AUDITOR GENERAL

WILLIAM O. MONROE, CPA

MARTIN COUNTY
DISTRICT SCHOOL BOARD
PINNACLE SYSTEM – STUDENT ATTENDANCE

SUMMARY

The Martin County District School Board (District) utilized Excelsior Software's Pinnacle System to, among other things, record, edit, report, and track student attendance-related information. Our audit focused on evaluating selected information technology (IT) controls applicable to the student attendance component of the Pinnacle System during the period January 2005 through April 2005.

As described below, we noted deficiencies in District management controls over selected IT 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.**

Finding No. 2: **Deficiencies were noted in the District's security over student data.**

Finding No. 3: **Deficiencies were noted in the District's IT disaster recovery planning.**

Finding No. 4: **The District did not monitor the content of individual workstations for compliance with software license agreements.**

BACKGROUND

The District used one of its middle schools to pilot Excelsior Software's Pinnacle System beginning in August 2001. From August 2002 through August 2004, the remaining 17 schools were brought onto the Pinnacle System. The Gradebook2 module within the Pinnacle System is used by District teachers to electronically record student daily attendance. Using the Pinnacle System's Attendance Viewer module, the attendance clerks at each school are responsible for modifying student attendance that may have changed since the teacher's initial entry, such as tardiness, excused absence, field trips, and other absences. Attendance clerks may also run reports to ensure that teachers are posting class attendance as required. The attendance clerks' modifications automatically update the teachers' files in the Pinnacle System and, through scheduled jobs, the Pinnacle System data is uploaded to the Total Educational Resource Management System (TERMS) Student System. The TERMS data serves as the official record for student attendance.

The District Educational Technology Department (ET) provides information technology services and networking support for the administrative functions of the District; supports school use of instructional media and technology; and installs various telecommunications networks that support District operations. ET maintains and administers the Pinnacle System, including installing updates provided by the vendor, setting up user accounts, and creating backup and file transfer jobs. It is comprised of 26 full-time positions and consists of the Administrative Technology, Instructional Technology, and Operations and Support groups. The organizational structure consists of an Executive Director, Administrative Technology Coordinator, Instructional Technology Coordinator, and Operations and Support

Supervisor. The Executive Director reports directly to the Superintendent.

Finding No. 1: Districtwide Security Program

An entitywide program for security planning and management is the foundation of an entity's security control structure and a reflection of senior management's commitment to addressing security risks. Principles needed to ensure the information security program addresses current risks include establishing a sound IT risk management process to identify, assess, and mitigate risks; implementing and communicating appropriate policies and controls; promoting security awareness; and monitoring the effectiveness of the policies and controls.

The absence of a Districtwide security program, and corresponding policies and procedures, may have contributed to the following information security control deficiencies we noted at the District:

- The District had not established formal policies and procedures addressing the Pinnacle Security Administrator functions. While the Systems Analyst for the Pinnacle System had been designated as the District's Pinnacle Security Administrator, formally defined policies and procedures, including delegation of authority and responsibility, had not been developed to adequately govern user access issuance and review, identification and implementation of system security related features, password changes and resets, and change control, including testing of application upgrades prior to placing into production.
- The District did not maintain a formal on-going security awareness and training program. Typical means for establishing and maintaining awareness include informing users of the importance of the information they handle and the legal and business reasons for maintaining its integrity and confidentiality; distributing documentation describing security policies, procedures, and individual responsibilities; requiring users to periodically sign a statement acknowledging their awareness and acceptance of responsibility; and requiring comprehensive security orientation, training and periodic refresher programs to communicate security guidelines to both new and existing employees. Although ET provided a presentation addressing security-related issues to new teachers hired for the 2004 school year and Board Rule 6Gx43-1.34(2a) states that "authorized users shall be ultimately responsible for all activity under their account and password", the District had not provided adequate means by which all users were informed of and acknowledged their security-related responsibilities.
- The District's risk management process regarding the Pinnacle System and its network needed improvement. Risk management is the process of identifying vulnerabilities and threats to IT resources used in achieving business objectives, and deciding what measures, if any, to take in reducing risk to an acceptable level. 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 established policies and procedures for the removal of sensitive data from hard drives. Specific details of this issue are not disclosed in this report to avoid the possibility of compromising District information. However, appropriate District personnel have been notified of this issue.
- Certain important security features, in the areas of user identification and authentication, workstation controls, and user access, available in the software had either not been utilized or were inadequate to protect the network and the administrative applications. Specific details of the security deficiencies are not disclosed in this report to avoid the possibility of compromising District information. However, appropriate District personnel have been notified of these issues.

Absent a formal Districtwide security program, the risk is increased that sound information security controls will not be established to prevent compromise of data confidentiality, integrity, and availability and that those security controls will not be used consistently throughout the District. Further, without an adequate security awareness 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.

Recommendation: The District should develop a formal Districtwide security program, along with corresponding policies and procedures, regarding IT security controls and risk management.

Finding No. 2:
Security Over Student Data

Security controls are established to protect the integrity, confidentiality, and availability of data and IT resources. State[1] and Federal[2] law provide, in part, for the privacy of student educational records. We identified deficiencies in the District's security over student data. Specific details of the security 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.

Recommendation: The District should enhance its security controls over student data.

Finding No. 3:
IT Disaster Recovery Planning

Deficiencies were noted in the District's IT disaster recovery planning.

Losing the capability to process, retrieve, and protect information maintained electronically can significantly affect an entity's ability to accomplish its mission. Having procedures in place is fundamental to protecting information resources, minimizing the risk of unplanned interruptions, and recovering critical operations should interruptions occur. The success and effectiveness of a disaster recovery plan requires detailed development of back-up and recovery procedures, including identification of facilities, personnel, hardware, software, communications, and support services, as well as a commitment from management. Adequate back-up procedures include storing copies of data and system software files securely at an off-site location.

The District's disaster recovery plan remained a work in progress. While the plan provided a framework for recovery, the supporting details for back-up files and rotation, supplies inventory, and job documentation for critical systems were incomplete. Additionally, the plan had not been formally approved and the disaster simulation exercises defined in the plan had not been performed, with the exception of testing a payroll run at the alternate site facility. Further, we noted that daily server back-ups were not taken off-site. The tapes remained in the robotic tape library. Subsequent to our audit fieldwork, the District indicated that off-site network back-up rotation had been implemented.

The lack of an approved and detailed disaster recovery plan jeopardizes the District's efforts to efficiently and effectively continue operations with minimal loss and processing disruption.

Recommendation: The District should continue its efforts toward maintaining a comprehensive and management-approved disaster recovery plan to ensure a minimum business impact in the event of a major disruption. The disaster recovery plan should be tested at least annually to ensure that any changes within the IT services environment are incorporated into the plan.

Finding No. 4:
Monitoring of Workstations

The District did not monitor the content of individual workstations for compliance with software license agreements.

It is a good business practice for an organization to periodically check its personal computers for compliance with the requirements of software license agreements. We noted that the District did not require prior approval by ET before allowing installation of personal software on individual workstations.

[1] Section 1002.22, Florida Statutes
[2] Title 20, Section 1232g, United States Code (Family Educational Rights and Privacy Act – FERPA)

According to Board Rule 6Gx43-1.34(2g), "All network users shall adhere to the rules of copyright regarding software, information and the attribution of authorship." Although we did not examine individual workstations, the District indicated that it does not monitor personal computers to ensure compliance with the above District guidelines. Without routine monitoring in place, the risk is increased that the District may be liable for software licensing violations.

Recommendation: The District should establish procedures for monitoring the installation of software to ensure adequate licensing.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to determine the effectiveness of selected general and application IT controls applicable to the Pinnacle System. Our scope focused on evaluating these selected controls during the period January 2005 through April 2005. 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

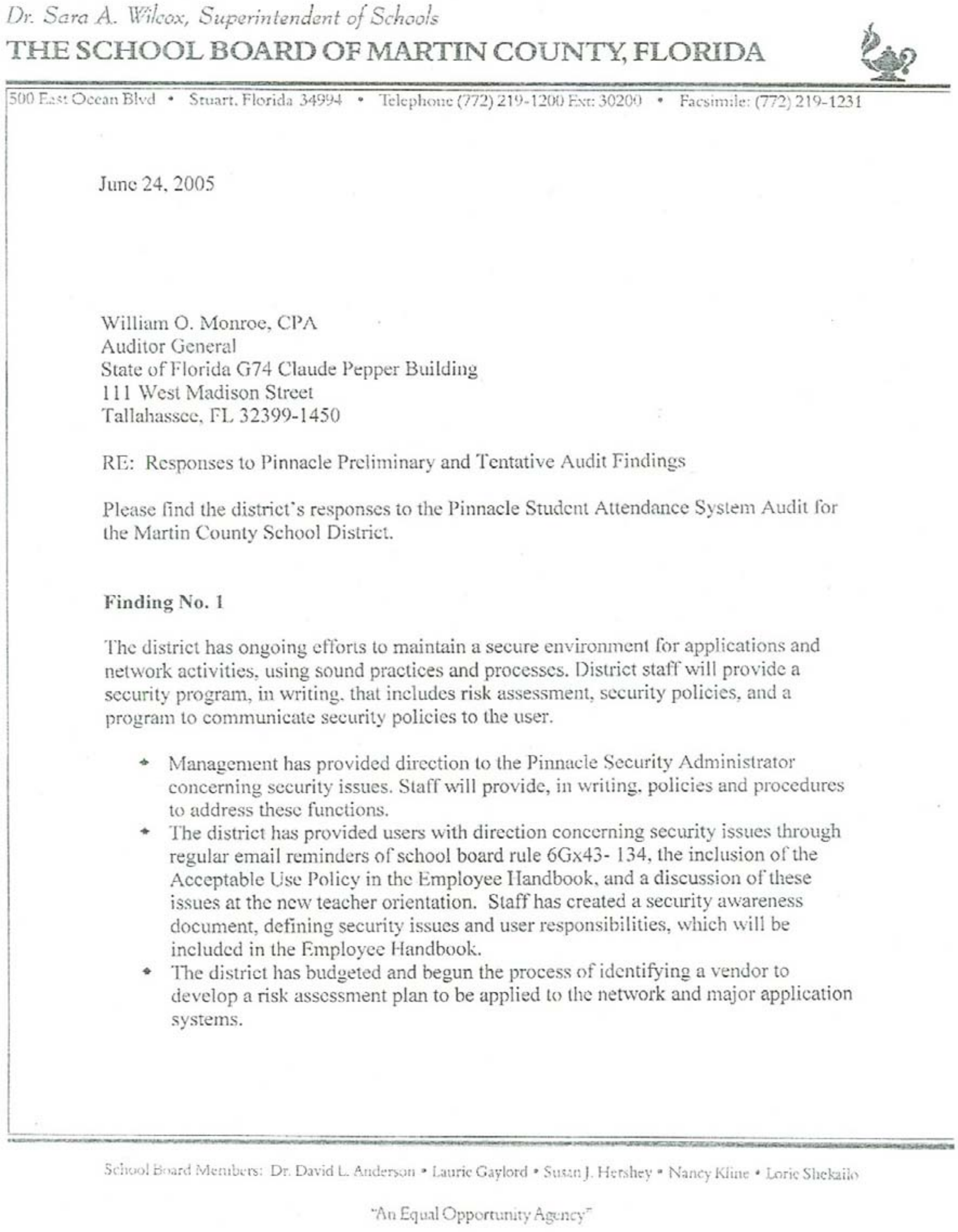
DISTRICT'S RESPONSE

In a letter dated June 24, 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 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.



Dr. Sara A. Wilcox, Superintendent of Schools

THE SCHOOL BOARD OF MARTIN COUNTY, FLORIDA

500 East Ocean Blvd • Stuart, Florida 34994 • Telephone (772) 219-1200 Ext: 30200 • Facsimile: (772) 219-1231

June 24, 2005

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

RE: Responses to Pinnacle Preliminary and Tentative Audit Findings

Please find the district's responses to the Pinnacle Student Attendance System Audit for the Martin County School District.

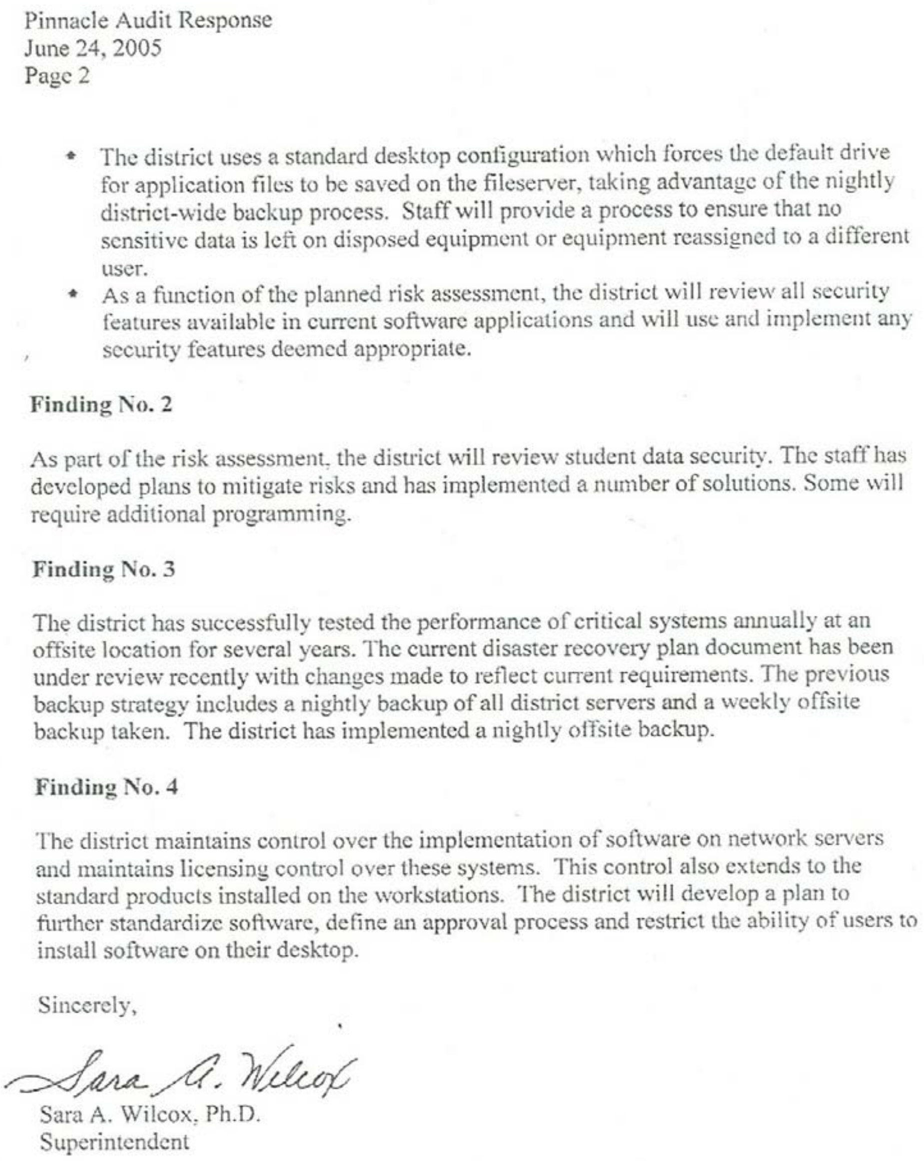
Finding No. 1

The district has ongoing efforts to maintain a secure environment for applications and network activities, using sound practices and processes. District staff will provide a security program, in writing, that includes risk assessment, security policies, and a program to communicate security policies to the user.

- Management has provided direction to the Pinnacle Security Administrator concerning security issues. Staff will provide, in writing, policies and procedures to address these functions.
- The district has provided users with direction concerning security issues through regular email reminders of school board rule 6Gx43- 134, the inclusion of the Acceptable Use Policy in the Employee Handbook, and a discussion of these issues at the new teacher orientation. Staff has created a security awareness document, defining security issues and user responsibilities, which will be included in the Employee Handbook.
- The district has budgeted and begun the process of identifying a vendor to develop a risk assessment plan to be applied to the network and major application systems.

School Board Members: Dr. David L. Anderson • Laurie Gaylord • Susan J. Hershey • Nancy Kline • Lorie Shekailo

"An Equal Opportunity Agency"



Pinnacle Audit Response
June 24, 2005
Page 2

- The district uses a standard desktop configuration which forces the default drive for application files to be saved on the fileserver, taking advantage of the nightly district-wide backup process. Staff will provide a process to ensure that no sensitive data is left on disposed equipment or equipment reassigned to a different user.
- As a function of the planned risk assessment, the district will review all security features available in current software applications and will use and implement any security features deemed appropriate.

Finding No. 2

As part of the risk assessment, the district will review student data security. The staff has developed plans to mitigate risks and has implemented a number of solutions. Some will require additional programming.

Finding No. 3

The district has successfully tested the performance of critical systems annually at an offsite location for several years. The current disaster recovery plan document has been under review recently with changes made to reflect current requirements. The previous backup strategy includes a nightly backup of all district servers and a weekly offsite backup taken. The district has implemented a nightly offsite backup.

Finding No. 4

The district maintains control over the implementation of software on network servers and maintains licensing control over these systems. This control also extends to the standard products installed on the workstations. The district will develop a plan to further standardize software, define an approval process and restrict the ability of users to install software on their desktop.

Sincerely,

Sara A. Wilcox

Sara A. Wilcox, Ph.D.
Superintendent

THIS PAGE INTENTIONALLY LEFT BLANK