreement with the Department for professional, technological, and administrative support services. Such service agreement was created and signed by the Department Secretary and the Division Director on August 7, 2006.

The Department's Information Systems and Services (ISS) section provides technical infrastructure support to the Division, including the Department server and network connections used by the FloridaPA System. The FloridaPA System is managed by the Division's Bureau of Recovery and Mitigation, Florida Recovery Office. The Division uses a contractor to provide application support services for the FloridaPA System and ISS is not responsible for FloridaPA System application software changes or granting user access privileges.

The FloridaPA System centralizes public assistance information by connecting applicants, State emergency management, and the Federal Emergency Management Agency and supports the following public assistance project management functions:

- Request for Public Assistance Submission and Approval
- Project Access
- Project Request Management
- Advanced Reimbursement Processing
- Detailed Financial Reports
- Quarterly Report Management

In addition, the FloridaPA System receives daily downloads of data from NEMIS, including Federal approval of public assistance payments.

The FloridaPA System was scheduled for an upgrade, including patches and enhancements, to be completed in early 2008. However, actual implementation of the upgrade occurred in September 2008.

FINDINGS AND RECOMMENDATIONS

As discussed in the following findings and recommendations, our audit disclosed that IT controls and practices applicable to the FloridaPA System needed improvement. The Division, being a separate entity established by law, is responsible and accountable for managing its IT resources, including, in particular, the FloridaPA System. However, some of the needed improvements will require the involvement of the Department as well and might be best addressed through enhancements to the Division's service level agreement with the Department.

Finding No. 1: Security Policies and Procedures

Effective security planning and management includes the establishment of written security policies and procedures to document management's expectations for addressing security risks. Security policies and procedures help to establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective controls, and monitoring the effectiveness of controls.

Our audit disclosed that Department and Division IT security policies and procedures applicable to the FloridaPA System needed improvement. Additionally, certain aspects of IT security were deficient, suggesting a need for more comprehensive IT security policies and procedures. Specifically:

- The Division had not established written IT security policies and procedures. Without written policies and procedures, the risk is increased that IT security controls may not be followed consistently and in a manner pursuant to management's expectations.
- As similarly noted in audit report No. 2006-134, the Department's IT security policies and procedures were not sufficiently comprehensive or fully approved. Department management had begun developing Departmentwide policies and procedures that included specific IT security elements and had created a list of identified Department policies and procedures that were to be revised, the unit responsible for the revisions, and a due date for completion. Also, the Department had not fully developed or approved specific policies and procedures addressing access authorization and removal and incident monitoring and response. Without current, officially approved, and comprehensive security policies and procedures, the risk is increased that controls may be inconsistently applied and responsibilities may be unclear, misunderstood, and improperly implemented.

- The Department, as similarly noted in audit report No. 2006-134, had not designated key IT employees with high access levels, including security administrators, programmers, and database administrators, as occupying positions of special trust and had not ensured that appropriate background checks of the employees, including fingerprinting, had been performed, pursuant to Sections 110.1127(1) and 435.04(1), Florida Statutes. Specifically, Section 435.04(1), Florida Statutes, provides that all employees in positions designated by law as positions of trust or responsibility shall be required to undergo security background investigations referred to as level 2 background screenings as a condition of employment and continued employment. The level 2 background screenings are to include fingerprinting for all purposes, Statewide criminal and juvenile records checks through the Department of Law Enforcement, and Federal criminal records checks through the Federal Bureau of Investigation. The sensitive responsibilities and high access levels of the key IT employees suggested a need to designate their positions as positions of special trust. In addition, the Department had not established written procedures describing the measures necessary for the oversight of these positions. By not designating positions of special trust for positions with high access levels or documenting detailed review procedures of the actions taken by the employees occupying those positions, the risk is increased that an individual with an inappropriate background could be employed in one of the positions and that inappropriate system actions taken by the employee, should they occur, may not be timely detected.

- Neither the Department, as similarly noted in audit report No. 2006-134, nor the Division had developed a comprehensive ongoing security awareness training program. New employees received some security awareness training during orientation and the Department displayed informational fliers regarding security; however, the Department had no ongoing security awareness training program to facilitate employees' education and training on security responsibilities, including data classification and acceptable or prohibited methods for storage and transmission, password protection and usage, copyright issues, malicious software and virus threats, remote access issues, Blackberries, laptops, workstation controls, and handling of confidential information. The purpose of a security awareness training program is to periodically remind employees of the importance of the information handled and the legal and business reasons for maintaining its integrity, confidentiality, and availability. Part of the awareness training is to provide employees with documentation describing security policies, procedures, and individual responsibilities. The lack of an ongoing security awareness training program may limit management's assurance that employees understand the importance of IT security and are sufficiently prepared to safeguard data and IT resources.

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.

Finding No. 2: Information Systems Development Methodology

Effective IT life cycle practices include, among other things, the establishment of an ISDM to govern system development and changes, including outlining procedures, practices, and guidelines governing the initiation, needs assessment or feasibility, planning, requirements analysis, design, acquisition development, integration, testing and acceptance, implementation, operations and maintenance, and disposition of information technology. Configuration management, an integral component of a comprehensive ISDM, assists in streamlining change management processes and prevents changes that could detrimentally affect the security posture of a system. In its entirety, the configuration management process reduces the risk that any changes made to a system result in a compromise to system or data confidentiality, integrity, or availability by providing a repeatable mechanism for effecting system modifications in a controlled environment.

Neither the Department nor the Division had developed or documented an ISDM to govern system development and changes and no ISDM governed the development of the FloridaPA System. The Department and Division did not use change management software or appropriately document configuration changes to the information system or network supporting the FloridaPA System. No procedures existed for configuration management and the Department's patch management software was not a current version. Outdated patch management was reported as an issue in a consultant's risk assessment document, dated September 2005, and was confirmed by the Department's Chief Information Officer (CIO) as continuing to be an issue as of June 30, 2008. Subsequent to audit inquiry, the Department's CIO indicated that the patch management software is now a current version and that all software patches have been installed. Under these conditions, the risk is increased that the Department and Division could overlook crucial design elements needed in a system that could result in project failure or adversely affect project management and allow vulnerabilities to remain within the FloridaPA System or its infrastructure that could be exploited and result in loss of system availability or data integrity.

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.

Finding No. 3: Security Controls – Management of Access Privileges

Effective security controls include access controls that are intended to ensure that users have only the access privileges needed to perform their duties, that access to sensitive resources is limited to only a few users, and that users are restricted from performing incompatible functions. Access controls include the use of individual user identifications (IDs) and passwords to allow for attributing user activities to the responsible user. The risk of inappropriate or unnecessary access privileges can be reduced through the employment of such controls as documenting authorizations for system access, periodically reviewing the appropriateness of access privileges, promptly removing the access privileges of former employees, and establishing individual user IDs and passwords.

Our audit disclosed aspects of the Division's management of FloridaPA System access privileges that needed improvement. Specifically:

- Division IT support staff were responsible for establishing access privileges to the FloridaPA System; however, no system access security documentation or policies and procedures existed to guide staff. Additionally, Division IT support staff had limited understanding of the various access levels and the access privileges that each level provided. Without guidance in the form of system access documentation and written access control policies and procedures, the risk is increased that inappropriate access privileges will be granted, as further demonstrated by the instances of excessive access privileges discussed below.
- Documentation of requests for FloridaPA System access privileges needed improvement. Requests for access were typically established when a new employee's computer and e-mail account were set up. If access was requested at a later date, it was normally requested through a telephone call or e-mail request. No supervisory approvals were required before access privileges were granted and no documentation was retained of the access privileges that were requested, approved, or granted. The absence of documentation of user access requests may limit management's ability to ensure that only approved access privileges have been granted.
- FloridaPA System access privileges were not periodically reviewed to ensure that access granted was appropriate and necessary. In addition, no one was responsible for monitoring access violations and investigating suspicious activity. Under these conditions, the risk is increased that inappropriate access capabilities and system actions may not be timely detected.
- The Division did not always timely remove FloridaPA System access privileges of former employees. Upon audit request, Department staff provided listings of former employees who terminated employment during the period July 2007 through May 2008. Our comparison of the listings to users with active access privileges in the

FloridaPA System disclosed that two former Division salaried employees still had access privileges as of June 23, 2008, 67 and 83 days after termination. In addition, one of the accesses was recorded as last used 55 days after the termination date. In response to audit inquiry, Division management indicated that they would remove the access privileges of the two employees. Our comparison of a listing of former Division Other Personal Services (OPS) employees who terminated employment during the period July 2007 through May 2008 to users with active access privileges to the FloridaPA System disclosed that four former Division OPS employees still had access privileges as of August 15, 2008. According to Division staff, the access privileges of one of the four former OPS employees had been used to access the FloridaPA System 334 days after the employee's termination date. Without timely removal of former employees' access privileges, the risk is increased that the access privileges may be misused by the former employee or others.

- Access to the FloridaPA System administrator function capabilities was not properly restricted by the system or in formal policy. Our audit disclosed that users with access levels of Administrator or State had the ability to add new applicant user IDs. The Division had established an unwritten policy of requiring all requests for new applicant user IDs be forwarded to Division IT Support to be set up. However, Administrator and State access capabilities were not changed to reflect the policy change. As of June 23, 2008, 78 employees had the ability to add new applicant user IDs, although these employees were not part of Division IT Support and their job responsibilities did not include granting access to new users. Additionally, three consultants who originally developed the FloridaPA System had access privileges that allowed them to add FloridaPA System user IDs. The consultants worked on an as-needed basis and did not require daily access. Our audit disclosed that one of the three consultants terminated employment with the vendor in December 2007, but the consultant's FloridaPA System access privileges remained active. Absent access controls that restrict administrator functions to appropriate staff, the risk is increased that unauthorized users may gain access to the FloridaPA System.

- Two generic nonapplicant user IDs existed, one of which had administrator-level access. Nonapplicant user access privileges are established for system users other than those persons applying for public assistance. Because of a lack of auditee logging and monitoring reports, the Division could not determine if the generic user IDs had been used. Furthermore, the use of generic IDs does not allow for attributing responsibility for user activities to a specific person.

- Eight user IDs had administrator-level access that was not appropriate based on job responsibilities. Three of the eight user IDs were assigned to contractors who did not require access on a daily basis. Of the remaining five, one user ID was the generic user ID described above and the remaining four user IDs belonged to former employees but the associated access privileges had not been removed. Under these conditions, the risk is increased that the access privileges could be misused to initiate erroneous or unauthorized transactions in the FloridaPA System.

- Access roles were assigned to 51 nonapplicant users that allowed them to approve an applicant request for payment at multiple processing levels, circumventing an appropriate separation of duties. Payment processing normally requires the approval of employees filling four different roles in the process. Under these conditions, the risk is increased that erroneous or unauthorized transactions could be initiated and approved by the same person.

- Because of an access-level software problem in the FloridaPA System, 161 nonapplicant users with an assigned access level of read-only also had the ability to update data, including contact logs and applicant profile information within the FloridaPA System. The unintentionally granted update capabilities increased the risk of erroneous or unauthorized changes to FloridaPA System information.

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 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.

Finding No. 4: Security Controls – User Authentication

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain Division security controls related to the FloridaPA System that needed improvement, in the area of user authentication. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the Division's data and IT resources. However, we have notified appropriate Division management of the specific issues. Without adequate security controls, the confidentiality, integrity, and availability of data and IT resources may be compromised, increasing the risk that Division data and IT resources may be subject to improper disclosure, modification, or destruction.

Recommendation: The Division should improve appropriate security controls to ensure the continued confidentiality, integrity, and availability of Division data and IT resources.

Finding No. 5: Transaction History Logging

Output controls help ensure, among other things, that a complete and accurate record of data processing is captured. Transaction history logs are a key output control that enables the tracking of transaction processing from transaction origin to inclusion in the entity's records.

Our audit disclosed that transaction history logging within the FloridaPA System was limited. Specifically, FloridaPA online screens logged accesses by nonapplicant user IDs by capturing the user name of the person who last accessed the screen and the date and time of the last access. However, the FloridaPA System did not record the last changes made to the data or provide a history of previous user accesses or data changes. The lack of a complete log of changes to critical data fields or records increases the risk that unauthorized or erroneous data changes, should they occur, may not be detected and corrected in a timely manner.

Additionally, the FloridaPA System maintained applicant contact logs that recorded the date and time of contacts between Division grant staff and applicants regarding a public assistance project. However, the system-generated date and time stamps could be modified by a nonapplicant user, including those with read-only access, jeopardizing the reliability of the contact logs.

Recommendation: The Division should establish sufficient transaction 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.

Finding No. 6: Nonapplicant User Documentation

Adequate system documentation allows for the transfer of knowledge and skills to new employees, thus promoting the effective and efficient use of the system to timely support business processes. Our audit disclosed that no user manual existed for the FloridaPA System nonapplicant users. In response to audit inquiry, Division staff indicated that the FloridaPA System was developed in a very short time frame due to the immediate needs of the 2004 hurricane season and, as a result, nonapplicant user documentation was not developed. The lack of current user documentation increases the risk of users not performing their job functions efficiently and timely, critical dependency on key individuals, and ineffective system knowledge transfer.

Recommendation: The Division should create and maintain user manuals for nonapplicant users and establish a periodic review process to ensure that the user manuals are updated as appropriate to reflect relevant system modifications.

Finding No. 7: NEMIS Upload

Proper upload procedures ensure that the system output reports are reviewed for accuracy and for identification and handling of errors contained in the output. Federal public assistance program data from NEMIS, including payment approvals and approved payment amounts, was uploaded to the FloridaPA System on a daily basis, Monday through Friday. A confirmation number was produced each time the upload was executed.

All errors encountered during the upload were appended to a daily report that could be viewed online in the FloridaPA System. Although errors were appended to the report daily, Division IT support staff did not review the error report and correct the errors. Division IT support staff instead relied on the grant accountants or State public assistance coordinators within the Division to notify them that a particular public assistance project was not updated. Upon notification of the errors, Division IT support staff then investigated the errors and made necessary corrections to the data. Additionally, errors that appeared on the error report were not dated, so there was no means for staff to determine when the errors occurred. In these circumstances, the risk is increased that inaccurate or incomplete FloridaPA System data may not be timely detected and corrected.

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.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for findings included in our report No. 2006-134 that were applicable to the scope of this audit.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to determine the effectiveness of selected general and application controls relating to the FloridaPA System 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; the safeguarding of IT resources, and to determine whether management has corrected, or was in the process of correcting, selected prior audit findings disclosed in audit report No. 2006-134.

The scope of our audit focused on evaluating selected IT controls applicable to the Department of Community Affairs and Division of Emergency Management related to the FloridaPA System during the period May 2008 through July 2008 and selected actions through September 2008.

In conducting our audit, we:

- Interviewed Department and Division personnel.
- Obtained an understanding of Department systems software and database controls.
- Obtained an understanding of Division application and user controls applicable to the FloridaPA System.
- Observed, documented, and tested key processes and procedures related to Department systems software and database controls.

- Observed, documented, and tested key processes and procedures related to Division application and user controls.
- Evaluated Department systems software and database controls, Division policies and procedures related to application and user controls, and techniques to safeguard the confidentiality, integrity, availability, relevance, and reliability of data.

We conducted this IT audit in accordance with applicable 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 our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

AUTHORITY

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.

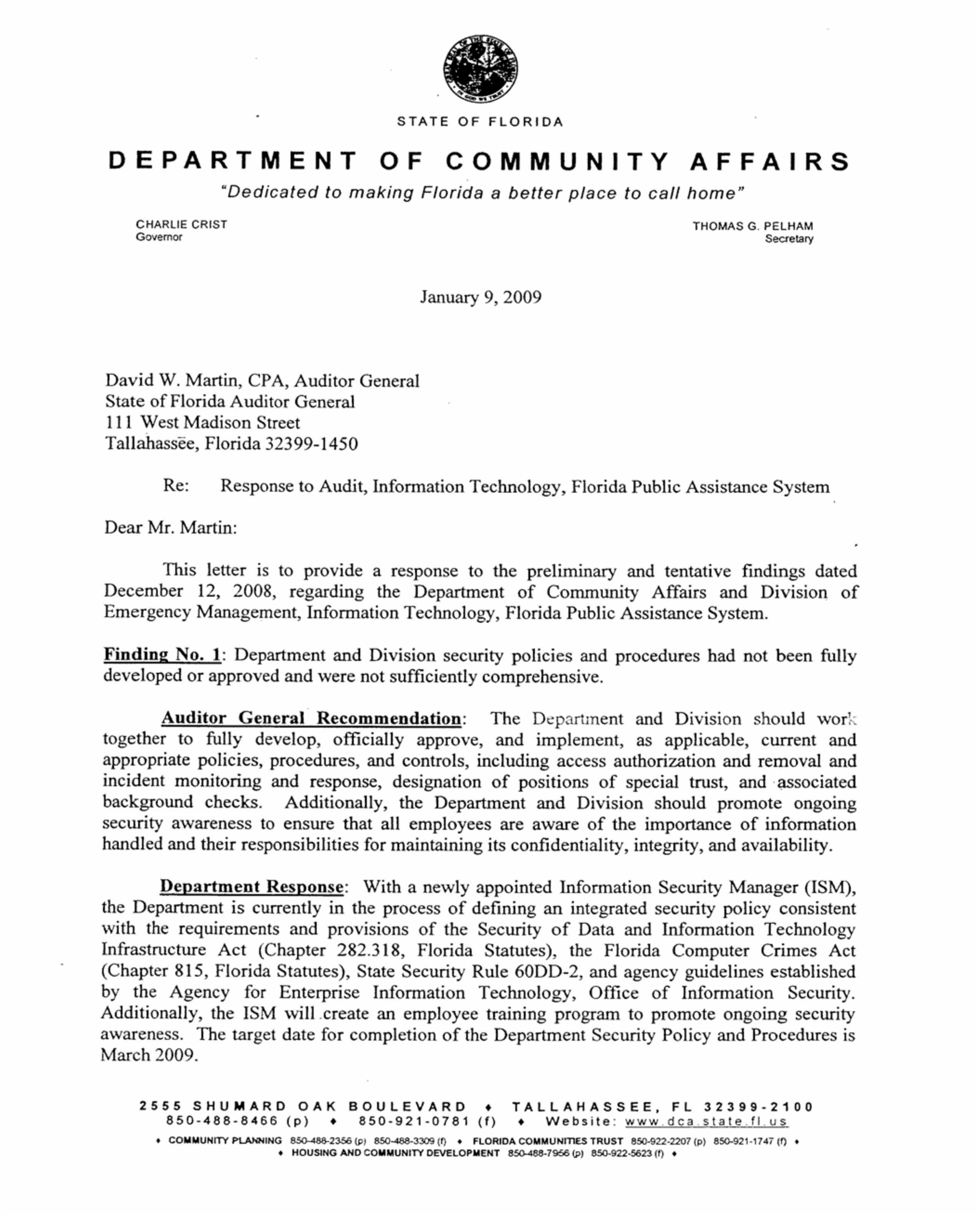
David W. Martin

David W. Martin, CPA
Auditor General

MANAGEMENTS' RESPONSES

In letters dated January 9, 2009, the Secretary of the Department and the Director of the Division provided responses to our preliminary and tentative findings. The letters are included at the end of this report as Exhibit A.

EXHIBIT A
MANAGEMENTS' RESPONSES



STATE OF FLORIDA

DEPARTMENT OF COMMUNITY AFFAIRS

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

CHARLIE CRIST
Governor

THOMAS G. PELHAM
Secretary

January 9, 2009

David W. Martin, CPA, Auditor General
State of Florida Auditor General
111 West Madison Street
Tallahassee, Florida 32399-1450

Re: Response to Audit, Information Technology, Florida Public Assistance System

Dear Mr. Martin:

This letter is to provide a response to the preliminary and tentative findings dated December 12, 2008, regarding the Department of Community Affairs and Division of Emergency Management, Information Technology, Florida Public Assistance System.

Finding No. 1: Department and Division security policies and procedures had not been fully developed or approved and were not sufficiently comprehensive.

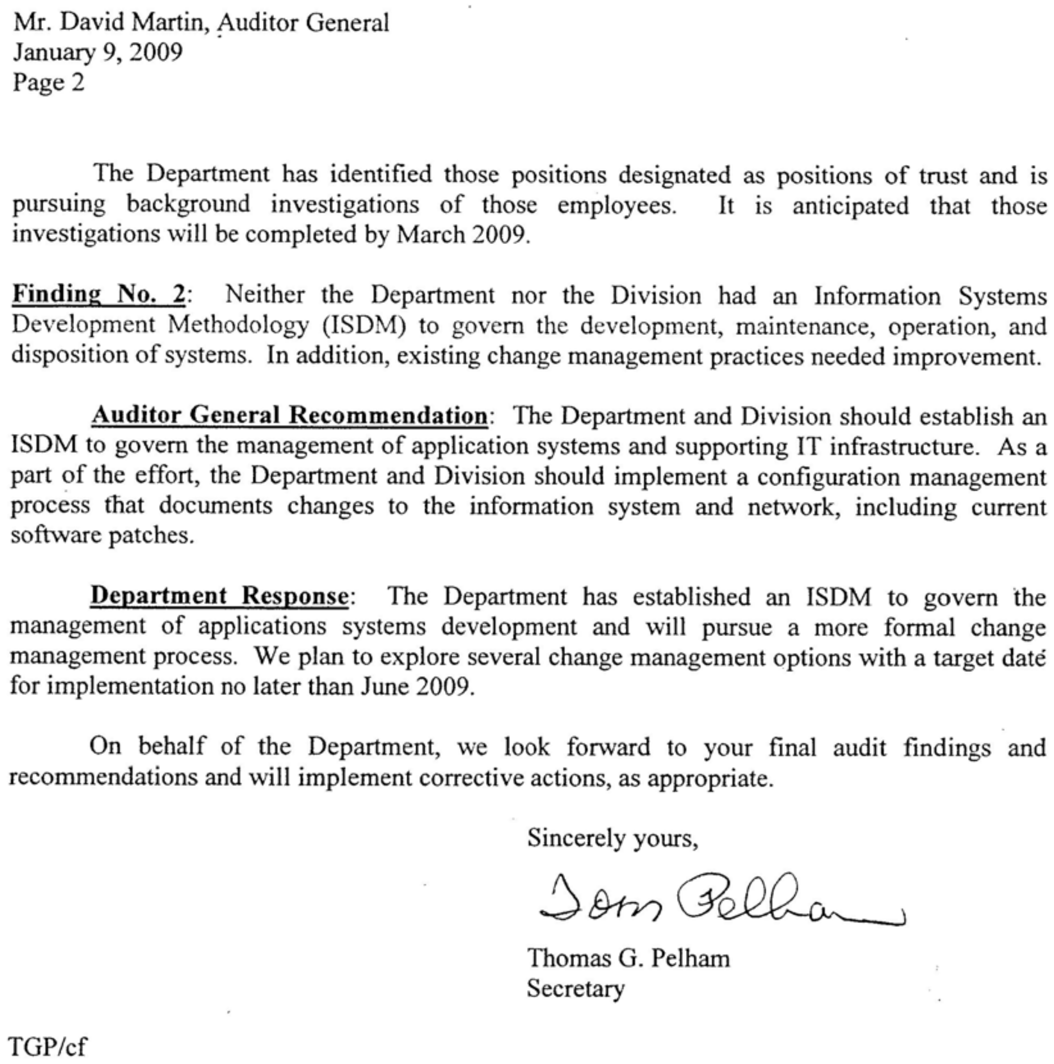
Auditor General Recommendation: The Department and Division should work together to fully develop, officially approve, and implement, as applicable, current and appropriate policies, procedures, and controls, including access authorization and removal and incident monitoring and response, designation 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: With a newly appointed Information Security Manager (ISM), the Department is currently in the process of defining an integrated security policy consistent with the requirements and provisions of the Security of Data and Information Technology Infrastructure Act (Chapter 282.318, Florida Statutes), the Florida Computer Crimes Act (Chapter 815, Florida Statutes), State Security Rule 60DD-2, and agency guidelines established by the Agency for Enterprise Information Technology, Office of Information Security. Additionally, the ISM will create an employee training program to promote ongoing security awareness. The target date for completion of the Department Security Policy and Procedures is March 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) ♦

EXHIBIT A (CONTINUED)
MANAGEMENTS' RESPONSES



Mr. David Martin, Auditor General
January 9, 2009
Page 2

The Department has identified those positions designated as positions of trust and is pursuing background investigations of those employees. It is anticipated that those investigations will be completed by March 2009.

Finding No. 2: Neither the Department nor the Division had an Information Systems Development Methodology (ISDM) to govern the development, maintenance, operation, and disposition of systems. In addition, existing change management practices needed improvement.

Auditor General 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 Response: The Department has established an ISDM to govern the management of applications systems development and will pursue a more formal change management process. We plan to explore several change management options with a target date for implementation no later than June 2009.

On behalf of the Department, we look forward to your final audit findings and recommendations and will implement corrective actions, as appropriate.

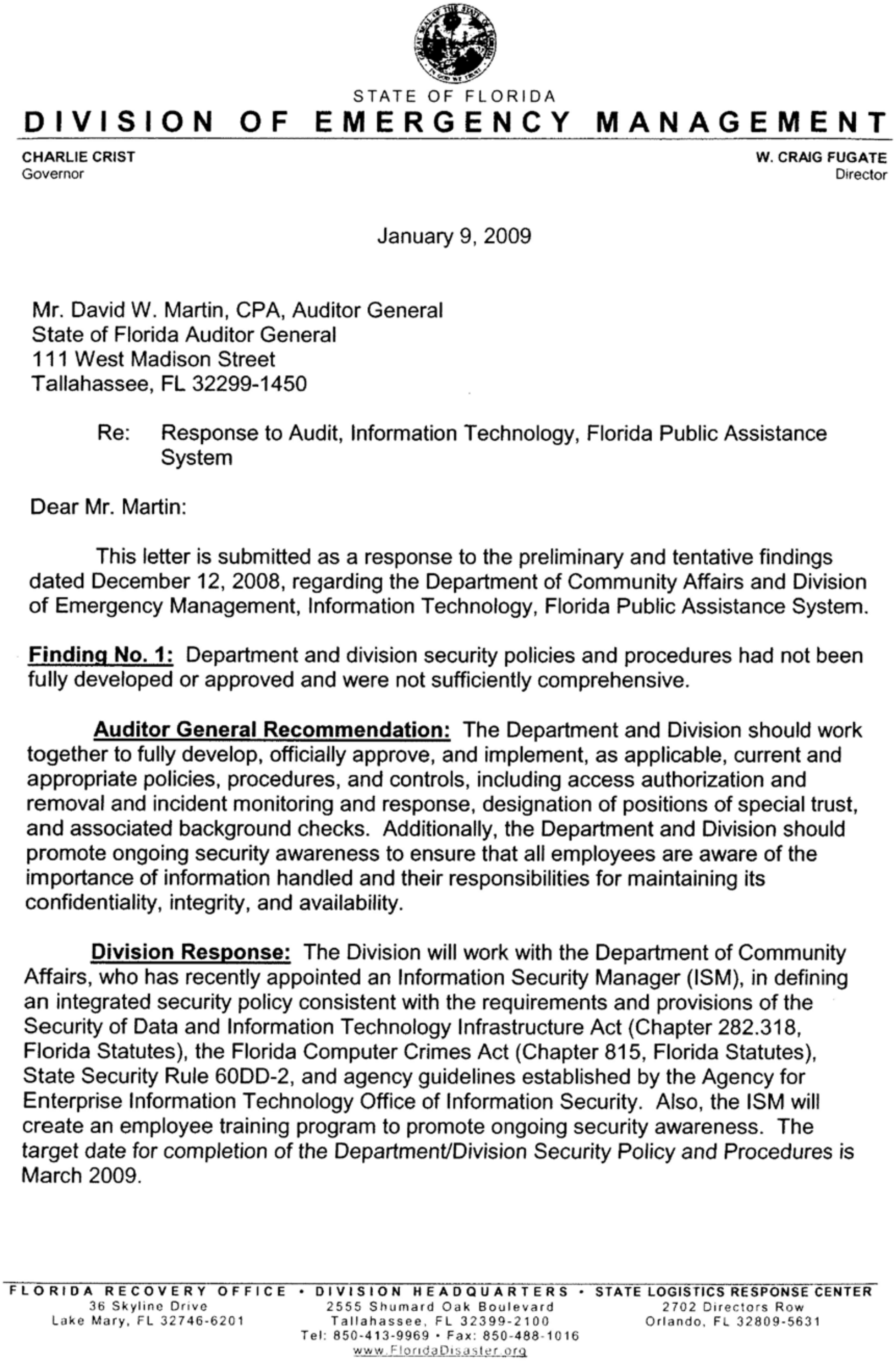
Sincerely yours,

Tom Pelham

Thomas G. Pelham
Secretary

TGP/cf

EXHIBIT A (CONTINUED)
MANAGEMENTS' RESPONSES



STATE OF FLORIDA
DIVISION OF EMERGENCY MANAGEMENT

CHARLIE CRIST
Governor

W. CRAIG FUGATE
Director

January 9, 2009

Mr. David W. Martin, CPA, Auditor General
State of Florida Auditor General
111 West Madison Street
Tallahassee, FL 32299-1450

Re: Response to Audit, Information Technology, Florida Public Assistance System

Dear Mr. Martin:

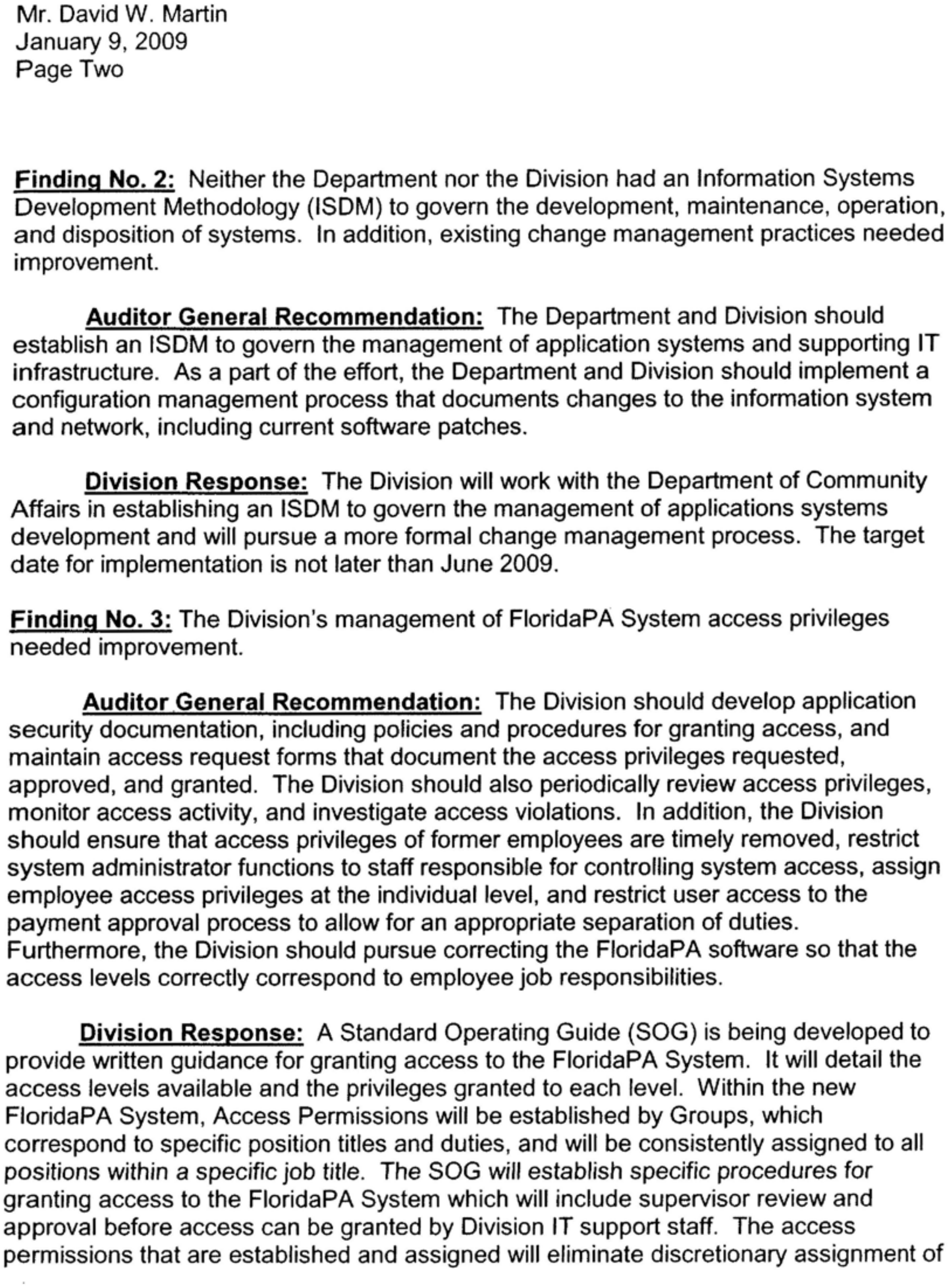
This letter is submitted as a response to the preliminary and tentative findings dated December 12, 2008, regarding the Department of Community Affairs and Division of Emergency Management, Information Technology, Florida Public Assistance System.

Finding No. 1: Department and division security policies and procedures had not been fully developed or approved and were not sufficiently comprehensive.

Auditor General 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.

Division Response: The Division will work with the Department of Community Affairs, who has recently appointed an Information Security Manager (ISM), in defining an integrated security policy consistent with the requirements and provisions of the Security of Data and Information Technology Infrastructure Act (Chapter 282.318, Florida Statutes), the Florida Computer Crimes Act (Chapter 815, Florida Statutes), State Security Rule 60DD-2, and agency guidelines established by the Agency for Enterprise Information Technology Office of Information Security. Also, the ISM will create an employee training program to promote ongoing security awareness. The target date for completion of the Department/Division Security Policy and Procedures is March 2009.

EXHIBIT A (CONTINUED)
MANAGEMENTS' RESPONSES



Mr. David W. Martin
January 9, 2009
Page Two

Finding No. 2: Neither the Department nor the Division had an Information Systems Development Methodology (ISDM) to govern the development, maintenance, operation, and disposition of systems. In addition, existing change management practices needed improvement.

Auditor General 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.

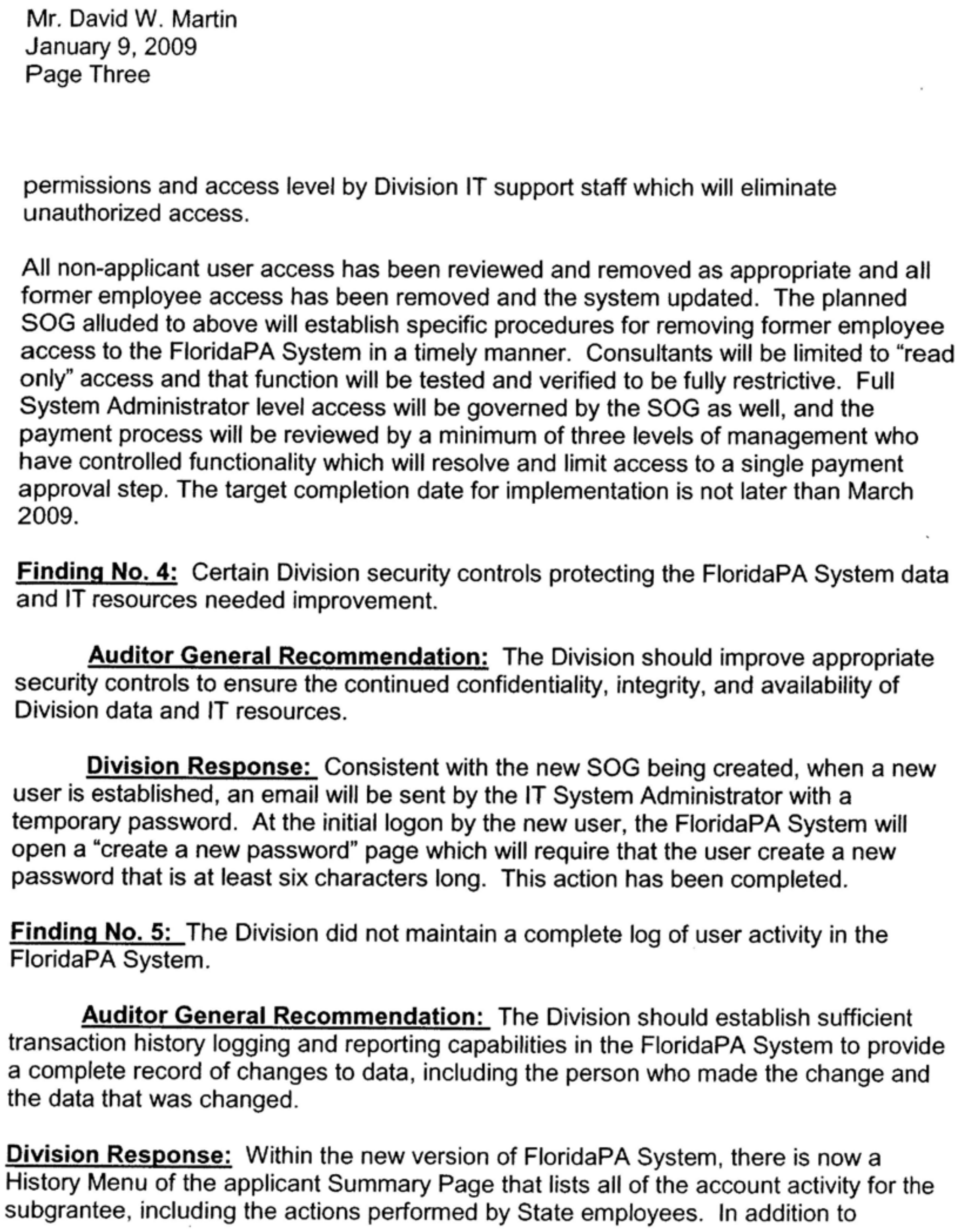
Division Response: The Division will work with the Department of Community Affairs in establishing an ISDM to govern the management of applications systems development and will pursue a more formal change management process. The target date for implementation is not later than June 2009.

Finding No. 3: The Division's management of FloridaPA System access privileges needed improvement.

Auditor General 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 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.

Division Response: A Standard Operating Guide (SOG) is being developed to provide written guidance for granting access to the FloridaPA System. It will detail the access levels available and the privileges granted to each level. Within the new FloridaPA System, Access Permissions will be established by Groups, which correspond to specific position titles and duties, and will be consistently assigned to all positions within a specific job title. The SOG will establish specific procedures for granting access to the FloridaPA System which will include supervisor review and approval before access can be granted by Division IT support staff. The access permissions that are established and assigned will eliminate discretionary assignment of

EXHIBIT A (CONTINUED)
MANAGEMENTS' RESPONSES



Mr. David W. Martin
January 9, 2009
Page Three

permissions and access level by Division IT support staff which will eliminate unauthorized access.

All non-applicant user access has been reviewed and removed as appropriate and all former employee access has been removed and the system updated. The planned SOG alluded to above will establish specific procedures for removing former employee access to the FloridaPA System in a timely manner. Consultants will be limited to "read only" access and that function will be tested and verified to be fully restrictive. Full System Administrator level access will be governed by the SOG as well, and the payment process will be reviewed by a minimum of three levels of management who have controlled functionality which will resolve and limit access to a single payment approval step. The target completion date for implementation is not later than March 2009.

Finding No. 4: Certain Division security controls protecting the FloridaPA System data and IT resources needed improvement.

Auditor General Recommendation: The Division should improve appropriate security controls to ensure the continued confidentiality, integrity, and availability of Division data and IT resources.

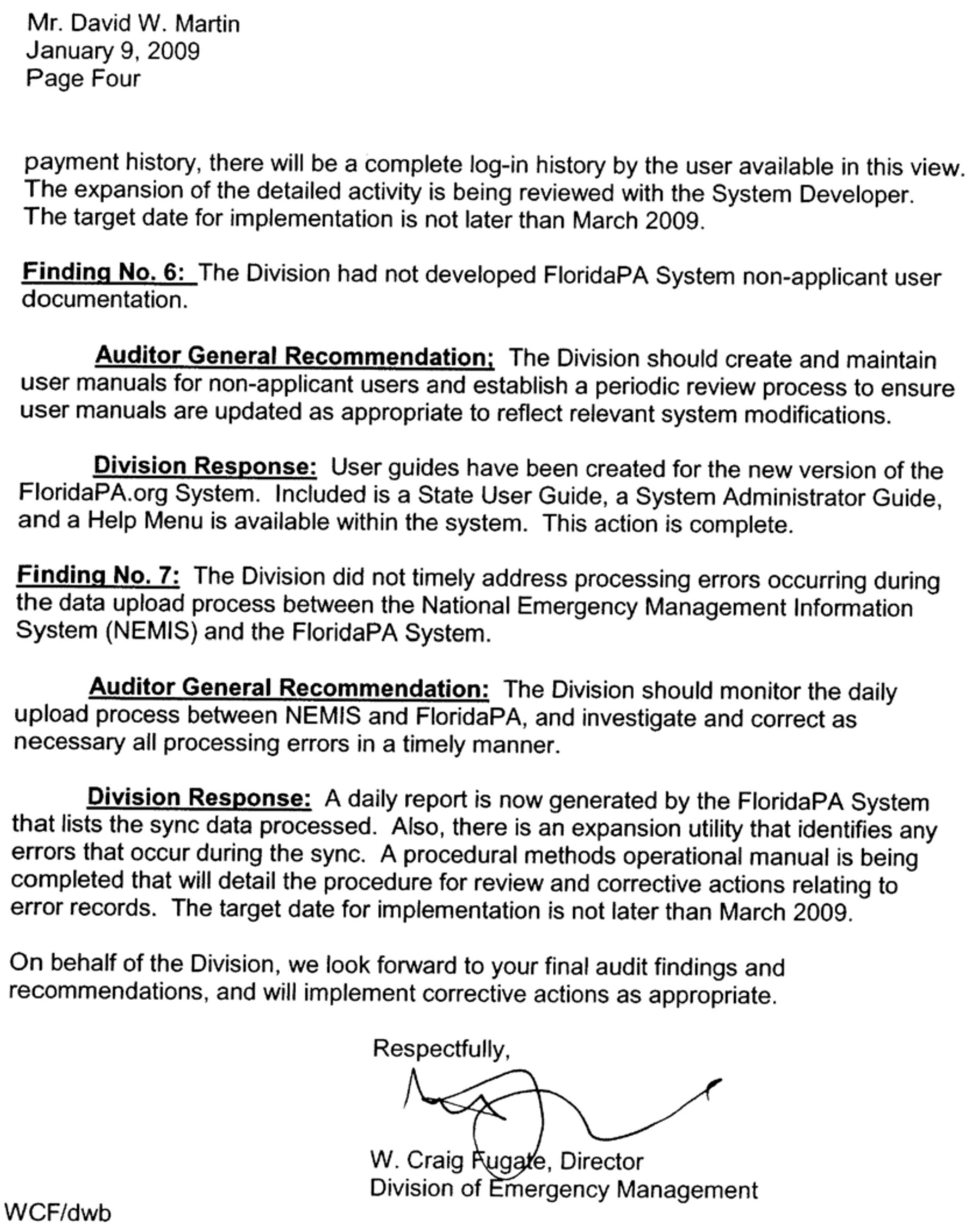
Division Response: Consistent with the new SOG being created, when a new user is established, an email will be sent by the IT System Administrator with a temporary password. At the initial logon by the new user, the FloridaPA System will open a "create a new password" page which will require that the user create a new password that is at least six characters long. This action has been completed.

Finding No. 5: The Division did not maintain a complete log of user activity in the FloridaPA System.

Auditor General Recommendation: The Division should establish sufficient transaction 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.

Division Response: Within the new version of FloridaPA System, there is now a History Menu of the applicant Summary Page that lists all of the account activity for the subgrantee, including the actions performed by State employees. In addition to

EXHIBIT A (CONTINUED)
MANAGEMENTS' RESPONSES



Mr. David W. Martin
January 9, 2009
Page Four

payment history, there will be a complete log-in history by the user available in this view. The expansion of the detailed activity is being reviewed with the System Developer. The target date for implementation is not later than March 2009.

Finding No. 6: The Division had not developed FloridaPA System non-applicant user documentation.

Auditor General Recommendation; The Division should create and maintain user manuals for non-applicant users and establish a periodic review process to ensure user manuals are updated as appropriate to reflect relevant system modifications.

Division Response: User guides have been created for the new version of the FloridaPA.org System. Included is a State User Guide, a System Administrator Guide, and a Help Menu is available within the system. This action is complete.

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.

Auditor General 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: A daily report is now generated by the FloridaPA System that lists the sync data processed. Also, there is an expansion utility that identifies any errors that occur during the sync. A procedural methods operational manual is being completed that will detail the procedure for review and corrective actions relating to error records. The target date for implementation is not later than March 2009.

On behalf of the Division, we look forward to your final audit findings and recommendations, and will implement corrective actions as appropriate.

Respectfully,

W. Craig Fugate, Director
Division of Emergency Management

WCF/dwb