AUDITOR GENERAL

WILLIAM O. MONROE, CPA

BREVARD COUNTY DISTRICT SCHOOL BOARD

Information Technology Audit

SUMMARY

The Brevard County District School Board (District) utilizes Comprehensive Information Management for Schools (CIMS) and CrossPointe software that provide application processing for District administrative systems. CIMS software processes financial data that supports functions such as general ledger, accounts payable, purchasing, and budget. CrossPointe software processes data that supports payroll, human resources, and student functions. The District is in the process of migrating all administrative systems to CrossPointe software, with the completion scheduled for July 2005.

Our audit focused on selected general information technology (IT) controls, including aspects of the District's management of the CrossPointe software implementation, and selected terms of the CrossPointe software contract, during the period October 2004 through January 2005, and selected District actions taken from July 2003 through February 2005. We also evaluated the District's progress in correcting selected IT-related deficiencies disclosed in audit report No. 02-129; the performance review and best financial management practice review issued by the Office of Program Policy Analysis and Government Accountability (OPPAGA), dated August 1999; and the management letter issued by the predecessor auditor, dated October 23, 2003.

Certain deficiencies were noted in the District's management controls over selected IT functions. Specifically, these deficiencies included:

Finding No. 1: **Improvements were needed in the District's IT risk management practices.**

Finding No. 2: **Improvements were needed in the District's security management.**

Finding No. 3: **The District lacked centralized IT administration controls and enforcement capabilities necessary to ensure that network configuration and security standards and procedures were applied and performed with adequacy, consistency, and appropriateness throughout the District.**

Finding No. 4: **Deficiencies were noted in the District's IT Disaster Recovery Plan.**

Finding No. 5: **The District lacked a formal information systems development methodology.**

BACKGROUND

In July 2002, the District entered into a contract with CrossPointe, Inc., for the purchase of an Enterprise Resource Planning (ERP) system consisting of student records, human resources, financial information, facilities management, and state reporting software components. The web-based student records, human resources, and state reporting components were installed by the District in November 2003, with the remaining components scheduled to be implemented by July 2005. The price for the software and the first year of maintenance was $1,050,000.

As previously mentioned, the District utilizes CIMS and CrossPointe software to provide application processing for the District's Administrative systems. CIMS and CrossPointe software operate in an IBM environment and under the direct management of Educational Technology (ET). ET is responsible for providing IT resources to meet the needs of the District. Web/Data Warehouse/Instructional Support Services, Application Services, Data Center Services, and Network Services are functional areas within ET and report directly to the ET Assistant Superintendent.

Finding No. 1: IT Risk Management

Risk management is the process of identifying vulnerabilities and threats to IT resources used by an organization in achieving business objectives, and deciding what measures, if any, to take in reducing risk to an acceptable level. Risk assessment is a tool in providing information in the design and implementation of internal controls, in the definition of an IT strategic plan, and in the monitoring and evaluation of those controls. One goal of a risk assessment is to identify the risk of, and protect data from, unauthorized use.

We noted deficiencies in the District's IT risk management practices. Specific details of these deficiencies are not disclosed in this report to avoid the possibility of compromising District information. However, appropriate personnel have been notified of these deficiencies.

Recommendation: The District should implement the appropriate IT risk management practices to provide increased assurance that IT-related risks are identified and managed in a cost-effective manner.

Finding No. 2: Security Management

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 and documented for each of the major functions of security administration include the design of the security hierarchy; the granting and revoking of data and resource access; and the reporting and monitoring of activity.

There were aspects of security management that needed improvement. Specifically:

- The District had not established formal policies and procedures for certain security controls, such as the use of file transfer protocol (FTP); the use of personal digital assistants (PDAs); the use of, and minimum security required for, wireless devices; incident response and reporting for ET personnel handling problems such as hacking, spam, and viruses; minimum password and user authentication controls; the granting, revoking, and maintenance of user access (including physical access to the District's PDAs and laptops); employee termination procedures; the periodic review of user access; the use of screen savers; and the documentation of security and network administrator daily activities. The absence of written policies and procedures for these functions increases the risk that the functions will not be carried out as management intended.
- The District had not implemented an ongoing comprehensive security awareness and training program for new and continuing employees covering the District's administrative and student applications. However, the District maintained *Network and Internet Acceptable Use and Safety* policies for both staff and students that covered, among other things, behavior and communication on the Internet; accessing the Internet using only their own account; transmission of any material; hacking and other unlawful activities; and the uses of the Internet for purposes other than work-related situations. The District also required both staff and students to annually sign the *Network and Internet Acceptable Use and Safety Agreement.* Additionally, the department head or supervisor informed new users of the importance of maintaining security over their passwords. Once this was discussed, access to the systems was granted. However, as previously stated, although there were policies and procedures covering the network and Internet, there were no security policies and procedures covering administrative and student applications or an ongoing security

awareness program for existing staff regarding information security and management's expectations. The lack of a comprehensive security awareness and training program increases the risk to, and the vulnerability of, the District's IT resources, and limits the assurance that the District's level of security over IT resources is adequate.

- Certain District staff had the capability to perform incompatible duties. Segregation of incompatible duties is fundamental to the reliability of an organization's internal controls. Appropriate segregation of duties can assist in the detection of mistakes or errors and potential fraud. Whenever practicable, one person should not control all stages of a process, to minimize the likelihood that errors or fraud could occur without detection. We noted instances of questionable employee access privileges that should be made more restrictive by the District to enforce an appropriate segregation of duties. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising District information. However, appropriate personnel have been notified of these issues.
- Certain important security features available in the software had not been utilized, and certain security controls were inadequate to protect the network and administrative systems. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising District information. However, appropriate personnel have been notified of these issues.

Absent sound security management, the risk is increased that information security controls will not be sufficiently assessed and imposed to prevent compromise of data confidentiality, integrity, and availability.

Recommendation: The District should implement a plan to ensure that policies and procedures are in place for security-related functions within the organization. The policies and procedures should be reviewed periodically and updated as needed for organizational and system-related changes to help ensure that management requirements are met by District staff when performing assigned tasks. Additionally, the District should develop and implement an ongoing security awareness and training program that encompasses both the internal network and administrative and student applications and extend its current procedures for an annual acknowledgement of the acceptable use agreement to encompass both the network and administrative and student applications. Also, the District should implement appropriate security control features to enhance security over its data and programs. Furthermore, the District should review the duties and access capabilities of staff and implement, to the extent practicable, a proper segregation of duties.

Finding No. 3:
School-site Network and Security Administration

Effective IT security and management strategies are coordinated across the enterprise with all components of a network managed as a cohesive unit.

Each school-site network was maintained by a school technician, with direct administrative supervision and control by the school's principal. Although the District's *School Site Local Area Network Installations* policy addressed standards for the network, including the security configuration of wireless networks, there were no network account standards for user IDs and passwords. Additionally, ET staff was limited in its authority to enforce standards issued by the District. Assigning network administration functions to personnel in a decentralized manner without sufficient management oversight and support may result in inefficient and ineffective network configuration and security.

Recommendation: The District should allow ET the authority to develop, monitor, and enforce standardized network management and security policy districtwide.

Finding No. 4:
IT Disaster Recovery Plan

IT disaster recovery plans 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. Testing the plan is essential to determine whether the plan functions as intended in an emergency situation, with the most useful tests simulating a disaster to test the overall service continuity.

Although the District had a comprehensive disaster recovery plan, the plan was last tested in October 2001. Additionally, there was no signed reciprocal agreement between the District and the entity where the District would process its data in an emergency.

Absent a test of the disaster recovery plan and a signed reciprocal agreement where processing would be performed in an emergency, the risk is increased that the District may be unable to continue critical operations during a disaster.

Recommendation: The District should perform periodic testing, at a minimum annually, of its disaster recovery plan and establish a formal agreement for offsite processing services in the event of a disaster.

Finding No. 5: Information Systems Development Methodology

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 acquired, designed, developed, and implemented, as well as when they are subsequently modified. Project management is an inherent part of the ISDM process and defines the scope and boundaries for managing a project, as well as the methodology used in managing the project. The methodology, at a minimum, covers the responsibilities, task breakdown, budgeting of time and resources, milestones, check points, and approvals. Additionally, once the system is implemented, written procedures serve to document the duties of business personnel using the new systems.

Although the District issued Administrative Procedure *7540 G – Computer Software Acquisitions* which addressed software acquisitions, development, and modifications, these procedures did not cover in detail all areas of an ISDM. Areas where policies and procedures were needed included:

- District management had not established policies and procedures governing the modification process for applications and data. Instead, the District used an informal and undocumented process to control maintenance activities. Additionally, the District had not documented application transactions that flowed through multiple systems.
- The District did not have adequate written policies and procedures in place for tracking, evaluating, and applying patches and upgrades to 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 these deficiencies.
- The District had not established corresponding project management procedures. The District instead relied on the experience of the manager over Application Services. Additionally, there were no written procedures for the CrossPointe Human Resource application detailing user functions.

Without an established methodology governing the maintenance of systems, management risks implementation of system modifications that may not satisfy the users' needs, meet the organization's business needs, or preserve appropriate controls. Also, 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. Furthermore, without procedures guiding project management and users of the application, the risk is increased that the project may not be timely implemented or meet the specified objectives.

Recommendation: Management should establish policies and procedures addressing the above-mentioned areas. In particular, management should develop and document a formal comprehensive ISDM which details the requirements needed to track all phases of the system development life cycle to ensure, in part, the ability to efficiently manage and track changes to systems software, applications, and data. Also, the District should formalize a project management plan addressing the issues noted above. Additionally, written policies and procedures should be in place for each function within the organization to ensure that management requirements are met by personnel when performing assigned tasks.

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 OPPAGA and within the scope of our audit. Certain other issues within Finding Nos. 2, 3, and 5, previously noted either in audit report No. 02-129, by the predecessor auditors, or OPPAGA, remained unresolved.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to determine the effectiveness of selected District IT controls, aspects of the District's software implementation project management, and software contract provisions. Our scope focused on selected general IT controls applicable to the CIMS and CrossPointe systems, the District's CrossPointe software implementation project, and the District contract with CrossPointe, for the period October 2004 through January 2005, with selected District actions taken from July 2003 through February 2005. We also evaluated the District's progress in correcting selected IT-related deficiencies disclosed in audit report No. 02-129; the OPPAGA performance review and best financial management practice review, dated August 1999; and the predecessor auditor's management letter, dated October 23, 2003. 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

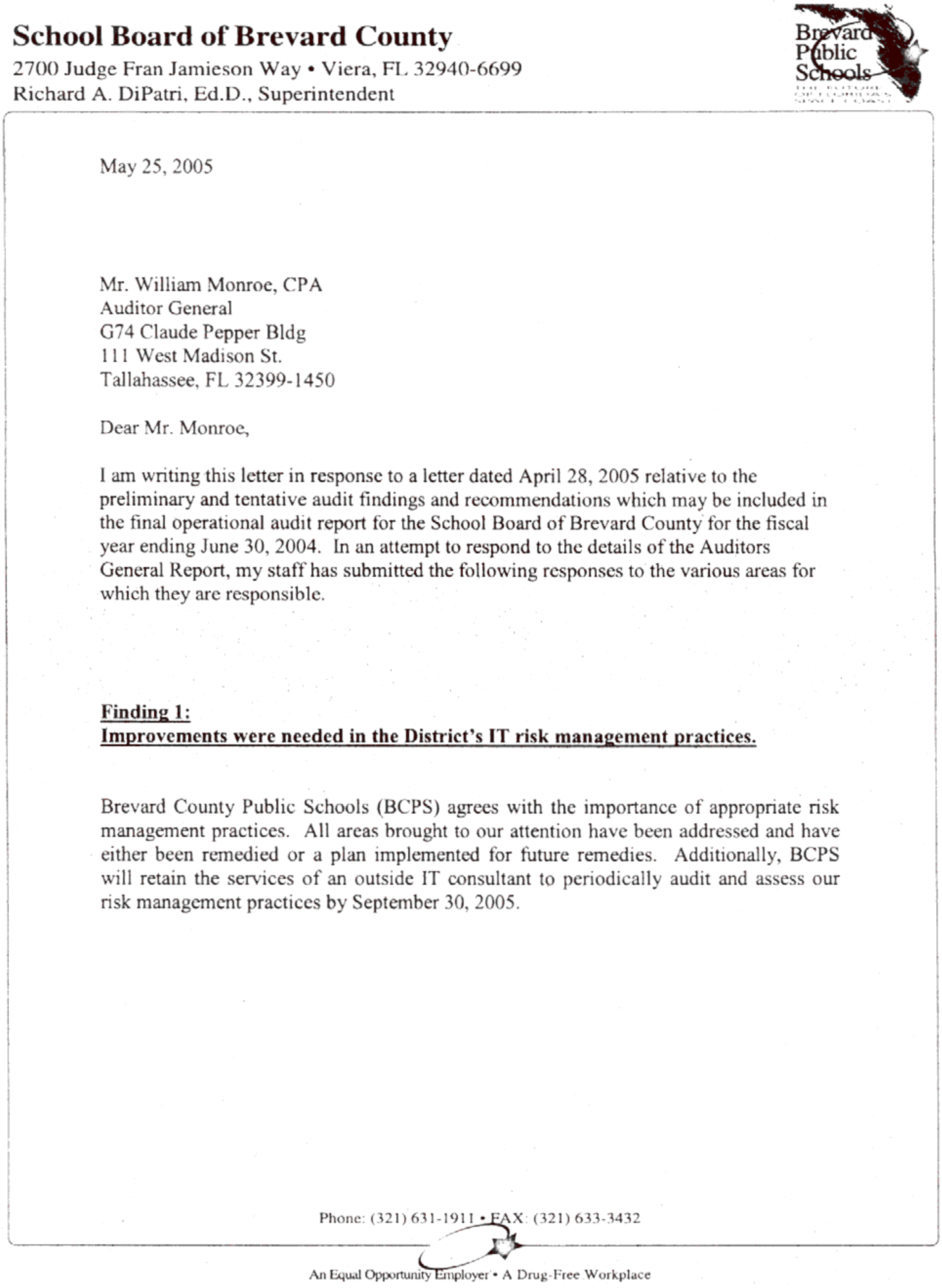
DISTRICT'S RESPONSE

In a letter dated May 25, 2005, 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 Stephanie Hogg, 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.



School Board of Brevard County
2700 Judge Fran Jamieson Way • Viera, FL 32940-6699
Richard A. DiPatri, Ed.D., Superintendent

Brevard Public Schools

May 25, 2005

Mr. William Monroe, CPA
Auditor General
G74 Claude Pepper Bldg
111 West Madison St.
Tallahassee, FL 32399-1450

Dear Mr. Monroe,

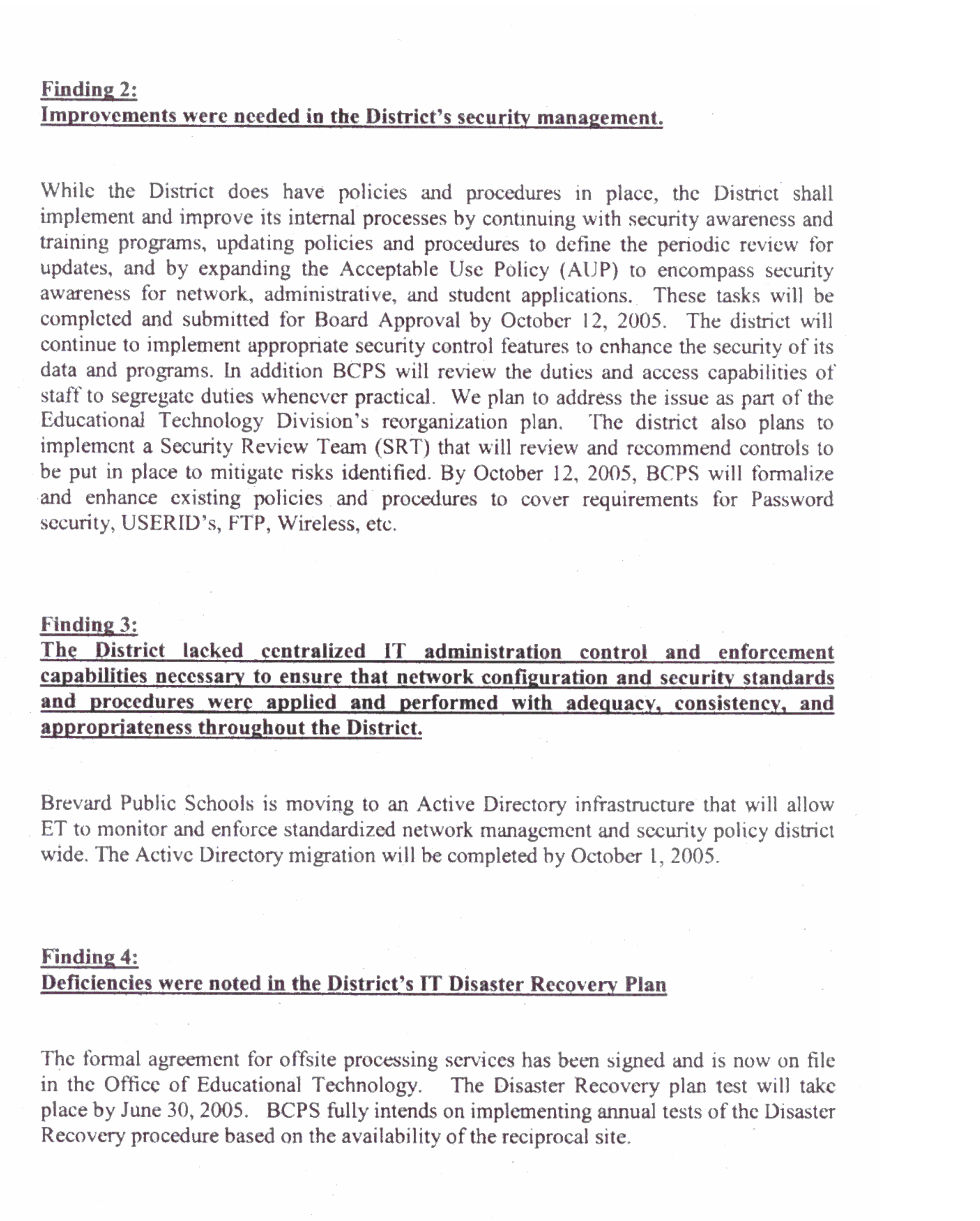
I am writing this letter in response to a letter dated April 28, 2005 relative to the preliminary and tentative audit findings and recommendations which may be included in the final operational audit report for the School Board of Brevard County for the fiscal year ending June 30, 2004. In an attempt to respond to the details of the Auditors General Report, my staff has submitted the following responses to the various areas for which they are responsible.

Finding 1:
Improvements were needed in the District's IT risk management practices.

Brevard County Public Schools (BCPS) agrees with the importance of appropriate risk management practices. All areas brought to our attention have been addressed and have either been remedied or a plan implemented for future remedies. Additionally, BCPS will retain the services of an outside IT consultant to periodically audit and assess our risk management practices by September 30, 2005.

Phone: (321) 631-1911 • FAX: (321) 633-3432

An Equal Opportunity Employer • A Drug-Free Workplace



Finding 2:
Improvements were needed in the District's security management.

While the District does have policies and procedures in place, the District shall implement and improve its internal processes by continuing with security awareness and training programs, updating policies and procedures to define the periodic review for updates, and by expanding the Acceptable Use Policy (AUP) to encompass security awareness for network, administrative, and student applications. These tasks will be completed and submitted for Board Approval by October 12, 2005. The district will continue to implement appropriate security control features to enhance the security of its data and programs. In addition BCPS will review the duties and access capabilities of staff to segregate duties whenever practical. We plan to address the issue as part of the Educational Technology Division's reorganization plan. The district also plans to implement a Security Review Team (SRT) that will review and recommend controls to be put in place to mitigate risks identified. By October 12, 2005, BCPS will formalize and enhance existing policies and procedures to cover requirements for Password security, USERID's, FTP, Wireless, etc.

Finding 3:
The District lacked centralized IT administration control and enforcement capabilities necessary to ensure that network configuration and security standards and procedures were applied and performed with adequacy, consistency, and appropriateness throughout the District.

Brevard Public Schools is moving to an Active Directory infrastructure that will allow ET to monitor and enforce standardized network management and security policy district wide. The Active Directory migration will be completed by October 1, 2005.

Finding 4:
Deficiencies were noted in the District's IT Disaster Recovery Plan

The formal agreement for offsite processing services has been signed and is now on file in the Office of Educational Technology. The Disaster Recovery plan test will take place by June 30, 2005. BCPS fully intends on implementing annual tests of the Disaster Recovery procedure based on the availability of the reciprocal site.

Finding 5:
The District lacked a formal information systems development methodology.

BCPS agrees that policies and procedures governing the modification process for applications and data should be formally documented. The District will document the informal and undocumented process mentioned in this finding by September 30, 2005. The District will also document applications transaction flow through multiple systems September 30, 2005.

Regarding system software, current procedures used to document, track and report on these upgrades, will be formally documented by September 30, 2005. As part of the Educational Technology Division's reorganization plan, we will address the issue of project management procedures. In conjunction with the District's Human Resource Department, the District will provide written procedures detailing the CrossPointe Human Resource application functions by September 30, 2005.

In closing, I would like to thank your staff out of the Tallahassee office, in particular Stephanie Hogg and Nancy Reeder, for their support, professionalism, courtesy and cooperation during the audit process. I look forward to the completion of the operational audit for the fiscal year ended June 30, 2004.

Sincerely,

Richard A. DiPatri, Ed.D.
Superintendent

Cc: School Board