AUDITOR GENERAL

WILLIAM O. MONROE, CPA

VOLUSIA COUNTY
DISTRICT SCHOOL BOARD

Information Technology Audit

SUMMARY

The information technology (IT) environment at Volusia County District School Board (District) consists of multiple hardware, software, and application platforms. The District utilizes SmartStream, an Enterprise Resource Planning (ERP) system, to provide application processing for its financial applications. Our audit focused on evaluating selected IT functions and determining the effectiveness of general controls applicable to the District for the period October 2003 through January 2004; determining management's awareness of, and actions taken regarding, the Health Insurance Portability and Accountability Act of 1996 (HIPAA); and determining whether the District had corrected, or was in the process of correcting, IT-related deficiencies disclosed by the predecessor auditor in a management letter dated October 17, 2002.

As described below, we noted deficiencies in certain general controls related to the District's functions and practices:

Finding No. 1: A Districtwide security program had not been formally devised to ensure that exposures and vulnerabilities of IT resources had been sufficiently assessed by management and addressed through enforced user and system security controls. Additionally, the District had not designated a chief security officer or similar function to provide for a unified security program over the District's information resources.

Finding No. 2: The District had not established written policies and procedures governing various IT functions, including an information systems development methodology. Additionally, the District had not sufficiently documented the overall data flow, interfaces, or customized processes for its systems.

Finding No. 3: The District's software change management practices needed improvement.

Finding No. 4: The District had inadequate segregation of duties within IT that permitted staff within the SmartStream environment to design, develop, program, test, and move stored procedures into production.

Finding No. 5: Deficiencies were noted in the District's business continuity controls.

BACKGROUND

On April 29, 1998, following an informal selection process, the District entered into a contractual agreement with GEAC Enterprise Solutions, Inc., for implementation of selected SmartStream software modules, including General Ledger, Funds Control, Budget, Asset Management, Accounts Payable, Purchasing, Personnel, Benefits, and Payroll, replacing the District's legacy financial, payroll, procurement, and human resources software systems. When the final module was placed into production on January 1, 2000, all modules were operational.

In May 2003, the District entered into a license agreement with CrossPointe, Inc., to replace its existing SmartStream human resources modules. The new application is expected to be completed by July 2004.

The Management Information Services (MIS) Executive Director reports to the Deputy Superintendent and is a member of the Superintendent's Management Team, where policies and projects affecting IT are discussed and adopted.

Finding No. 1: Districtwide Security Program

Effective security relies on a security structure that includes consideration of data classification and ownership, organizational and operational policies, a thorough review of security, user awareness, and security administration procedures. Specific procedures developed for each of the major functions of security administration include designing the security hierarchy; granting and revoking data and resource access; and reporting and monitoring activity. Also, a systematic risk assessment framework incorporates a recurring assessment of relevant information risks to the achievement of business objectives and forms a basis for determining how the risks are managed. Additionally, it is a good business practice to assign the responsibility for implementing and overseeing the security program to a chief security officer or similar function that reports to a level of management that maximizes the independence and objectivity of the security function.

The absence of a Districtwide security program, and corresponding policies and procedures, along with the lack of a formally designated chief security officer or similar function, may have contributed to the following information security control deficiencies we noted at the District:

- The District had not established policies and procedures for security controls, such as the granting, revoking, documenting, and monitoring of user access to information resources; periodic review of user access; security administrator and database administrator functions; and proper use of wireless networks, computers, keyboards, and personal digital assistants (PDAs).
- The District's IT risk management process needed improvement. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising District information. However, appropriate District personnel have been notified of these issues.
- The District had not finalized its security awareness and training program. School Board Policy 518 regarding the use of electronic information services (such as the Internet, databases, electronic mail, and any computer-accessible source of information) and school office equipment was available on the District's internal network. The policy stated that anyone who violated the terms of the policy may be denied access and may be subject to disciplinary action. All existing District employees were required to sign an acknowledgement of receipt of this policy during December 2002 and all new employees were required to sign the acknowledgement form prior to being granted network, mainframe, or SmartStream application access. The District conducted its first security awareness training class on December 11, 2003, which was attended by departmental and school security contacts. Items discussed included topics such as

electronic mail security, virus protection, Policy 518, and password integrity, among other items. Although training material was distributed at this meeting, this training material had not been formally disseminated to all information resource users. Without an adequate security awareness and training program for all staff with access to IT resources, the risk is increased that employees may not be aware of their security responsibilities or the consequences of not fulfilling those responsibilities.

- Certain important security features available in the software had not been utilized and certain security controls protecting the network and the administrative applications needed improvement. Specific details of these security deficiencies are not disclosed in this report to avoid any possibility of compromising District information. However, appropriate District personnel have been notified of these deficiencies.

- The District did not have adequate policies and procedures in place to ensure that access capabilities were timely revoked or modified, as necessary, for individuals who either terminated employment or transferred to a position that no longer required them to have access. The primary objective for timely revocation of system access privileges for former employees is to ensure that the privileges are not exploited by the former employee or others.

  During our testing of user access for employees who had terminated employment between January and October 2003, we noted that user IDs for three employees continued to have access after the employees' termination dates. Two of the employees were no longer employed with the District but had active Windows NT access. The other employee had a one-month break in service with the District, but did not have Windows NT or SmartStream access inactivated during that time period. The District indicated that it had an informal policy whereby the District's personnel office notifies the Security Administrator Specialist of employee terminations and transfers. However, notification was not received for the two terminated employees and the other employee's temporary departure from the District was not treated as a regular termination. Because the District had not maintained sufficient logs, we were not able to determine if there had been any logon activity for the user IDs in question during the period between the termination of an employee and the actual date that the employee's computer access was deactivated.

  Without adequate procedures to ensure the timely revocation of access for terminated employees or the modification of access for transferred employees, the risk is increased that a former employee's access privileges could be used by an unauthorized individual to make unauthorized changes to data files, programs, or applications or that the employee may gain access to information that is beyond the scope of his current position's duties.

- Access authorization forms approving user access to the District's network and SmartStream applications were not on file for all users. During our testing of user access authorization, we noted that documentation of approval of network access was not available for 13 of the 14 users tested. Additionally, documentation for SmartStream application access was not on file for 13 of the 14 users tested. When unnecessary access privileges exist, the risk is increased that unauthorized disclosure, modification, or destruction of data could occur through the misuse of the access capabilities.

- The District's monitoring of system security events and activity needed improvement. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising District information. However, appropriate District personnel have been notified of the issues.

Absent a formal security program, the risk is increased that sound information security controls will not be sufficiently assessed and imposed to prevent compromise of data confidentiality, integrity, and availability. Without the formal designation of a chief security officer or similar function, the risk is increased that the District's security program for data and IT resources will not be fully controlled and the integrity, confidentiality, and availability of information systems data and resources may be compromised.

Recommendation: The District should develop a formal security program including an assessment of defined risk, mitigating controls, and acceptance levels. The program should incorporate increased user awareness, acknowledgment, and accountability of imposed controls. Also, notification procedures and reporting tools should be enhanced to ensure that inappropriate access privileges are timely revoked and that access is properly authorized. Further, the District should designate an Information Security Manager and specify the duties to be performed by the Manager. Responsibilities may include: facilitating risk assessments; coordinating the development and distribution of IT policies and procedures; routinely monitoring compliance with these policies; promoting security awareness and training among users; and providing reports to senior management on policy-related matters.

Finding No. 2: Policies and Procedures

Each function within an organization needs complete, well-documented policies and procedures to describe the scope of the function, its activities, and the interrelationships with other departments. Policies establish the organization's direction, while procedures indicate how policies are to be implemented and followed. A formalized and documented information systems development methodology (ISDM) can provide consistent guidance to all staff at all levels of skill and experience. An ISDM typically details the procedures that are to be followed when applications are being designed and developed, as well as when they are subsequently modified. It also provides that all external and internal interfaces are properly specified, designed, and documented. We noted the following deficiencies in District IT policies and procedures:

- District management had not developed or implemented an ISDM, nor established corresponding policies and procedures governing systems development and modification, such as data modification and data conversion using utilities, programs, or manual means; acquisition, installation, authorization of modifications, and testing of application software; movement of programs into production and monitoring; the use of FTP; the use of unauthorized software on personal computers; scheduling and monitoring of job activity; software and hardware performance issues and actions taken; and change (patch) management for application and systems software. The District used an informal and undocumented process to control its development and maintenance activities. Specific deficiencies in the District's software change management practices, that might have been avoided had effective policies and procedures existed, are discussed in Finding No. 3.
- The District had not sufficiently documented the overall data flow, interfaces, or customized processes for its systems. The District maintained multiple software and hardware platforms to provide its business and student data processing functions. Various processes and interfaces were utilized to share data and provide customized applications. As

of January 2004, there were four basic extraction processes used by the District to reformat data to input into the SmartStream application. In some cases, the data was extracted from SmartStream and in other cases it came from external systems and was reformatted to an acceptable input into SmartStream. Our audit revealed that none of these processes had been documented. During our fieldwork, the District documented the Invoice Processing procedures through flowcharts, screen prints, and written steps. However, there was no documentation describing how these processes and interfaces worked together for the remaining three processes.

In the absence of policies and procedures outlining controls and measures necessary for the quality and consistency with which the District's objectives are achieved, the risk is increased that management will not have a basis for determining whether directives are properly performed nor will personnel have guidelines for meeting management's expectations. Also, without an established methodology governing the development, maintenance, or acquisition of IT systems and projects, management risks the successful implementation of the system or project and may not satisfy the users' needs or meet the organization's business needs. Additionally, without adequate documentation describing the overall data flow, interfaces, and customized processes of systems, the risk is increased that as changes are made within the software and hardware platforms, mistakes and errors could occur. This issue could become more critical as the District migrates its Human Resources activities from the SmartStream application to the CrossPointe application.

Recommendation: Management should develop and distribute policies and procedures addressing the above-mentioned areas to appropriate personnel. In particular, management should develop and document a formal ISDM to guide the development, maintenance, and acquisition of IT systems and projects. Additionally, management should document the overall data and transaction flow, interfaces, and customized processes for its systems.

Finding No. 3:
Software Changes

Proper software change control procedures require that documentation is maintained to evidence software change requests and associated approvals, to ensure that only authorized changes are moved into the production environment.

We noted deficiencies in certain software change management practices of the District:

- The District did not modify the SmartStream system at the program level. Consequently, in order to manipulate data in a manner other than how SmartStream processes information, the District processed data in an ETL (Extraction, Transformation, and Load) mode. Stored procedures were written by the District to extract SmartStream data, summarize it, and then re-input it in a specified file format. Most of these processes were developed during the implementation of SmartStream. However, change requests to modify the stored procedures could be initiated by a user or MIS personnel whenever a problem was identified. Since, as similarly noted in Finding No. 2, there were no formal change management procedures to record and monitor these types of changes, they were informally authorized, approved, prioritized, and monitored within MIS without formal documentation.
- Additional deficiencies were noted in the District's management of changes or patches to application and systems software. Specific details of these deficiencies are not disclosed in this report

to avoid the possibility of compromising District information. However, appropriate District personnel have been notified of the deficiencies.

Failure to maintain adequate documentation of program changes may result in difficulty in ensuring that only authorized program changes are moved into production.

Recommendation: As a part of developing an ISDM, the District should establish appropriate software change management procedures to provide increased assurance that all software changes are properly authorized, tested, and implemented.

Finding No. 4: Segregation of Duties

Segregation of work responsibilities is fundamental, so that one individual does not control all critical stages of a process. A proper segregation of duties would include a group independent of the user and programming staff controlling movement of programs and data.

As previously mentioned in Finding No. 3, stored procedures were used by the District to extract SmartStream data, summarize it, and then re-input it in a specified file format. Most of these processes were developed during the implementation of SmartStream. However, change requests could be initiated by a user or MIS personnel, whenever a problem was identified. The stored procedure was then designed, written, tested, and moved into production by the same programmer.

Without an adequate segregation of duties, the risk is increased that erroneous or fraudulent transactions could be processed, that improper program changes could be implemented, and that computer resources could be damaged or destroyed.

Recommendation: To the extent practicable, management should separate incompatible functions within the applications development section and prohibit any individual from being able to design, write, test, and move stored procedures into production.

Finding No. 5: Business Continuity Controls

Business continuity controls are intended to ensure continuous service to meet District business requirements, make certain IT services are available as required, and lessen the business impact in the event of a major disruption. Business continuity planning identifies and provides information on supporting resources needed and the roles and responsibilities of those involved in the recovery process, including user department personnel.

We identified deficiencies in the District's business continuity controls. Specific details of these deficiencies are not disclosed in this report to avoid the possibility of compromising District information. However, appropriate District have been notified of the deficiencies.

Recommendation: The District should enhance its business continuity controls.

OTHER MATTERS

HIPAA[1] addresses data interchange, privacy, and information security standards for personal health information. Pursuant to HIPAA, the United States Department of Health and Human Services has published regulations on electronic data interchange standards, privacy, and security. The final Transaction Rule, which contains electronic data interchange standards, was incorporated as a Federal regulation and had a compliance date of October 16, 2002. The final Privacy Rule was

[1] Public Law 104-191

incorporated as a Federal regulation and compliance was required by April 14, 2003. The final Security Rule was incorporated as a Federal regulation and has a compliance date of April 21, 2005. HIPAA also provides for civil and criminal penalties for noncompliance.

In response to our inquiry regarding the HIPAA legislation, the District indicated that information obtained in its operation and sponsorship of various health and welfare programs was subject to HIPAA regulations. The District had determined it was not subject to the Transaction Rule and had received written documentation from each of its health and dental carriers outlining their HIPAA compliance programs. The District should continue to evaluate the impact of HIPAA requirements on all District IT activities due to the dynamic nature of the data transmitted over the network by District units which may be subject to this Act in the future.

PRIOR AUDIT FINDINGS

Except as discussed in the preceding paragraphs, the District had corrected, or was in the process of correcting, portions of the IT-related deficiencies as reported by the predecessor auditor. Certain issues within Finding Nos. 1, 2, and 5, previously noted by the predecessor auditor, remained unresolved.

SCOPE, OBJECTIVES, AND METHODOLOGY

The scope of this audit focused on evaluating management controls and selected IT functions applicable to the District during the period October 2003 through January 2004. Our objectives were to determine the effectiveness of selected controls related to the District; to determine management's awareness of, and actions taken regarding HIPAA; and to determine whether the District had corrected, or was in the process of correcting, IT-related deficiencies disclosed by the predecessor auditor in a management letter dated October 17, 2002.

In conducting our audit, we interviewed appropriate District personnel, observed District processes and procedures, and performed various other audit procedures to test selected IT controls.

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 information technology audit.

William O. Monroe

William O. Monroe, CPA
Auditor General

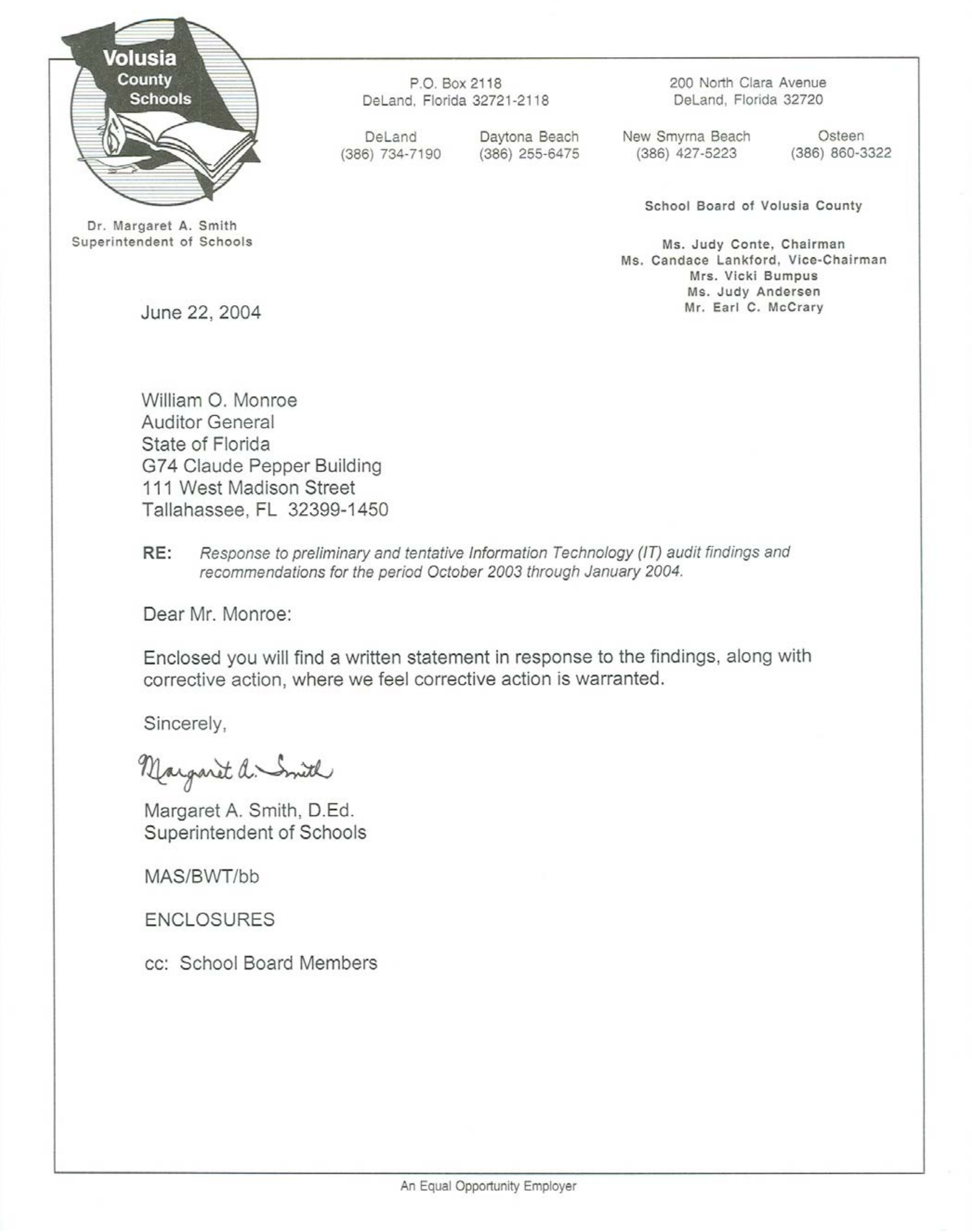
DISTRICT'S RESPONSE

In a letter dated June 22, 2004, the Superintendent provided responses to our preliminary and tentative findings. This letter is included in its entirety at the end of this report.

To promote accountability and improvement in government operations, the Auditor General makes audits of the information technology programs, activities, and functions of governmental entities. This information technology audit was made in accordance with applicable standards contained in ***Government Auditing Standards*** issued by the Comptroller General of the United States. This audit was conducted by Kathy Sellers, CISA, and supervised by Nancy Reeder, CPA*, CISA. Please address inquiries regarding this report to Jon Ingram, CPA*, CISA, Audit Manager, via 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 (http://www.state.fl.us/audgen); by telephone (850 487-9024); or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

*Regulated by State of Florida.



Volusia County Schools

P.O. Box 2118
DeLand, Florida 32721-2118

200 North Clara Avenue
DeLand, Florida 32720

DeLand
(386) 734-7190

Daytona Beach
(386) 255-6475

New Smyrna Beach
(386) 427-5223

Osteen
(386) 860-3322

Dr. Margaret A. Smith
Superintendent of Schools

School Board of Volusia County

Ms. Judy Conte, Chairman
Ms. Candace Lankford, Vice-Chairman
Mrs. Vicki Bumpus
Ms. Judy Andersen
Mr. Earl C. McCrary

June 22, 2004

William O. Monroe
Auditor General
State of Florida
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

RE: *Response to preliminary and tentative Information Technology (IT) audit findings and recommendations for the period October 2003 through January 2004.*

Dear Mr. Monroe:

Enclosed you will find a written statement in response to the findings, along with corrective action, where we feel corrective action is warranted.

Sincerely,

Margaret A. Smith

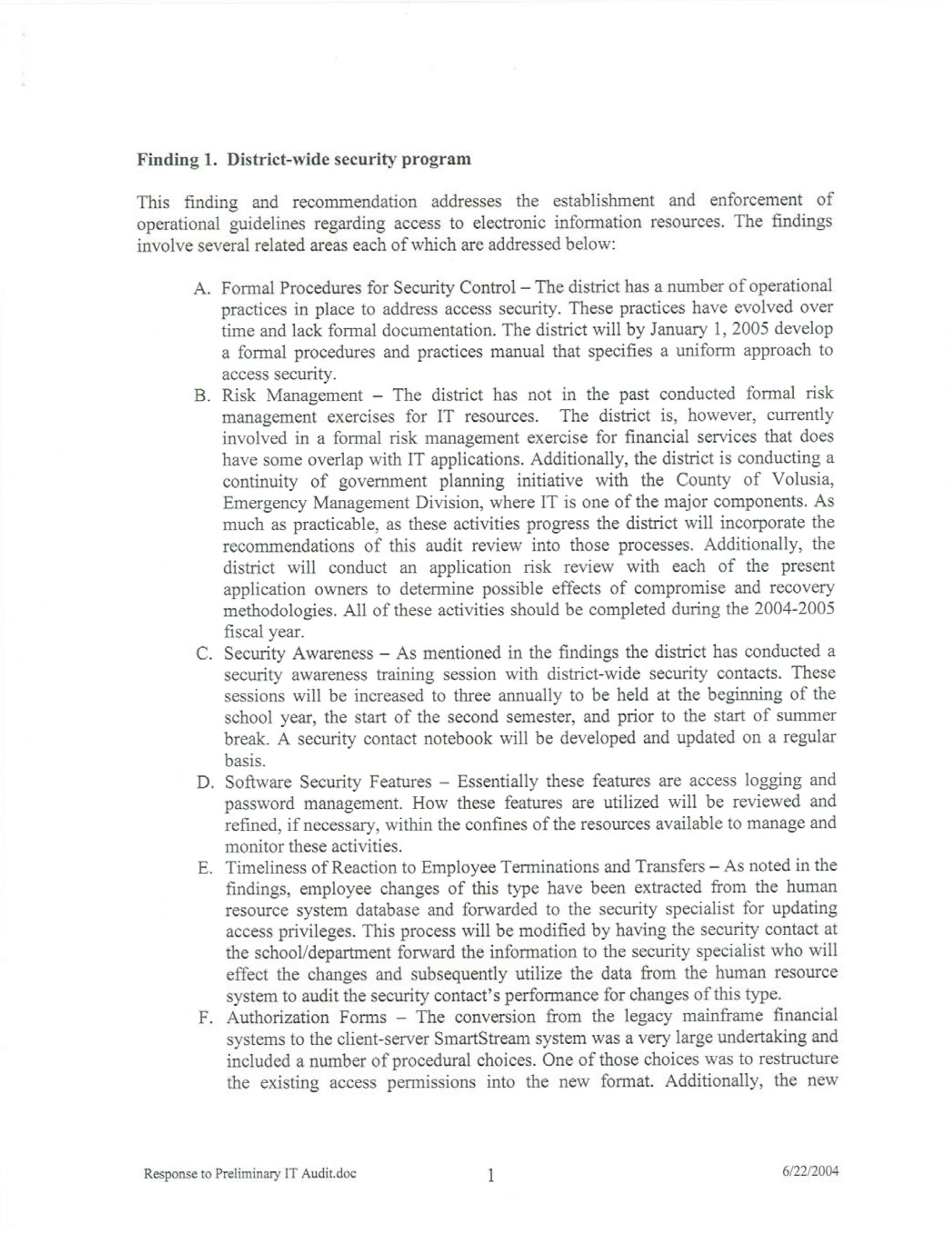
Margaret A. Smith, D.Ed.
Superintendent of Schools

MAS/BWT/bb

ENCLOSURES

cc: School Board Members

An Equal Opportunity Employer



Finding 1. District-wide security program

This finding and recommendation addresses the establishment and enforcement of operational guidelines regarding access to electronic information resources. The findings involve several related areas each of which are addressed below:

A. Formal Procedures for Security Control – The district has a number of operational practices in place to address access security. These practices have evolved over time and lack formal documentation. The district will by January 1, 2005 develop a formal procedures and practices manual that specifies a uniform approach to access security.

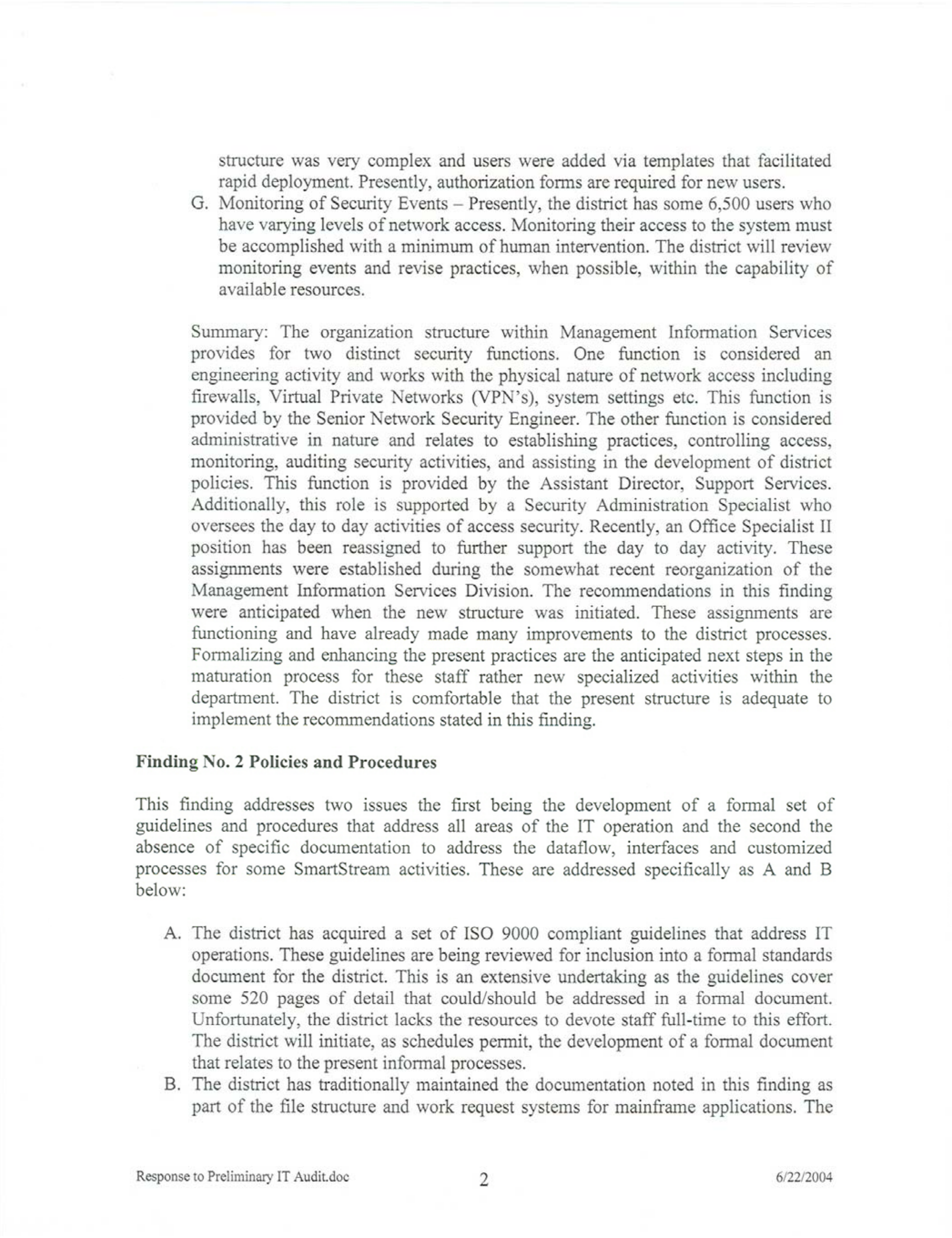
B. Risk Management – The district has not in the past conducted formal risk management exercises for IT resources. The district is, however, currently involved in a formal risk management exercise for financial services that does have some overlap with IT applications. Additionally, the district is conducting a continuity of government planning initiative with the County of Volusia, Emergency Management Division, where IT is one of the major components. As much as practicable, as these activities progress the district will incorporate the recommendations of this audit review into those processes. Additionally, the district will conduct an application risk review with each of the present application owners to determine possible effects of compromise and recovery methodologies. All of these activities should be completed during the 2004-2005 fiscal year.

C. Security Awareness – As mentioned in the findings the district has conducted a security awareness training session with district-wide security contacts. These sessions will be increased to three annually to be held at the beginning of the school year, the start of the second semester, and prior to the start of summer break. A security contact notebook will be developed and updated on a regular basis.

D. Software Security Features – Essentially these features are access logging and password management. How these features are utilized will be reviewed and refined, if necessary, within the confines of the resources available to manage and monitor these activities.

E. Timeliness of Reaction to Employee Terminations and Transfers – As noted in the findings, employee changes of this type have been extracted from the human resource system database and forwarded to the security specialist for updating access privileges. This process will be modified by having the security contact at the school/department forward the information to the security specialist who will effect the changes and subsequently utilize the data from the human resource system to audit the security contact's performance for changes of this type.

F. Authorization Forms – The conversion from the legacy mainframe financial systems to the client-server SmartStream system was a very large undertaking and included a number of procedural choices. One of those choices was to restructure the existing access permissions into the new format. Additionally, the new



structure was very complex and users were added via templates that facilitated rapid deployment. Presently, authorization forms are required for new users.

G. Monitoring of Security Events – Presently, the district has some 6,500 users who have varying levels of network access. Monitoring their access to the system must be accomplished with a minimum of human intervention. The district will review monitoring events and revise practices, when possible, within the capability of available resources.

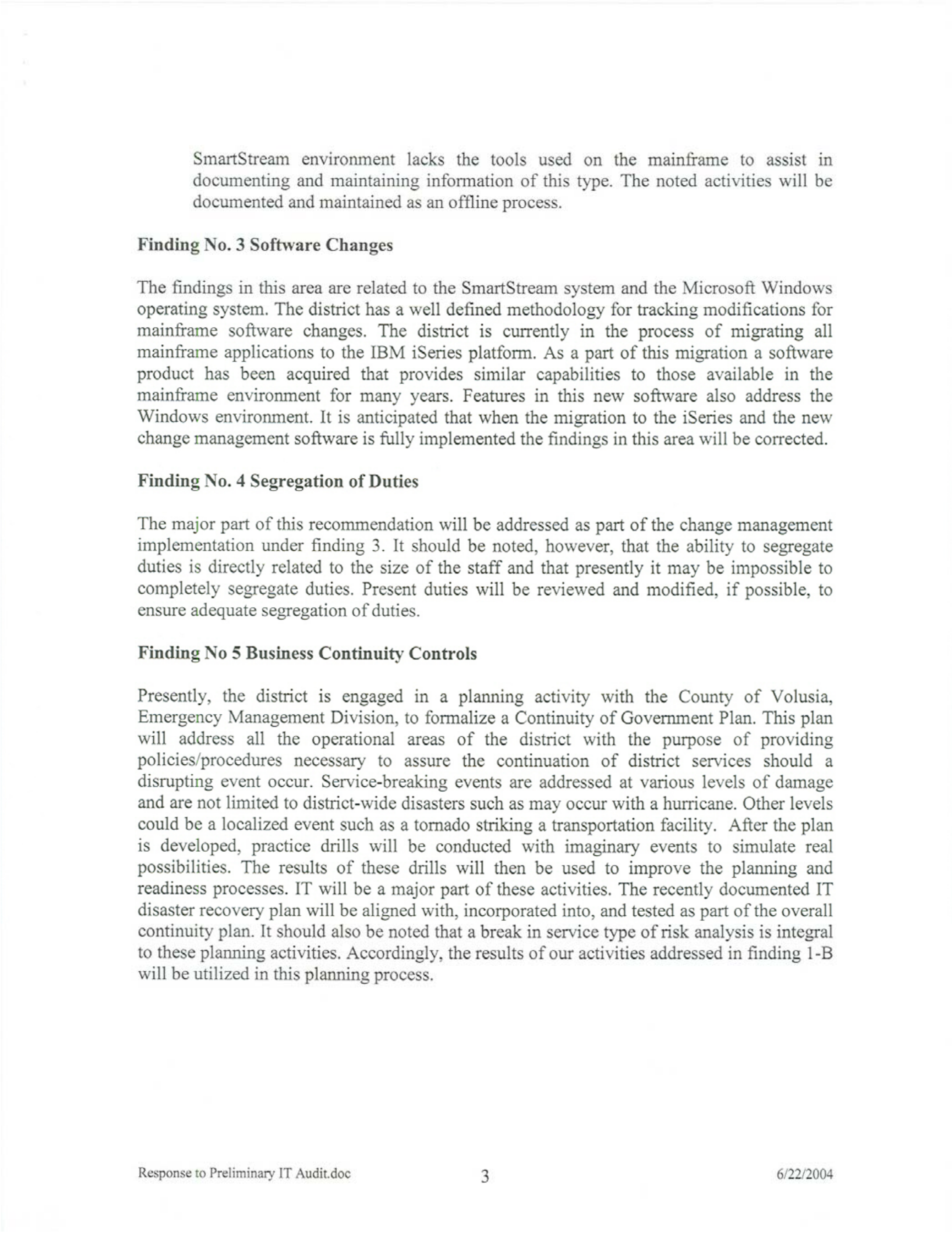
Summary: The organization structure within Management Information Services provides for two distinct security functions. One function is considered an engineering activity and works with the physical nature of network access including firewalls, Virtual Private Networks (VPN's), system settings etc. This function is provided by the Senior Network Security Engineer. The other function is considered administrative in nature and relates to establishing practices, controlling access, monitoring, auditing security activities, and assisting in the development of district policies. This function is provided by the Assistant Director, Support Services. Additionally, this role is supported by a Security Administration Specialist who oversees the day to day activities of access security. Recently, an Office Specialist II position has been reassigned to further support the day to day activity. These assignments were established during the somewhat recent reorganization of the Management Information Services Division. The recommendations in this finding were anticipated when the new structure was initiated. These assignments are functioning and have already made many improvements to the district processes. Formalizing and enhancing the present practices are the anticipated next steps in the maturation process for these staff rather new specialized activities within the department. The district is comfortable that the present structure is adequate to implement the recommendations stated in this finding.

Finding No. 2 Policies and Procedures

This finding addresses two issues the first being the development of a formal set of guidelines and procedures that address all areas of the IT operation and the second the absence of specific documentation to address the dataflow, interfaces and customized processes for some SmartStream activities. These are addressed specifically as A and B below:

A. The district has acquired a set of ISO 9000 compliant guidelines that address IT operations. These guidelines are being reviewed for inclusion into a formal standards document for the district. This is an extensive undertaking as the guidelines cover some 520 pages of detail that could/should be addressed in a formal document. Unfortunately, the district lacks the resources to devote staff full-time to this effort. The district will initiate, as schedules permit, the development of a formal document that relates to the present informal processes.

B. The district has traditionally maintained the documentation noted in this finding as part of the file structure and work request systems for mainframe applications. The



SmartStream environment lacks the tools used on the mainframe to assist in documenting and maintaining information of this type. The noted activities will be documented and maintained as an offline process.

Finding No. 3 Software Changes

The findings in this area are related to the SmartStream system and the Microsoft Windows operating system. The district has a well defined methodology for tracking modifications for mainframe software changes. The district is currently in the process of migrating all mainframe applications to the IBM iSeries platform. As a part of this migration a software product has been acquired that provides similar capabilities to those available in the mainframe environment for many years. Features in this new software also address the Windows environment. It is anticipated that when the migration to the iSeries and the new change management software is fully implemented the findings in this area will be corrected.

Finding No. 4 Segregation of Duties

The major part of this recommendation will be addressed as part of the change management implementation under finding 3. It should be noted, however, that the ability to segregate duties is directly related to the size of the staff and that presently it may be impossible to completely segregate duties. Present duties will be reviewed and modified, if possible, to ensure adequate segregation of duties.

Finding No 5 Business Continuity Controls

Presently, the district is engaged in a planning activity with the County of Volusia, Emergency Management Division, to formalize a Continuity of Government Plan. This plan will address all the operational areas of the district with the purpose of providing policies/procedures necessary to assure the continuation of district services should a disrupting event occur. Service-breaking events are addressed at various levels of damage and are not limited to district-wide disasters such as may occur with a hurricane. Other levels could be a localized event such as a tornado striking a transportation facility. After the plan is developed, practice drills will be conducted with imaginary events to simulate real possibilities. The results of these drills will then be used to improve the planning and readiness processes. IT will be a major part of these activities. The recently documented IT disaster recovery plan will be aligned with, incorporated into, and tested as part of the overall continuity plan. It should also be noted that a break in service type of risk analysis is integral to these planning activities. Accordingly, the results of our activities addressed in finding 1-B will be utilized in this planning process.