SEPTEMBER 2002 REPORT NO. 03-023

AUDITOR GENERAL
WILLIAM O. MONROE, C.P.A.

ST. PETERSBURG COLLEGE

INFORMATION TECHNOLOGY AUDIT
For the Period January 1, 2001, through December 31, 2001

Summary

Our audit focused on management controls and selected information technology (IT) functions applicable to the PeopleSoft applications at the St. Petersburg College (College) for the period January 1, 2001, through December 31, 2001.

PeopleSoft Education and Government (E&G) software is being used to provide collegewide administrative support. The College is running version 7.5 of the PeopleSoft Financials and version 7.6 of the PeopleSoft HR/Payroll System, and is implementing version 8 of the PeopleSoft Student System.

Certain deficiencies were noted in the College's access, systems development and modifications, and general management controls. Specifically, these deficiencies included:

- ***Lack of a collegewide security program to ensure that exposures and vulnerabilities of IT resources had been sufficiently assessed by management and addressed through enforced user and system access controls;***
- ***Lack of policies and procedures defining change management procedures regarding PeopleSoft applications;***
- ***Lack of formal testing of the College's disaster recovery plan regarding the continued operations of PeopleSoft applications through the hot-site.***

Background:

St. Petersburg College, with more than 49,000 students, is the fourth largest and the oldest community college in the State. It has campuses in St. Petersburg, Clearwater, Tarpon Springs, and Seminole and has health, corporate training, and other centers located in St. Petersburg, Clearwater, Largo, and Pinellas Park. Effective June 6, 2001, pursuant to Chapter 2001-170, Laws of Florida, the former St. Petersburg Junior College's name was changed to St. Petersburg College. Additionally, the law authorized the College to offer upper division classes leading to bachelor's degrees in Education, Nursing, and Technology Management.

The College is under the general direction and control of the Florida Department of Education, Division of Community Colleges, and is governed by law and rules of the State Board of Education. The President of the College is Dr. Carl M. Kuttler, Jr. A District Board of Trustees (Board) governs and operates the College. The Board constitutes a corporation and is composed of five members appointed by the Governor, approved by four members of the State Board of Education, and confirmed by the Senate. Board members during our audit period were Evelyn M. Bilirakis, Kenneth P. Burke, W. Richard Johnston, Susan D. Jones, and Cecil B.

Keene. Mr. Keene was appointed in April 2001, while all others were appointed in 1999.

The College is currently in the midst of a multi-year technology migration to the full suite of PeopleSoft E&G software. This includes: (a) PeopleSoft Financials (General Ledger, Accounts Payable, Purchasing and Asset Management), placed in production June 1997; (b) PeopleSoft HR/Payroll (Human Resources, Payroll and Base Benefits), placed in production January 2000; and, (c) PeopleSoft Student Administration, earliest anticipated production date of Summer 2003. The College is currently running "REGIS" student registration and administration software on a Unisys Clearpath mainframe computer. The PeopleSoft system runs on a basic three-tier architecture, client, application server, and database server.

Finding No. 1:

A collegewide 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 access controls.

Effective security relies on a security structure that includes consideration of data classification and ownership, operational policies, organization and resources, user awareness, and security administration procedures. Specific procedures should be developed for each of the major functions of security administration including designing the security hierarchy; granting and revoking data and resource access; and reporting and monitoring activity. Management should establish a systematic risk assessment framework incorporating a recurring assessment of the relevant information risks to the achievement of business objectives and forming a basis for determining how the risks should be managed. Employees should receive and acknowledge documentation describing security policies, procedures, individual responsibilities, and the consequences of security violations.

The absence of a collegewide security program, and the resulting policies and procedures, may have contributed to the following information security control deficiencies we noted at the College:

- The College had not developed an adequate security awareness and training program for its staff. A Board-approved rule (6Hx23-6.900) regarding information technology acceptable use was available on the College's internal network. The policy stated that prohibited use includes circumventing software security procedures or obtaining information system access and passwords to which one is not entitled; unauthorized modifications to hardware or software; and unauthorized access alteration, or destruction of another employee's data, programs, or electronic mail. The policy further depicts consequences in broad terms. However, the users were not required to acknowledge in writing that they were presented with, understood, and would comply with the College's security policies. The College indicated that it currently requires all new users given access to the HR/Payroll system to sign a Protection of Information agreement.
- 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 College information. However, appropriate College personnel have been notified of these deficiencies.

- Procedures for revoking access for terminated or transferred employees were not consistently applied nor was there a viable reporting mechanism which could be used to ensure appropriate action had been taken. The Board procedures for both network and administrative applications security passwords stated the employee's manager was responsible for notifying the appropriate security administrator when employees were terminated or transferred. However, according to each security administrator, notification of termination or transfer should be received from Human Resources.

  Employee transfer procedures with regard to notification, revocation, and reinstatement of access were not explicitly defined. Transferred employees were terminated from the old position and hired in the new position, while remaining in the PeopleSoft Human Resources database with an effective termination date.

  Our review of a calendar year 2001 employee termination report disclosed that, of six employees terminated from employment with the College during 2001, two retained active network accounts on one domain server subsequent to their dates of termination. Access for one of these employees was revoked during the time of our fieldwork. Access for the remaining terminated employee continued with both an active network and application user account in the terminated employee's name, but was being used by the employee who replaced this terminated employee. The respective security administrator was not notified to revoke this terminated employee's access. Absent the ability to trace each transaction or event back to a responsible individual, the College may not be able to hold individuals accountable for their actions.

Absent a formal security program, the risk exists that sound information security controls will not be sufficiently assessed and imposed to prevent compromise of data confidentiality, integrity, and availability. Without review of user access and increased user awareness, acknowledgment, and accountability, a security breach may not be prevented or timely detected and corrected.

Recommendation:

The College should develop a formal security program including an assessment of defined risk, mitigating controls, and acceptance levels. The program should also incorporate increased user awareness, acknowledgment, and accountability of imposed controls. Further, notification procedures and reporting tools should be enhanced to ensure that inappropriate access privileges are timely revoked.

Finding No. 2:

Administrative Information Systems (AIS) management had not formulated policies and procedures defining change management with regard to PeopleSoft applications.

As with other essential business functions of an entity, the IT organization should be guided by policies and procedures describing the scope of its function, activities, and interrelationships with other departments. Policies and procedures establish the organization's direction and provide benchmarks against which compliance can be measured and contribute to an effective control environment.

Although the College followed informal practices to control system changes to the PeopleSoft applications, there were no formal policies and procedures written to define management's expectations for these functions. Additionally, software change requests and approvals were not consistently documented. Requests and approvals were communicated and authorized through various means, including informal, verbal discussions, and via e-mail with AIS staff and College management. In some instances, documentation of the program changes was maintained on-line and in the project's folder. The absence of defined policies and procedures reduces management's assurance that controls and measures necessary for the continued and consistent achievement of intended goals and initiatives will be performed.

Recommendation:

The College should formally define, document, and distribute policies and procedures necessary to achieve management's objectives with regard to assigned change management functions for PeopleSoft applications.

Finding No. 3:

The College's disaster recovery plan regarding the continued operation of PeopleSoft applications through the hot-site had not been formally tested.

The most significant tasks in contingency planning involve testing and validating the plan. Contingency plan testing verifies the completeness and practicality of the plan; determines the feasibility and compatibility of the plan's back-up facilities and procedures; identifies and corrects weaknesses in the plan; and provides training for the information systems department and user department back-up and recovery teams.

The College's Clearwater Campus functioned as a hot-site for both the College's network and PeopleSoft applications. Databases on the UNIX system at the primary data center and at Clearwater were run in parallel. The Clearwater system existed in standby mode so no local changes to or use of the Clearwater databases were made except for automatic application of the archive logs from the production database. The College had tested database recovery at the hot-site, but had not conducted a formal test of its current disaster plan, such as recovery team notification procedures, compatibility of alternate facilities equipment and software, restoration and operation of systems software, communications facilities, and critical application systems at the alternate site. Without the performance of detailed testing procedures, the College may not be assured of full and timely recovery of operations in the event of a disaster.

Recommendation:

The College should continue its plans to formally test the disaster recovery plan for the PeopleSoft applications to ensure response time, actions, and personnel have been sufficiently addressed.

Other Matters:

The United States Congress passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, which addresses electronic data interchange, privacy, and information security standards for personal health information. HIPAA also provides for civil and criminal penalties for noncompliance. Pursuant to HIPAA, the United States Department of Health and Human Services has published regulations on electronic data interchange standards and privacy, with security regulations expected to be published in 2002. Because of the significance of these provisions on the handling and transmission of personal health information, advance planning to evaluate the impact of the HIPAA requirements on the College will serve to reduce the difficulties in making the necessary transition to comply with these new requirements.

The College provides student health programs as well as providing employee health insurance through a self-insurance program underwritten by a commercial insurer.

In response to our inquiries regarding the College's awareness of the HIPAA legislation and any actions the College had taken, the College indicated that it was aware of HIPAA and the pending rule requirements and had undertaken an analysis of its effects; however, a final analysis of its impact and a final plan of action had not been completed on a collegewide basis. We were notified that the College's attorney was researching the issue and his initial consideration was that the College's student health records did not fall under the mandates of HIPAA, but rather under the Family Educational Rights to Privacy Act (FERPA).

The College should complete its analysis of the impact of the HIPAA requirements and, should any requirements be applicable, develop a transition plan to ensure compliance therewith.

Scope, Objectives, and Methodology:

The scope of this audit focused on evaluating selected information technology functions applicable to St. Petersburg College during the period January 1, 2001, through December 31, 2001. Our objectives were to determine the effectiveness of selected general controls relating to St. Petersburg College.

To meet our audit objectives, we reviewed applicable Florida Statutes, administrative rules, and auditing literature; interviewed appropriate College personnel; obtained an understanding of management controls relating to selected information technology functions; observed controls processes and procedures; and performed various other audit procedures to test selected controls related to the College.

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 audit.

William O. Monroe

William O. Monroe, CPA

Auditor General

Department Response:

In a response letter dated September 3, 2002, the President of the College generally concurred with our audit findings and recommendations. The College's response can be viewed in its entirety on the Auditor General Web site.

THIS PAGE INTENTIONALLY LEFT BLANK

ST. PETERSBURG COLLEGE
INFORMATION TECHNOLOGY AUDIT

We conducted our audit 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 M. Reeder, CPA, CISA. Please contact Jon Ingram, CPA*, CISA, Audit Manager, with any questions regarding this report. He may be reached via e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.*

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

**Regulated by State of Florida*

SPC ST. PETERSBURG COLLEGE

OFFICE OF THE PRESIDENT
District Office
(727) 341-3241

September 3, 2002

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

Dear Mr. Monroe:

Thank you for your report dated August 1, 2002, providing findings and recommendations to assure our compliance with state requirements for information technology security, software change management, and disaster recovery.

As you know, St. Petersburg College places a great deal of importance on audit findings and recommendations, and has received some of the best audit results among community colleges. We fully intend to address those areas requiring additional strengthening.

The following are our responses to the findings and recommendations in your report.

Your report states in Finding No. 1: A collegewide 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 access controls. The report further states that the College had not developed an adequate security awareness and training program for its staff.

College Response: While we do agree that a security awareness-training program has not been developed, we are also pleased to report that a collegewide security program has been devised. Over the past three (3) years, the college has implemented a multi-tiered security architecture, including: multiple internet firewalls; central intrusion detection software; central email attachment scanning software; network log-on access controls; database log-on access controls; and desktop virus protection. The college has invested over $180,000 in initial costs for security technology, and currently expends $42,000 per year in recurring costs for security technology. In 2001, the President's Cabinet approved nine (9) updated formal procedures covering physical controls and network access controls for all central systems.

More recently, two (2) employees on technical staff, Messrs. Jeff Rohrs and Shannon Tufts, have completed the CISSP (Certified Information Systems Security Professionals) course, passed the exam, and are now officially CISSPs as recognized by the SANS Institute.

In the coming year, as provided for in the College's 2002-2003 operating budget, the College plans to implement further strengthening of its security program by: a) establishing a new senior network design and security engineer position; b) accomplishing an information systems security audit by an independent firm; c) creating a security awareness training course; and
(d) strengthening security documentation and procedures.

Your report states in Finding No. 2: Administrative Information Systems (AIS) management had not formulated policies and procedures defining change management with regards to PeopleSoft applications.

College Response: The College plans to further strengthen its PeopleSoft change management control with the upgrade of the STAT change management control system. The new STAT upgrade has already been purchased and installed, and staff training is on schedule to be completed in the coming weeks. New policy and procedures will be developed around the STAT change management control system, stipulating how users are to request changes to the PeopleSoft systems, authorization to approve such changes, recording and tracking of actual changes, and so forth.

Your report states in Finding No. 3: The College's Disaster Recovery Plan regarding the continued operation of PeopleSoft applications through the hot-site had not been formally tested.

College Response: The College transferred to in-house its PeopleSoft disaster recovery from SunGard Recovery for cost saving and logistical purposes. The in-house recovery utilizes the Oracle database replication features and internal tape back-up procedures. Both the Oracle replication and tape back-up procedures have undergone initial testing, and are currently in operation. As recommended in the audit report, the College plans to revise its formal disaster recovery plan document to reflect the in-house recovery processes, and to conduct a formal disaster recovery test for the PeopleSoft applications.

<u>Your report states in Other Matters:</u> The College indicated that it was aware of HIPAA and the pending rule requirements and had undertaken an analysis of its effects; however, a final analysis of its impact and a final plan of action had not been completed on a collegewide basis.

<u>College Response</u>: The College will complete an analysis of HIPAA impacts, and develop an action plan, as recommended in the Audit Report. The College requests that the Auditor General staff make available to us HIPAA security regulations as they are published in 2002.

We at St Petersburg College thank you for your report findings and recommendations. We will make productive use of them.

Sincerely,

Carl M Kuttler

Carl M. Kuttler, Jr.

CMKjr:cc

Cc: Conferlete Carney, SPC
David Creamer, SPC
Daya Pendharkar, SPC
Jeff Rohrs, SPC
Ginger Tendl, SPC
Kathy Sellars, Auditor General Office