REPORT NO. 01-013

COLLEGIS Contract
and Selected Information Systems Functions
District Board of Trustees
Valencia Community College

INFORMATION TECHNOLOGY REVIEW

For the Period July 26, 1999, Through February 29, 2000, and Selected College Actions Through June 22, 2000

WILLIAM O. MONROE, CPA

Scope and Objectives

The scope and objectives of this review included:

- Evaluating the COLLEGIS contract and selected information systems functions applicable to the College during the period July 26, 1999, through February 29, 2000, and selected College actions through June 22, 2000, including:
  - Application Systems Development and Modifications,
  - Production Control and Computer Operations,
  - Systems Software and Database Management,
  - Access to Programs and Data, and
  - Physical and Environmental Safeguards.
- Determining whether the provisions of the contract between the College and COLLEGIS are adequate to meet the needs of the College and whether the College and COLLEGIS are complying with these provisions.
- Obtaining an understanding of the components of internal control related to selected client/server applications, including selected computer general and application controls, and determining whether they have been placed in operation.
- Determining whether selected computer general and application controls are adequately designed and operating effectively.
- Evaluating the extent to which the College has corrected, or is in the process of correcting, deficiencies disclosed in the prior audit (report No. 13398, dated March 1, 1999).

Methodology

We conducted our audit in accordance with generally accepted auditing standards and applicable standards contained in *Government Auditing Standards* issued by the Controller General of the United States. To meet the audit objectives described above, we:

- Reviewed the prior audit report and working papers;
- Completed a preliminary survey;
- Interviewed appropriate College and COLLEGIS personnel;
- Reviewed written policies, procedures, and documentation;
- Observed processes and procedures;
- Reviewed applicable Florida Statutes and Florida Administrative Code;
- Obtained an understanding of the College's internal control procedures and assessed control risk;
- Performed tests of controls and various other audit procedures/tests as determined necessary.

Audit Supervised By: Nancy M. Reeder ***Audit Team Leader: Orva Sue Graham***

Auditor General

The Auditor General is provided for by the State Constitution and is appointed by the Legislature to audit public records and perform related duties. The Auditor General is the instrument by which accountability of government is reported to the Legislature and the citizens of the State of Florida. We provide unbiased, objective information on the operation of government.

TABLE OF CONTENTS

LETTER OF TRANSMITTAL

EXECUTIVE SUMMARY

FINDINGS AND RECOMMENDATIONS

PRIOR AUDIT FINDINGS

APPENDIX A - BACKGROUND

APPENDIX B - STATEMENT FROM AUDITED OFFICIAL

AUDITOR GENERAL
STATE OF FLORIDA

G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

WILLIAM O. MONROE, CPA
AUDITOR GENERAL

850/488-5534
Fax: 488-6975

October 10, 2000

The President of the Senate, the Speaker of the
House of Representatives, and the
Legislative Auditing Committee

Pursuant to the provisions of Section 11.45, Florida Statutes, and as part of the Legislature's oversight responsibility for operations of Community Colleges, I have directed the following be made:

COLLEGIS CONTRACT
AND SELECTED INFORMATION SYSTEMS FUNCTIONS
DISTRICT BOARD OF TRUSTEES
VALENCIA COMMUNITY COLLEGE
INFORMATION TECHNOLOGY REVIEW
For the Period July 26, 1999, Through February 29, 2000,
and Selected College Actions through June 22, 2000

The results of the review are included in this report.

Respectfully submitted,

William O. Monroe

William O. Monroe, CPA

Auditor General

William O. Monroe, CPA

COLLEGIS CONTRACT AND SELECTED INFORMATION SYSTEMS FUNCTIONS DISTRICT BOARD OF TRUSTEES VALENCIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY REVIEW

For the period July 26, 1999, through February 29, 2000
and Selected College Actions through June 22, 2000

Introduction:

On June 17, 1998, Valencia Community College outsourced the management and operation of its information technology functions to COLLEGIS, Inc., which staffs the College's Office of Information Technology. The contract, as amended, provides for the College to pay COLLEGIS $14,916,000 for the period of June 18, 1998, through June 17, 2003, with optional extensions that, if exercised, could increase the total contract cost to $18,550,900.

Our review of the COLLEGIS contract and selected information systems functions of the College disclosed deficiencies in the College's management of the contract and in selected computer general controls. These deficiencies, along with related recommendations, are summarized in the following paragraphs.

Finding No. 1

The College contracted for the provision of information technology (IT) services with COLLEGIS without having a long-range information resource technology plan and without soliciting proposals from other vendors.

The College, with COLLEGIS' assistance, was in the process of developing a Strategic Technology Plan that, as of June 22, 2000, was still in draft status. Notwithstanding a provision of State Board of Education Rules that exempted the College from the three-bid requirement, we believe the significant financial and administrative impact of the COLLEGIS contract should have prompted the College to solicit additional proposals from other vendors providing similar services. A lack of documentation of the contract negotiations with COLLEGIS precluded us from determining whether the negotiations were conducted in the College's best interests.

The College should ensure that IT purchases are made in accordance with an approved long-range information resource technology plan and that proposals are solicited before the College enters into arrangements similar to the COLLEGIS contract.

Finding No. 2:

The College has not enforced a contract provision with regard to COLLEGIS implementing the Oracle financial services and human resources/payroll systems. As a result, the College has incurred $233,833.50 in additional costs for Oracle consultants.

The contract with COLLEGIS provides that COLLEGIS shall, among other things, develop a detailed implementation project plan and provide various technology services described in the contract and accompanying exhibits. A detailed implementation project plan, that would have specified additional consulting services costs to be paid for by the College, was not developed. COLLEGIS billed the College and was reimbursed a total of $233,833.50, in excess of the contract cost, for the cost of two Oracle consultants that COLLEGIS hired to assist in the project. These services should have been provided by COLLEGIS, at no additional charge, as part of the scope of services described in the COLLEGIS contract.

The College should seek reimbursement from COLLEGIS for the payments made for the Oracle consultants. The College should also require COLLEGIS to provide technically proficient staff capable of providing the expertise necessary to accomplish the scope of services specified under the contract.

Finding No. 3:

The College's draft Strategic Technology Plan for 2000-2004 does not include estimated costs and timelines to ensure feasibility and performance of the strategic objectives set forth in the plan.

Since September 1998, an external technology strategic planning consultant engaged by COLLEGIS has led the development of a Strategic Technology Plan for 2000-2004. As of June 22, 2000, the draft plan had not been approved by the Board.

The College should include dollar amounts and time frames in its strategic technology plans so that subordinate short-range operational plans and budgets can be developed to accomplish the long-range goals and objectives of the College.

Finding No. 4:

The College has not performed certain provisions for which it is responsible in its contract with COLLEGIS. Additionally, the College is not adequately monitoring COLLEGIS' performance under the contract.

The contract with COLLEGIS places certain responsibilities on COLLEGIS and other responsibilities on the College. We found compliance deficiencies on the part of both COLLEGIS and the College.

Generally, the College has not, as provided in the contract, formally established various plans, policies, procedures, and standards to guide COLLEGIS in performing its duties. Additionally, as of February 29, 2000, annual outcome measurements to use in monitoring COLLEGIS service delivery had not been distributed to the governance committee.

The College should develop and formally adopt the above-mentioned criteria and performance measures to guide and monitor COLLEGIS' contract performance.

Finding No. 5:

The College's information resources disaster recovery draft plan lacks key provisions, including a formal agreement with the back-up site and disaster recovery planning for the current client/server environment.

In the College's contract with COLLEGIS, the vendor is required to ensure that backup and disaster recovery processes have been implemented and tested. The draft plan being developed by COLLEGIS is targeted for completion by the end of calendar year 2000. The plan addresses the mainframe computing environment, but not the client/server environment in which the new financial services and human resources/payroll systems operate.

No formal agreement exists with Northeast Regional Data Center, the back-up site identified in the draft plan. Disaster recovery planning for the current human resources/payroll, financial services, and student applications has not been documented or tested at the alternate site.

The College should continue to develop its disaster recovery plan and address the aforementioned provisions. The College should also test the plan at least annually.

Finding No. 6

The College has not established formal policies and procedures governing application systems development and maintenance. Controls over the program change process need strengthening.

Contractually required information technology policies and procedures have not been finalized by COLLEGIS. The College continues to operate without formal standards governing application change control for either its mainframe systems or purchased client/server systems.

Current program change practices need improvement in the areas of documenting testing, user acceptance, and supervisory review of changes; monitoring the progress of program changes; and moving changes into the production environment. The College should complete its systems development and maintenance standards and distribute them to appropriate personnel.

Finding No. 7:

Deficiencies were noted in the College's information technology access controls.

Access control deficiencies that need addressing by the College include:

- Access policies and procedures are not current with respect to the College's new client/server computing environment and do not address some significant security matters.
- Internet usage policies need to be developed.
- The College needs a security awareness program that emphasizes the importance of information security.
- Computer programmers and operators have inappropriate access capabilities.
- Access capabilities of former employees were not, in some instances, revoked in a timely manner.

Finding No. 8

The College has not established appropriate access control procedures regarding passwords.

We noted the following password control deficiencies, many of which were attributed by the College to limitations in its mainframe security systems:

- Mainframe users are not forced to change their password after their initial sign-on to the system or when a security administrator has reset their password.
- Except in the ICCF security system, mainframe users were not periodically forced to change their password.
- A password verification program is not used to limit the recycling of user passwords or the use of easily compromised passwords.
- Passwords are not encrypted in the CICS mainframe security tables and can be viewed or printed in plain text by security administrators and contracted system programmers.

The College should research the feasibility of implementing a mainframe security system capable of establishing the security parameters listed above. The College should also determine if its client/server environment has features that can be used to correct the exposures listed above.

Finding No. 9:

The College does not routinely use audit trails and logs to aid in the review and investigation of unauthorized access attempts to the College's information resources.

The College has not established procedures for security administrators and College administrators to regularly monitor system security. The mainframe security systems are limited in their recording and reporting of certain security events, limiting the ability of security administrators to monitor system activity for violations.

The College should regularly review access violation reports to timely detect unauthorized attempts to access computer programs and/or data. The College should also consider procuring a security product that could provide the reporting capability not currently available. Additionally, the College should review Oracle alerts as a potential source of information to the College.

Prior Audit Findings

Findings this Audit: 9
Findings Prior Audit: 6
Repeat Findings: 3 (Nos. 5-7)

For those functions within the scope of this audit, the College has corrected the deficiencies noted in audit report No. 13398, except as noted in this report.

Summary of President's Response to Audit Findings

Pursuant to Section 11.45(7)(d), Florida Statutes, the President provided a written response to the audit findings and recommendations included in this report. In his response, the President disagreed with some of our audit findings. The President's complete response is shown as Appendix B in the detailed report.

A copy of report No. 01-013 as well as the other reports issued by the Auditor General can be obtained on the Auditor General web site (www.state.fl.us/audgen)***; by telephone at (850) 487-9030; or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).***

Please contact Mark Roddenberry, Audit Manager, with any questions at e-mail markroddenberry@aud.state.fl.us ***or telephone (850) 488-0701.***

FINDINGS AND RECOMMENDATIONS

In planning and performing our review, we considered the College's internal control relevant to those information systems functions within the scope of audit. Our purpose in considering internal control was to determine the nature, timing, and extent of tests necessary to the accomplishment of our audit objectives, not to provide assurance on internal control.

Our review of selected computer general controls related to the College indicated that management had generally established and maintained a system of internal control to provide reasonable assurance that specific entity objectives will be achieved. Nothing came to our attention during our review that caused us to believe that there were any internal control deficiencies that would have a material effect on the College's overall entity objectives.

We noted certain matters involving the design and operation of the College's internal control that we consider to be reportable conditions. Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of internal control that, in our judgment, could adversely affect management's assurance of compliance with applicable laws, administrative rules, and other guidelines; the effective and efficient operation of the information systems functions; the reliability, integrity, and availability of data and system-generated reports; and the safeguarding and confidentiality of information resources. Those matters coming to our attention for the information systems functions within the scope of review are noted below, beginning with finding No. 1.

A material weakness is a condition in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that operating deficiencies may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions.

Our consideration of internal control would not necessarily disclose all matters in the College's internal control that might be reportable conditions and, accordingly, would not necessarily disclose all reportable conditions that are also considered to be material weaknesses. However, we believe that none of the reportable conditions described below is a material weakness.

Matters coming to our attention relating to significant deficiencies in the design or operation of the College's internal control for the information systems functions reviewed are presented below. These control deficiencies would not have a material effect on the overall evaluation of internal control. These deficiencies and related recommendations are discussed in the following findings under the categories of **Contract Adequacy, Performance, and Monitoring** and **Computer General Controls**.

Contract Adequacy, Performance, and Monitoring

> The College contracted with Coopers and Lybrand in September 1997 to develop a requirements analysis and request for proposals (RFP) for new Year 2000 compliant administrative systems. The RFP was issued in February 1998. In May 1998, responses to the RFP were evaluated by the College and Coopers and Lybrand, after which the College selected finance, human resource, and payroll software from the Oracle Corporation.

In September 1997, the College made contact with COLLEGIS regarding technology issues at the College. In November 1997, COLLEGIS gave a presentation to the College's Executive Council outlining the nature of services that COLLEGIS could provide with regard to outsourcing information technology at the College. The Executive Council, consisting of the College's four vice presidents, three provosts, executive dean, and attorney, provides advice to the College President on various issues. In March 1998, COLLEGIS, at the request of the College, conducted an assessment of the state of technology support at the College.

The College's information technology needs were identified by COLLEGIS and presented on May 12, 1998, to the Executive Council in its *Technology Assessment and Recommendations for Valencia Community College*, dated April 21, 1998. The Council unanimously supported the outsourcing of information technology at the College. On May 20, 1998, the District Board of Trustees was informed of the technology assessment and results thereof. The Vice President for Administrative Services and the College's attorney negotiated a contract with COLLEGIS, which the Board approved on June 17, 1998.

The technology assessment identified such concerns as the "need for an institution-wide technology plan," the "need for coordination and planning for the Year 2000," "antiquated financial management software system … that is not Year 2000 compliant … (t)here is a magnitude of manual operations performed today because data is difficult to share between offices," the "need for (an) information technology governance structure," and the "need for organized project implementation procedures" as critical. The subsequent contract with COLLEGIS was designed to address many of the concerns identified in the Technology Assessment. Based on our review, nothing came to our attention that would cause us to dispute the needs as identified by COLLEGIS. The College has indicated that its Year 2000 preparations were successful in that no significant problems related to the Year 2000 have occurred. Additionally, progress has been made toward meeting other needs discussed in the assessment. However, we noted certain deficiencies related to contracting performance and monitoring, which are discussed in finding Nos. 1-4.

Finding No. 1:

The College contracted for the provision of information technology (IT) services with COLLEGIS without having a long-range information resource technology plan and without soliciting proposals from other vendors.

State Board of Education Rule 6A-14.0734(2)(h), Florida Administrative Code, provides that the acquisition of IT resources as defined in Section 282.303(13), Florida Statutes, is exempt from the three-bid requirement; however, the acquisition shall be made in accordance with the College's long-range Information Resource Technology Plan. According to Section 282.303(13), Florida Statutes, IT resources include data processing services and personnel, as well as hardware and software, communications, supplies, facility resources, maintenance, and training.

The College has not had a unified strategic information resource technology plan addressing issues such as technology requirements, costs, regulatory requirements, staffing, and in- or outsourcing. Instead, individual campuses had developed their own plans. However, the College with assistance from COLLEGIS has developed a draft Strategic Technology Plan for 2000-2004. As of June 22, 2000, the plan was still in draft status. (See finding No. 3 for a further discussion with regard to the plan.)

Although the College did not have a long-range strategic information resource technology plan prior to the date of the contract, the contract was signed on June 17, 1998, and calls for the College to pay COLLEGIS $12,998,000 over a period of five years. There is an optional two-year extension for $3,365,400. The contract provides that the vendor will perform all Computer Services Department functions as a centralized Office of Information Technology (OIT) in support of faculty, staff, and administrators collegewide. As previously mentioned, the Vice President for Administrative Services and the College's attorney negotiated a contract with COLLEGIS, which the Board approved on June 17, 1998. College management indicated that the contract drafting/negotiation process included many meetings between the College and COLLEGIS, with the signed contract being the summation of the negotiations. However, due to the lack of documentation of the negotiation process that produced the signed contract, we were unable to determine whether the contract negotiations were conducted in the best interests of the College. Additionally, considering the significant financial and administrative impact that this contract has on the College, prudent business practices would suggest that College management should have solicited proposals from other vendors providing similar services.

In a memorandum dated December 6, 1999, College management indicated that the College did not evaluate any contractors other than COLLEGIS because it desired to act quickly to prepare the College's computer systems and other technology components for the Year 2000. However, if a long-range information resource technology plan had been in existence, the College would have been in a better position to determine its information technology needs. When the acquisition of information technology resources is not based on the organization's long-range plan, there is a risk of implementing systems or contracting for services that do not meet the organization's mission and goals as expected. Due to the lack of a long-range information resource technology plan, which should have identified the College's information technology needs, we were unable to determine whether outsourcing was in the best interests of the College. Additionally, whenever a vendor is allowed to both assess an entity's needs and provide services to meet those needs without a solicitation of proposals from other vendors providing similar services, the risk exists that the College may contract for services at a higher than necessary cost and may contract with a vendor who lacks the expertise to carry out the provisions of the contract.

The President stated in his response that the College's long-range Information Resource Technology Plan was not a prerequisite to the COLLEGIS contract. Although the Florida Administrative Code does not specifically identify services in the list of information technology acquisitions to be made in accordance with a long-range Information Resource Technology Plan, a plan would provide IT direction and a management strategy for the utilization of IT resources within the College. A long-range Information Resource Technology Plan should identify IT resources including hardware, software, services, networks, data, policies, standards, and facilities that are required to support the business processes of the College. The existence of a long-range Information Resource Technology Plan would have better enabled the College to determine its IT needs prior to entering into the contract with COLLEGIS.

Additionally, the President responded that Florida law clearly states the College was not required to solicit proposals from other vendors providing similar services. Although the Florida Administrative Code exempts the College from the three-bid requirement, it does not prohibit it from soliciting bids or proposals from other vendors. The College incorrectly interprets our position to reflect that we believe the State of Florida promotes imprudent business practices. The Florida Statutes and the Florida Administrative Code establish minimum legal requirements, but do not necessarily address what is prudent in all circumstances. Notwithstanding the President's response, we believe that management's responsibility for the stewardship of College funds and resources dictates that it follow not only minimum legal requirements but also business

practices that are necessary in specific circumstances to ensure that College objectives are achieved in a cost-effective manner. In the circumstances described above, the College should have solicited proposals from other vendors providing similar services prior to entering into a contract with an initial cost of $12,998,000.

Furthermore, the President stated that the College engaged in a thorough and vigorous contract negotiation with COLLEGIS, which was documented by the General Counsel. In the course of our audit, we made a written request to the Vice President for Administrative Services for any materials that would show evidence of the contract negotiation process. We were not provided with the General Counsel's documentation to which the President refers in his response. Instead, the Vice President for Administrative Services responded in writing that the actual signed contract was the summation of the negotiations and that the College was not aware of anything else that could be furnished which had not already been requested or furnished.

Recommendation:

The College should ensure that information technology purchases are made in accordance with an approved long-range information resource technology plan and that proposals are solicited before the College enters into arrangements similar to the COLLEGIS contract so that the management and operation of technology resources will be based on the College's planned objectives and budget.

Finding No. 2:

The College has not enforced a contract provision with regard to COLLEGIS implementing the Oracle financial services and human resources/payroll systems. As a result, the College has incurred $233,833.50 in additional costs for Oracle consultants.

In May 1998, when the College chose to implement the Oracle financial services and human resources/payroll systems, the College indicated that its Executive Council did not believe the College had the capabilities in-house to implement the new administrative software it was acquiring and concluded that the College would save money by hiring COLLEGIS to both operate its data center and implement the software. The contract with COLLEGIS states that as of the effective date of the contract, June 18, 1998, COLLEGIS shall perform the services described in the contract and in Exhibits A and B of the contract. Exhibit A, Section III.A.1, of the contract (Migration Projects-Implement Financial Services and Human Resources Systems-COLLEGIS Responsibilities), states that COLLEGIS will "develop (a) detailed implementation project plan in consultation with (the) Client user implementation team" and "provide services related to Oracle application development, customization, Legacy interfaces, and database administration." Exhibit A, Section I.G.5 of the contract (COLLEGIS Responsibilities-Administrative Support Services), states that COLLEGIS will provide "database technology expertise to insure efficient database design, access, and operation." Exhibit A, Section III.A.1, of the contract (Migration Projects-Implement Financial Services and Human Resources Systems-Client Responsibilities), states that the College will "fund training, installation support and implementation consulting services as specified in the implementation project plan." A detailed implementation project plan, that would have specified additional consulting services costs to be paid by the College, was not developed.

Oracle Financials Implementation Project Update reports submitted by COLLEGIS to the College as well as minutes from Oracle project status meetings, during the period of December 2, 1998, through February 1, 1999, indicate that COLLEGIS attempted but failed to hire an employee with the necessary Oracle expertise to accomplish the implementation of the new Oracle financial services and human resources/payroll

systems. However, at the February 15, 1999, Oracle status meeting, COLLEGIS indicated that they had obtained the services of two experienced Oracle consultants from another vendor.

COLLEGIS paid for the services of these consultants from Abraxas Technologies for several weeks without reimbursement from the College. However, in April 1999, COLLEGIS began to bill the College for the invoices received from Abraxas Technologies. COLLEGIS submitted invoices to the College in June, July, August, and September 1999 for services provided by Abraxas Technologies during the months of April 1999 through August 1999. These invoices, which totaled $233,833.50, were paid to COLLEGIS by the College to reimburse COLLEGIS for five months of Oracle consulting services provided to the College. However, these services should have been provided by COLLEGIS, at no additional charge, as part of their scope of services according to the provisions of the contract previously cited.

While legal liability for the $233,833.50 in consulting fees paid by the College might be the subject of judicial determination, it is our position that the contract between the College and COLLEGIS implies an understanding between the parties that COLLEGIS had all of the expertise necessary to help the College implement its new Oracle administrative applications. Notwithstanding the President's response, we believe that the cost of any outside consultation should have been borne by COLLEGIS because it was not addressed in the implementation plan.

The contract with COLLEGIS appears to be a "form" contract and provides that COLLEGIS will assume all responsibilities for providing computer services to the College. As previously mentioned in the finding, provisions of the contract stipulate that COLLEGIS in consultation with the College will develop a detailed implementation plan; will provide services related to Oracle application development, customization, legacy interfaces, and database administration; and will provide database technology expertise to ensure efficient database design, access, and operation. An additional provision stipulates that the College will fund training, installation support and implementation consulting services as specified in the project implementation plan. A detailed project implementation plan was not prepared. In the absence of such a plan, which should have specified any additional cost requirements for the College, we found no other contractual provisions that would authorize payments by the College for Oracle consulting services. The construction or interpretation of a contract is necessary when the language of a contract is ambiguous or uncertain. Clearly, COLLEGIS' contract is ambiguous as it relates to who is responsible for the payment of consultants. It is a fundamental rule of contract law that doubtful language in a contract should be interpreted most strongly against the party who has selected that language. Since the contract was prepared by COLLEGIS, this rule of construction would argue that the College was not liable for consulting services. As a result, the College should seek reimbursement from COLLEGIS for the payments made for the Oracle consultants from Abraxas Technologies.

Recommendations:

The College should seek reimbursement from COLLEGIS for the payments made for the Oracle consultants from Abraxas Technologies. The College should also require COLLEGIS to provide technically proficient staff capable of providing adequate database technology expertise to ensure efficient database design, access, and operation, as specified within the scope of services under the contract.

Finding No. 3:

The College's draft Strategic Technology Plan for 2000-2004 does not include estimated costs and timelines to ensure feasibility and performance of the strategic objectives set forth in the plan.

Senior management should be responsible for developing and implementing long- and short-range plans that fulfill the organization's mission and goals. In this respect, senior management should ensure that information technology issues as well as opportunities are adequately assessed and reflected in the organization's long- and short-range plans. Information technology long-range plans supporting the achievement of the organization's overall mission and goals should regularly be developed. The plans should include cost and time guidelines.

Since September 1998, an external technology strategic planning consultant engaged by COLLEGIS has led the Educational Technology Committee, chaired by the Vice President for Administrative Services, in its development of a Strategic Technology Plan for 2000-2004. We reviewed a draft of this plan, which is presented in the form of "strategic objectives" with subordinate "strategies," and noted that it does not include anticipated funding amounts or dates. Under the heading "Restraining Forces," an introduction to the plan explains why the costs and timelines are not included: "There is no consistent framework for decision-making with regard to establishment of funding priorities for the acquisition and support of information technologies college-wide." Without costs and timelines, it is difficult to determine whether the strategies in the plan are feasible and cost-effective. As of December 6, 1999, College management indicated that the plan would be presented to the Board for approval in January 2000. As of June 22, 2000, the plan had not been approved by the Board. If the College does not adequately plan for the funding of its information technology needs, the College may later find that it cannot accomplish its strategic objectives.

Recommendation:

The College should include dollar amounts and time frames in its strategic technology plans so that subordinate short-range operational plans and budgets can be developed to accomplish the long-range goals and objectives of the College.

Finding No. 4:

The College has not performed certain provisions for which it is responsible in its contract with COLLEGIS. Additionally, the College is not adequately monitoring COLLEGIS' performance under the contract.

The contract with COLLEGIS places certain responsibilities on COLLEGIS and other responsibilities on the College. We performed a test of contract compliance with respect to both COLLEGIS and the College. Exhibit A of the contract contains 285 provisions. We judgmentally sampled 25 of these provisions. Of the 25 contract provisions we sampled, the College bore the entire responsibility for 4 and partial responsibility for 3. Of these, the College was deficient in compliance with 5. By contract, the College is to:

- "fund procurement and payment for hardware and software as part of approved Strategic Plan" per Exhibit A, Section II.A.2 of the contract. As previously discussed in finding No. 3, the Board has not approved the Strategic Technology Plan.
- "adopt a policy and procedures for receipt, storage, and documentation of information technology equipment and software" per Exhibit A, Section IV.F.2.a of the contract. The

College has not adopted these policies and standards. In a memorandum dated October 8, 1999, the College stated that its Educational Technology Committee has not yet met contract provision IV.F.2.a to "adopt a policy and procedures for receipt, storage, and documentation of information technology equipment and software" and that no special procedures have been approved for information technology assets.

- "approve standards for PC hardware and software" per Exhibit A, Section IV.H.2.b of the contract. The College has not approved these standards.
- "communicate Internet hardware and software standards to appropriate students, faculty, staff, administrators, and community members" per Exhibit A, Section IV.J.2.b of the contract. The College has not communicated these standards.
- although, according to Exhibit A, Section IV.C.1.a of the contract, COLLEGIS is to "prepare annual college-wide technology budget request in support of the Technology Strategic Plan and annual tactical plans," the College bears partial responsibility for this contract provision because COLLEGIS cannot prepare a budget request in support of the Technology Strategic Plan until such a plan is approved by the College.

Of the 25 contract provisions sampled for our test of contract compliance, COLLEGIS bore the entire responsibility for 18 and partial responsibility for 3. Of these, COLLEGIS was deficient in compliance with 4. By contract, COLLEGIS is to:

- ensure that "a response is made to requests for service within four hours of the initial call unless (the) caller requests a delayed response. At a minimum the initial response provides a confirmation of the receipt of (the) request and notification of the estimated time to completion of the requested service" per Exhibit A, Section VI.D.3.b of the contract. COLLEGIS is solely responsible for, but has yet to establish, procedures to determine whether there is a response to calls to the help desk within four hours and whether work on requests is being completed within agreed-upon time frames.
- "develop an annual Client technology tactical plan and budget" per Exhibit A, Section I.B.5 of the contract. COLLEGIS cannot develop these items in conformity with the Technology Strategic Plan until this plan is approved by the College.
- "prepare (an) annual college-wide technology budget request in support of the Technology Strategic Plan and annual tactical plans" per Exhibit A, Section IV.C.1.a of the contract. Again, COLLEGIS cannot prepare a budget request in support of the Technology Strategic Plan until the plan is approved by the College.
- "provide monthly network statistics for capacity planning and outcomes measurement" per Exhibit A, Section I.D.13 of the contract. COLLEGIS cannot provide these statistics because the College's network infrastructure is not currently capable of providing advanced performance measurement data.

Generally, the College has not formally established various plans, policies, procedures, and standards it agreed to establish in the contract. The approvals of these items would represent guidance from the College for the manner in which COLLEGIS performs its duties. When the College does not perform its responsibilities with regard to the contract, the risk exists that COLLEGIS could not be held accountable for performing other provisions that depend on them. When the College does not provide guidance to

COLLEGIS in the form of the required plans, policies, procedures, and standards, then COLLEGIS is in the position of making certain decisions that may not be in the best interests of the College.

Additionally, in managing third-party services, a continuous process for monitoring of the service delivery of the third party should be set up by management to ensure adherence to the contract agreements. Exhibit A, Sections II.B.3 and II.B.4 of the contract specify that the College's contract administrator is to work with COLLEGIS to develop annual "outcome measurements that are reasonable and attainable within existing staffing and funding levels" and the College is to "complete (the) outcome measurements and distribute (them) to (the) governance committee at least 60 days before the beginning of each fiscal year." In response to a request for annual outcome measures for the 1998-1999 and 1999-2000 fiscal years, College management provided us with the *COLLEGIS Annual Report to Valencia Community College for the year ended June 17, 1999* (dated July 17, 1999). This document provided a summary of objectives, initiatives, and outcome measures for the 1998-1999 fiscal year. Subsequently, the College developed *Proposed Deliverables and Outcome Measures for 1999-2000*; however, as of February 29, 2000, this document had not been distributed to the governance committee. When the College does not timely develop and monitor performance measurements, it risks failing to receive all of the services to which it is entitled under the contract.

Recommendations:

The College should develop and formally adopt the various plans, policies, procedures, and standards it committed to establish when it signed the contract with COLLEGIS. The College should also timely develop and monitor performance measurements that will ensure that all contracted services are provided.

Computer General Controls

The College has outsourced the management and operation of its Office of Information Technology to COLLEGIS. However, the College is ultimately responsible for ensuring that good computer general controls are in place. According to Exhibit A, Section I.B.22, of the contract with COLLEGIS, "the Client (the College) and COLLEGIS shall timely and effectively respond to audit recommendations and finds, and shall formulate and implement corrective action." Although the deficiencies identified in prior audit report No. 13398 existed prior to the contract with COLLEGIS, both the College and COLLEGIS are responsible for ensuring that corrective action has been taken with regard to these deficiencies.

Finding No. 5:

The College's information resources disaster recovery draft plan lacks key provisions, including a formal agreement with the back-up site and disaster recovery planning for the current client/server environment.

As organizations become more dependent on the computer to perform day-to-day business activities, the impact of system failures becomes more extensive. Disaster recovery planning should be based on a business impact analysis. Management can then determine the acceptable business risk and develop a disaster recovery plan to address the alternate processing of critical business applications. The plan should include responsibilities of user and information services staff. Back-up copies of critical files, programs, data, special forms, and documentation should be taken periodically and stored off-site. A back-up facility with compatible hardware and software may be appropriate. A reciprocal disaster recovery agreement should be made. For every service provided by information services, the business risk, acceptable business standards, and other factors must be assessed and procedures

developed to ensure that recovery is successful. The plan must be tested periodically, modified based on the test results, and continually maintained.

By Exhibit A, Section VI.C.1.h of the contract, COLLEGIS is required to ensure that "backup and disaster recovery processes have been implemented and tested." Although the College has not yet implemented an information resources disaster recovery plan, the *Proposed Deliverables and Outcome Measures for 1999-2000* indicates that COLLEGIS is to "Assist the College in the development and adoption of a formal, comprehensive disaster recovery plan to be completed by the end of calendar year 2000." As of December 6, 1999, COLLEGIS has prepared a draft plan that addresses the mainframe environment, but does not address the client/server environment. Since the College has installed new financial services and human resources/payroll client/server systems, the ability to recover the client/server environment following a disaster has become more important for the College.

Section 10 of the draft plan indicates that the College plans to use the Northeast Regional Data Center (NERDC) as a back-up site. This section also states that "ideally, this disaster recovery plan should be tested at least once a year." Although the legacy mainframe payroll system was most recently tested at NERDC on July 30, 1997, disaster recovery planning for the current human resources/payroll, financial services, and student applications has not been documented nor tested at an alternate site. Additionally, current information system configurations are not assessed on a regular basis in conjunction with planning for testing at an alternate site. The College may attempt to use NERDC as its alternate processing site in the event of a disaster; however, no written agreement with this or any other facility guaranteeing the availability of specified computer resources, such as equipment, processing time, and support personnel, under stated conditions has been developed and signed. Without a comprehensive information resources disaster recovery plan, the risk exists that failure to restore information technology services could cause undue hardship to the College, its vendors, and its students.

In that the College's disaster recovery plan with regard to the current client/server-based systems is still being developed, we will review the adequacy of the College's comprehensive disaster recovery plan in a future audit. While the College claims to have an "informal and reciprocal agreement with NERDC" for use as an alternative processing site in the event of a disaster, the College indicated to us in writing that no written agreement existed. The College implies that it is scheduling annual testing of its disaster recovery plan at NERDC. However, the College previously represented to us in writing that the legacy mainframe payroll system is the only system that has been tested at an off-site location and that this system was tested only once, on July 30, 1997. The College also stated in its written response to our original request for its disaster recovery plan that "recovery based on legacy systems would be obsolete now."

Recommendations:

To help ensure a smooth recovery in the event of an actual emergency, the College should continue to develop its disaster recovery plan giving consideration to the aforementioned provisions. The plan should also be tested at least annually.

Finding No. 6:

Deficiencies were noted with regard to systems development and maintenance controls. Specifically, the College's policies and procedures manual had not been updated to ensure that management directives were followed with regard to systems development and maintenance. Additionally, controls over the program change process needed improvement.

Each function in an organization needs complete, well-documented policies and procedures to describe the scope of the function, its activities, and the interrelationships with other departments. Sound policies and procedures provide benchmarks against which compliance can be measured and contribute to an effective control environment. Control activities are the policies and procedures that help ensure that management's directives are carried out. Additionally, user involvement, technical assistance, adequate system testing, and program transfer and documentation procedures should be in place to support a controlled systems development and maintenance environment.

By Exhibit A, Section IV.I.1.b of the contract, COLLEGIS is required to "document information technology policies and procedures in accordance with COLLEGIS standards." In addition, the following appears in the *Proposed Deliverables and Outcome Measures for 1999-2000* developed by the College and COLLEGIS: "Make recommendations for, and assist in the development of, standards, policies, and procedures through the College's IT governance structure." Although COLLEGIS is in the process of making the College's OIT policies and procedures current, final versions of these do not yet exist. There is not a set of formal standards promoting conformity with regard to the continued maintenance of the College's mainframe systems. The financial services and human resources/payroll systems are purchased client/server applications that the College has decided not to modify. However, procedures and documentation standards for implementing and testing the new systems, as well as making user changes to these systems' settings, have not been established.

Deficiencies noted regarding controls over the program change process included:

- The College was not effectively using its Programming Request form, which included a signature line for user acceptance of work performed. Users were verbally notified of work performed but were not required to provide an acceptance signature. There was also no evidence of systems analyst or supervisory review of the work completed by the programmer.
- The notification feature of help desk software, DK Systems, was not utilized to allow management to track program change requests and monitor the completion of requests to ensure that they were being completed within a reasonable timeframe.
- College management indicated that there was no documentation regarding a test plan or the actual testing of the new Oracle financial services application by the functional owner.
- The same programmer, who had modified a program, moved the program from the test area back to the production environment.
- A report was not routinely produced by SOURCE/Conversational Monitoring System (CMS), for supervisory review of programs moved into the production environment.

Lack of user and supervisory involvement in the program change process and failure to document testing of new and modified systems increase the risk that systems will not support the objectives of the entity, that

inaccurate or erroneous data will not be prevented from entering the system, and that the modifications will impair the functionality, usability, and performance of the system. Standards provide a measure for quality and consistency with which an entity's objectives are achieved. Without proper policies and procedures in place, management will have no benchmark to evaluate how well personnel are carrying out management's directives. In turn, personnel will not have the proper guidelines for their understanding of how they are to perform the duties that management has assigned to them.

Correspondence with the College regarding these control weaknesses, in a memorandum dated December 4, 1999, indicated that programmers are no longer allowed to move programs to the production environment and that a new system has been implemented to track programming requests. Per College management, their new system incorporates a sign-off process involving users, supervisors, and systems analysts. We will review the adequacy of the College's actions regarding the new controls over the program change process in a future audit.

Recommendation:

The College should complete and distribute current policies and procedures, related to systems development and maintenance, to personnel who require them in the performance of their duties.

Finding No. 7:

Deficiencies were noted with regard to access controls. Specifically, we noted the lack of an up-to-date policies and procedures manual with regard to system access; the lack of Internet usage policies; that an adequate security awareness program had not been implemented; inappropriate levels of systems access; and inadequate procedures over revocation of access rights for terminated employees.

Exhibit A, Section IV.I.1.b of the contract states that COLLEGIS is required to "document information technology policies and procedures in accordance with COLLEGIS standards." In addition, the following item appears in the *Proposed Deliverables and Outcome Measures for 1999-2000* developed by the College and COLLEGIS: "Develop a security and access control policy/plan and present the plan to the College's IT governance structure for approval and formal adoption." Furthermore, Exhibit A, Section IV.K.1.c of the contract states that COLLEGIS is required to "develop plans and recommend policies and procedures to provide appropriate security for system access and data integrity." As critical applications move to the client/server environment, security policies and procedures must incorporate rules, principles, and procedures that govern how the organization manages, protects, and controls information and resources of the client/server. Internet usage policies should be developed to protect the information resources of the College's networks and ensure that management's directives are carried out. Also, employee termination practices should address the timely deletion of assigned log-on ID and passwords to prohibit unauthorized system access.

During our review, we noted the following deficiencies:

- The College does not have an up-to-date policies and procedures manual with regard to system access in the client/server environment. Additionally, although certain aspects of system access control for the mainframe and computer room access have been addressed in the draft disaster recovery plan, the plan does not provide directives for authorization processes of information security access within the College, nor the assignment of responsibilities and definition of authority for the security administration positions.

COLLEGIS is in the process of making the College's OIT policies and procedures current; however, final versions of these do not yet exist.

- The College has not developed Internet usage policies to protect the information resources on its networks. In a memorandum dated September 24, 1999, the Vice President of Administrative Services stated that "Internet usage policies will be developed and approved through the College's IT governance structure (Ed-Tech)."
- The College has not implemented an adequate security awareness program for users that emphasizes the importance of security over the information for which the College is responsible. Additionally, there is no requirement that users, after receiving security awareness training, sign a security awareness/nondisclosure statement before they receive a user identification (ID) giving them access to the College's systems.
- All computer operators and application programmers retained full update capabilities to all mainframe production program libraries and data files defined to CMS, in addition to job control language (JCL) libraries defined in Interactive Computing Control Facility (ICCF) security. Computer operators had been given full access to JCL because of limitations in the VSE operating system. Additionally, the systems analyst for student systems maintained the ability to log on as a user with update capabilities to certain student financial aid application screens.
- Procedures regarding the notification of employment termination for part-time employees do not ensure the timely revocation of employees' access rights. At the time of employment termination, part-time employees are not required to have an Employee Checkout Sheet completed, which is used to request the termination of full-time employee access rights to system resources. Security administrators are supposed to be notified of the termination of part-time employees by memoranda from the terminated employees' departments; however, our review of the access capabilities for all OIT, Financial Services, and Financial Aid employees terminated during the period of July 1, 1998, through June 30, 1999, revealed that of the eight part-time and nine full-time employees reviewed, one part-time employee had terminated on September 30, 1998, but still had access on September 2, 1999 (337 days after termination).

The greatest risk related to information systems security is that the integrity, confidentiality, or availability of information systems data and resources may be compromised through inappropriate or unauthorized physical or logical access. As previously mentioned, without proper policies and procedures in place, management has no benchmark to evaluate how well personnel are carrying out management's directives. In a memorandum dated December 6, 1999, the College indicated that new policies and procedures were being implemented which limit programmer and operator access to production libraries. When systems analysts, programmers, and computer operators are allowed to access and update production programs and data, the risk exists that unauthorized modifications to programs, application data files, and/or the operating system will be made and not be detected in a timely manner. We will review the adequacy of the College's actions regarding the limitation of programmer and operator access in a future audit.

Recommendation:

The College should review the other deficiencies mentioned above and implement appropriate corrective action.

Finding No. 8:

The College has not established appropriate access control procedures regarding passwords.

An adequate password system that limits computer access to properly authenticated individuals is important for the security of the College's software and data. Passwords should be internally one-way encrypted. When a user logs on for the first time, the system should force a password change to improve confidentiality. Thereafter, the system should force periodic password changes. Additionally, the system should not permit the use of easily guessed passwords or the reuse of the immediately previous password at the time of a password change. Our review of access control procedures regarding passwords disclosed the following deficiencies:

- In the mainframe environment, there are not mandatory password changes for new users after their initial sign-on or when a security administrator has reset passwords, because, according to College management, none of the security systems-SISS, ICCF, and CICS-have the capability to force the user to change this base password on initial log-on or after the resetting of a password.
- With the exception of the ICCF security system on the mainframe, passwords are not expired by the security system to force user password changes on a periodic basis. According to College management, CICS and SISS do not have the capability to force user password changes on a periodic basis. Oracle applications have an option that can be set to require periodic changes, but the option is not set to require the change.
- A password verification program is not used to limit the recycling of user passwords or the use of easily compromised passwords.
- Passwords are not encrypted in the CICS mainframe security tables. Security administrators and contracted system programmers may browse the unencrypted passwords online or print them out.

Each of the password function weaknesses described above increases the risk that a password will be learned or guessed by another individual. In a memorandum dated December 6, 1999, the College responded that its Educational Technology Steering Committee would recommend a collegewide policy regarding password changes. We will review the adequacy of any password policies adopted in a future audit.

Recommendations:

Although the College has indicated that a requirement to change passwords could result in their being written down and perhaps in their being taped to PCs or the inside of desk drawers, the College should research the feasibility of implementing a security system on the mainframe with the capability of implementing the security parameters listed above. The College should also research their client/server environment to determine if there are features that can be used to correct the exposures listed above.

Finding No. 9

The College does not routinely use audit trails and logs to aid in the review and investigation of unauthorized access attempts to the College's information resources.

An entity that has important computer applications needs to ensure that the related software and data are protected from unauthorized and inappropriate access. For example, if an invalid password is entered a predefined number of times, the log-on ID should be automatically deactivated for a significant period of time. Procedures for reporting the occurrence of a security event should be established. The reports should be based either on the individual initiating the event or the data and resources affected by the event. Specific reports that should be generated and reviewed regularly by both security personnel and owners may include: attempted or actual access violations for data and resources; invalid log-on attempts; access to sensitive data and resources; access to data or resources by privileged users; and access modifications made by security personnel.

Our review indicates that security administrators and College administrators do not currently have procedures in place for the regular monitoring of system security. The mainframe security systems are limited in their recording and reporting of certain security events, limiting the ability of security administrators to monitor system activity for violations.

Computer operators monitor computer consoles for job completion activity. Console logs are set to record access to program libraries, data sets, tape files, disk files, database files, on-line applications, and system software commands. Operations personnel review console logs only when a problem arises. Reports detailing invalid access attempts are not printed and reviewed on a regular basis. According to College management, none of the security systems in place at the College, except ICCF, have any provisions to limit the number of invalid access attempts before suspending a user ID. Also, CICS, ICCF, and application security packages are limited in their ability to record security events beyond the reporting of dataset changes and terminal activity. Additionally, the mainframe security packages do not provide management with the ability to monitor unauthorized attempts to sign on to the system, unauthorized attempts to access system resources, and unauthorized attempts to view or change security definitions and rules.

Oracle applications provide for "alerts" that can be activated by the system to immediately notify appropriate staff by e-mail of questionable activity in the databases. Although the College is not yet using such alerts to provide information concerning activity in its financial services and human resources/payroll databases, the College indicated in a memorandum dated December 4, 1999, that it plans to do so as it gains more understanding of its systems.

The lack of review and monitoring functions puts the College at risk for undiscovered unauthorized access attempts or data file manipulation.

Recommendations:

Due to the previously disclosed deficiencies, in finding No.8, regarding password controls and access rights for terminated employees, the College should regularly review access violation reports so that unauthorized attempts to access computer programs and/or data will be discovered timely. If the current security packages do not allow this, the College should consider procuring a security product that could provide the security administrators with such reports. Additionally, the College should review Oracle alerts as a potential source of information to the College.

Prior Audit Findings

Findings this Audit: 9
Findings Prior Audit: 6
Repeat Findings: 3 (Nos. 5-7)

For those functions within the scope of this audit, the College has corrected the deficiencies noted in audit report No. 13398, except as noted in this report.

STATEMENT FROM AUDITED OFFICIAL

In accordance with the provisions of Section 11.45(7)(d), Florida Statutes, a list of audit findings and recommendations was submitted to the College. The President's written response to the audit findings and recommendations is included in its entirety as Appendix B.

Appendix A
Background

Information Technology Outsourcing

On June 17, 1998, the College outsourced the management and operation of its information technology functions to COLLEGIS, Inc., which staffs the College's Office of Information Technology. The contract agreement was for a five-year term, terminating on June 17, 2003, with the option to extend the term of the contract agreement for an additional two-year period. The contract provides for the College to pay COLLEGIS $12,998,000 over the first five years. The College would pay COLLEGIS $1,682,700 for each year of the optional two-year extension. In addition, the College has signed two addenda to the contract. Under the first, the College will pay COLLEGIS $1,078,000 over a period of four years, with an optional fifth year for an additional $269,500. Under the second, the College will pay COLLEGIS $210,000 a year for three personal computer specialists until June 30, 2003, or upon termination of the contract, whichever date is earlier. Therefore, it is anticipated that the College will pay COLLEGIS $14,916,000 in contract-related charges for the period of June 18, 1998, through June 17, 2003. If the College chooses to use the two-year extension on the original contract and the one-year extension on the first addendum, the College can anticipate paying COLLEGIS an additional $3,634,900, for a total of $18,550,900. Under the contract agreement, COLLEGIS' responsibilities include overseeing the development and implementation of COLLEGIS value-added programs; directing the implementation of the College's Strategic Technology Plan; providing on-site technical and support staff; maintaining efficiency of operations of the network infrastructure; managing telecommunications; and providing other related administrative support services. The College's responsibilities include establishing a Technology Governance Structure, funding and paying for hardware and software, providing computing facilities, training College staff in the use of the College's application software, and providing additional funding for COLLEGIS personnel in the event of a significant increase in the College's technology initiatives.

Major Systems

In July 1998, the College purchased new financial services and human resources/payroll systems from Oracle to replace systems that were 17 and 29 years old, respectively, and which were not Year 2000 compliant. In the fall of 1998, two implementation teams composed of user department staff and the financial user liaison began to work on the set-up of the new administrative systems. The Oracle financial services system went into production on July 1, 1999. The Oracle human resources/payroll system was implemented in parallel with the College's old payroll system on October 1, 1999. Final cutover to the new system occurred on January 1, 2000. A Sun Ultra 450 server hosts the Oracle financial services and human resources/payroll application and database systems.

The College's Student Information System, including student receivables, fee payments, and financial aid, runs on its International Business Machines, model 9672-R11, mainframe. The legacy finance and payroll systems will remain on this machine for historical purposes only for a limited period of time. The College is reviewing other student systems for possible purchase. It is anticipated that the new student system will be of the client/server type.

Appendix B
Statement from Audited Official

VALENCIA
Community College

August 29, 2000

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

Dear Mr. Monroe:

I am enclosing Valencia Community College's response to the preliminary and tentative audit findings and recommendations which may be included in a report to be prepared on the audit of the District Board of Trustees, Valencia Community College, for the period July 26, 1999, through February 29, 2000 and Selected College Actions taken through June 22, 2000.

Sincerely,

Sanford C. Shugart
President

/gs

Enclosure

P.O. Box 3028, Orlando, FL 32802-3028 • 407-299-5000, Suncom 339-0111

VALENCIA COMMUNITY COLLEGE
RESPONSE TO
PRELIMINARY AND TENTATIVE AUDIT FINDINGS
FOR THE PERIOD JULY 26, 1999, THROUGH FEBRUARY 29, 2000
AND
SELECTED COLLEGE ACTIONS TAKEN THROUGH JUNE 22, 2000

Finding No. 1:
The College contracted for the provision of information technology services with COLLEGIS without having a long-range information resource technology plan and without soliciting proposals from other vendors.

Recommendation:
The College should ensure that information technology purchases are made in accordance with an approved long-range information resource technology plan and that proposals are solicited before the College enters into arrangements similar to the COLLEGIS contract so that the management and operation of technology resources will be based on the College's planned objectives and budget.

Response:
It is the College's position that neither the Florida Statutes or the Florida Administrative Code required the College to bid the COLLEGIS contract or to enter into the COLLEGIS contract in accordance with a long-range information resource technology plan, and that the College has acted in compliance with the law and accepted business practices with regard to the COLLEGIS contract.

The COLLEGIS Contract Was Exempt from the Three-Bid Requirement
In their Preliminary and Tentative Audit Findings, the auditors stated that "State Board of Education Rule 6A-14.0734(2)(h), Florida Administrative Code, provides that the acquisition of information technology resources as defined in Section 282.303(13), Florida Statutes, is exempt from the three-bid requirement..." The findings further state, "[a]ccording to Section 282.303(13), Florida Statutes, information technology resources include data processing services and personnel, as well as hardware and software, communications, supplies, facility resources, maintenance, and training." The auditors correctly identify this provision, which clearly exempts the COLLEGIS contract from the three-bid requirement, as the scope of services forming the basis of the COLLEGIS contract encompasses the elements set forth in the statutory definition of "information technology resources."

The College's Long-Range Information Resource Technology Plan Was Not a Prerequisite to the COLLEGIS Contract
The auditors inaccurately quote the remainder of 6A-14.0734(2)(h) to read, "the acquisition shall be made in accordance with the College's Long-Range Information Resource Technology Plan." The erroneous implication created by this characterization of the rule is that it refers to the acquisition of information technology resources, which it does not. The accurate reading of the rule as enacted reveals that "[a]cquisitions *of data processing equipment or software* shall be made in accordance with the [C]ollege's Long-Range Information Resource Technology Plan." (emphasis added). The College's contract with COLLEGIS did not provide for the acquisition of data processing equipment

or software, and accordingly there was no requirement that the College's contract to acquire information technology resources be in accordance with or be based on the College's Long-Range Information Technology Resource Technology Plan. Ironically, the refinement of such a plan was made part of the scope of services of the COLLEGIS contract and was one of the bases for the College to enter into the agreement.

The College Followed Prudent Business Practices

The auditors take a strong position that "prudent business practices would suggest that College management should have solicited proposals from other vendors providing similar services," despite applicable Florida law that clearly states otherwise. To the extent that the auditors' position suggests that the State of Florida promotes imprudent business practices, and that the applicable Administrative Rule should be ignored, the College respectfully disagrees. It is the position of the College that it sought guidance from the State of Florida as to what constitutes prudent business practices in the acquisition of information technology resources, and found such guidance in the Florida Administrative Code - specifically in the form of an express exemption from the three-bid requirement for the provision of information technology resources, the exact subject matter of the COLLEGIS contract.

The College Engaged in a Thorough and Vigorous Contract Negotiation with COLLEGIS

The auditors state that "the Vice President for Administrative Services and the College's attorney negotiated a contract with COLLEGIS..." and "due to the lack of documentation of the negotiation process that produced the signed contract, we were unable to determine whether the contract negotiations were conducted in the best interests of the College." This statement implies that the auditors fully examined the negotiation process and that somehow Valencia and COLLEGIS did not engage in an arms-length, good faith contract negotiation, which is objectionable and simply not the case.

Had the auditors simply consulted the College's General Counsel during the course of their investigation on this issue, which inexplicably they did not, they would have discovered that in preparation for this contract negotiation, the College's General Counsel contacted attorneys nationwide to discuss matters involving the outsourcing of information technology services in general, and COLLEGIS specifically. Using the information gleaned from these contacts, publications and the internet, and several sample contracts gathered from institutions around the country, the College worked through successive draft contracts, in efforts to minimize institutional liability and maximize effectiveness and returns on its investment. General Counsel's documentation of the negotiation reveals the wide-ranging discussion, and the major differences between the first draft contract as presented by COLLEGIS and the final executed contract are evidence enough of the informed and intense contract negotiation as engaged in by the College.

Finding No. 2:

The College has not enforced a contract provision with regard to COLLEGIS implementing the Oracle financial services and human resources/payroll systems. As a result, the College has incurred $233,833.50 in additional costs for Oracle consultants.

Recommendations:
The College should seek reimbursement from COLLEGIS for the payments made for the Oracle consultants from Abraxas Technologies. The College should also require COLLEGIS to provide technically proficient staff capable of providing adequate database technology expertise to ensure efficient database design, access, and operation, as specified within the scope of services under the contract.

Response:
The College did enforce contract provisions with regard to COLLEGIS implementation of the Oracle administrative systems. This is documented by the fact that COLLEGIS did pay for consulting services without reimbursement from the College. In April 1999, COLLEGIS, INC. notified the College that the consultants hired from Abraxas Technologies and paid for by COLLEGIS, INC. were no longer needed for technical project coordination and management. The College concurred but based on experience with the consultants, strongly believed Abraxas could be of significant assistance to the College functional implementation team whose responsibilities are outside the deliverables of COLLEGIS. At that time, the College agreed to reimburse COLLEGIS, INC. for additional work by consultants to support the functional implementation teams. This process was later documented in Addendum #3. Even though these consultants were not specified in the project plan, it was clearly the intent of the College to fund these implementation consulting services, as provided by Section III (2) (c).

Finding No. 3:
The College's draft Strategic Technology Plan for 2000-2004 does not include estimated costs and timelines to ensure feasibility and performance of the strategic objectives set forth in the plan.

Recommendation:
The College should include dollar amounts and time frames in its strategic technology plans so that subordinate short-range operational plans and budgets can be developed to accomplish the long-range goals and objectives of the College.

Response:
The College will present to the District Board of Trustees, on September 19, 2000, an executive summary of the Educational Technology Plan which outlines the estimated costs and timelines of the strategic objectives set forth in the Plan. The executive summary is derived from the Educational Technology Plan approved by the Educational Technology Steering Committee on July 13, 2000.

Finding No. 4:
The College has not performed certain provisions for which it is responsible in its contract with COLLEGIS. Additionally, the College is not adequately monitoring COLLEGIS' performance under the contract.

Recommendations:
The College should develop and formally adopt the various plans, policies, procedures, and standards it committed to establish when it signed the contract with COLLEGIS. The College should also

timely develop and monitor performance measurements that will ensure that all contracted services are provided.

Response:
The effective date of the College's agreement with COLLEGIS, INC. commenced on June 18, 1998 and terminates the initial term at midnight on June 17, 2003. The College has the option to extend the term for an additional two (2) year period by giving notice to COLLEGIS six (6) months prior to the end of the initial term. At the time of the audit, the College had just completed year one (1) of the five (5) year initial term.

As previously discussed in the response to Finding No. 3, the College's Educational Technology Steering Committee approved the Plan on July 13, 2000. The executive summary derived from the Plan will be presented to the Board of Trustees at its regularly scheduled meeting on September 19, 2000. The summary will show the timelines and estimated costs to ensure feasibility and performance of the strategic objectives set forth in the Plan.

The Educational Technologies Committee reviewed the frameworks for adopting PC hardware and software standards, as well as internet hardware and software standards at its meeting of January 31, 2000. Campus and functional subcommittees were asked to review the frameworks and report to the Steering Committee. The Steering Committee is scheduled to meet on August 30, 2000, to further refine the frameworks. The College will finalize the Educational Plan by presentation to the Board of Trustees on September 1, 2000. The College will develop the outcome measures in a more timely manner and present them to the governance committee (the Educational Technology Steering Committee). It was not contemplated that all deliverables pursuant to the contract would be completed in the first year of the contract. The executive summary of the Educational Technology Plan contemplates completion of these policies during fiscal year 2001.

Finding No. 5:
The College's information resources disaster recovery draft plan lacks key provisions, including a formal agreement with the back-up site and disaster recovery planning for the current client/server environment.

Recommendations:
To help ensure a smooth recovery in the event of an actual emergency, the College should continue to develop its disaster recovery plan giving consideration to the aforementioned provisions. The plan should also be tested at least annually.

Response:
One component of a comprehensive disaster recovery plan specifies the responsibilities of the Office of Information Technology (OIT), whose mission is to establish and document processes and procedures to ensure the continuity of the College's business information resources in the event of a business disruption caused by a natural or man-made disaster. In the event of a disaster affecting any of the functional areas of the College, OIT serves as liaison between the functional area(s)

affected and other organizations providing major services. The following points are addressed for the development of a quality disaster recovery program:

- COLLEGIS has been working to assist the College in the development of a comprehensive disaster recovery plan during the past several months. In fiscal 1999-2000, a software package from Phoenix Disaster Recovery Planning was purchased and will assist in developing procedures and providing a repository for systems data. The procedures module aids in developing background, risk and approach for a disaster recovery plan. The database module will condense hardware, software, systems, personnel, team members, skills, suppliers and other information into a single manageable repository.

- Both COLLEGIS and the College have recognized the importance and need for a formal and comprehensive disaster recovery plan. The College's Educational Technology Plan supports this need and includes funding for the further formal development of this plan in the current fiscal year (2000-2001). It also recommends funding for the future maintenance and support of the plan for subsequent years (2001-2005).

- The College's existing disaster recovery plan is considerably more than a draft. It currently encompasses the mainframe environment and work has been started to include the client/server environment. A tape rotation schedule is in place providing daily, weekly and monthly backups of the data and operating systems and tapes are stored in various buildings in fire and waterproof safes.

- With regard to off-site facilities (hot sites), there is both an informal and reciprocal agreement with NERDC in Gainesville, Florida. This agreement also includes periodic testing of our disaster recovery plan, which is scheduled to occur on an annual basis. John Beevis from NERDC and Art Ward have made arrangements to conduct such a test during the fourth quarter of 2000. Additionally, there have been discussions with a local vendor, Central Data, to host data backups and to be a hot site for the College. At present back-up tapes are kept on campus in different buildings and are rotated based on an internally developed rotation schedule.

Finding No. 6:
Deficiencies were noted with regard to systems development and maintenance controls. Specifically, the College's policies and procedures manual had not been updated to ensure that management directives were followed with regard to systems development and maintenance. Additionally, controls over the program change process needed improvement.

Recommendation:
The College should complete and distribute current policies and procedures, related to systems development and maintenance, to personnel who require them in the performance of their duties.

Response:

Both the mainframe and client/server systems have been monitored within the Programming Request System (PRS), an OIT developed tool that assists management and programming personnel with evaluating, modifying, testing and deploying systems development and maintenance.

The Programming Request System (PRS) has been deployed to the end-user community for electronic entry and acceptance of programming requests. The PRS system enforces the approval, tracking, and user acceptance of all programming and change requests. This system electronically maintains audit trails for all requests from entry and approval through the acceptance and closure state. The end user, through either an electronic or written approval process, now officially accepts all requests. A senior programming staff member (technical supervisor) in conjunction with the functional representative conducts review of all work performed before final user acceptance.

Procedural and administrative training on the use of the PRS system was provided to the end-user community in March/April 2000. Attendee lists are kept on file.

The College's help desk utilizes DK Help software to collect and monitor incoming network/PC requests (trouble tickets) as separate entities from administrative systems programming and change requests. With regard to administrative systems, the DK Help notification feature has been replaced by the PRS system. The PRS system has a reporting function that reports statistics on the administrative systems, whereas the DK Help software produces statistics on PC/network requests.

In the mainframe system environment, SOURCE CMS provides secure program move procedures. Programming staff no longer move programs to the "production" environment. Operations administrators, who follow a process that separates all "moves to production" from the programming staff members, perform this task. On a monthly basis, a detail listing of all moves initiated within SOURCE CMS, categorized by month, is printed, reviewed, and kept in the tape library in Operations.

Finding No. 7:
Deficiencies were noted with regard to access controls. Specifically, we noted the lack of an up-to-date policies and procedures manual with regard to system access; the lack of Internet usage policies; that an adequate security awareness program had not been implemented; inappropriate levels of systems access; and inadequate procedures over revocation of access rights for terminated employees.

Recommendation:
The College should review the other deficiencies mentioned above and implement appropriate corrective action.

Response:
OIT is working with the College towards completion of an updated Policies and Procedures manual that encompasses all aspects of the College's systems and internal/external information exchange. A key component of this process is the involvement of the College's Educational Technologies Committee in the drafting, review and recommendation process for these policies. This committee is now actively working with OIT to draft and develop these policies for College approval, including

policies for passwords, security, email usage, and Internet usage.

Security Awareness as related to the mainframe systems and the responsibilities of the programming staff is addressed as follows:

- SOURCEC is now implemented completely. The product tracks all changes to source code under VM and VSE.

- As of February 2000 the system administrators are the only IT personnel to have the ability to move changed programs into production. The tracking of moves is monitored via the Programming Request System (PRS) and within the SOURCEC product.

- Accessibility to the administrative system data and functions allows the systems analyst to fully test development efforts thoroughly. End-users require that analysts "see what they see" for effective system resolution.

Security Awareness as related to employment and termination is addressed as follows:

- Human Resources does not currently include security awareness training nor a nondisclosure statement during employee orientation. OIT and HR have communicated regarding the updates needed for the new employee packet.

- Employee termination practices are as follows:

  a.) The Help Desk receives HR Form #21 "Employee Checkout Form" and deletes the client from GroupWise, Novell, Mainframe SISS and DK Help accounts.

  b.) In the event the employee was temporary or part-time help, we receive notification from the employee supervisor via email requesting for the accounts to be terminated as of a certain date. On that date we delete the accounts.

  c.) An automated system response is sent by Oracle to the Help Desk stating that the employee has terminated employment with the College Payroll Department. When that message is received, the "former" employee's access to electronic systems is terminated.

Finding No. 8:
The College has not established appropriate access control procedures regarding passwords.

Recommendations:
Although the College has indicated that a requirement to change passwords could result in their being written down and perhaps in their being taped to PCs or the inside of desk drawers, the College should research the feasibility of implementing a security system on the mainframe with the capability of implementing the security parameters listed above. The College should also research its client/server environment to determine if there are features that can be used to correct the exposures listed above.

Response:
The College's mainframe and client/server applications do provide for more robust password capabilities than are currently being utilized. However, activation and enforcement of such capabilities must be in response to a College accepted password/security policy. The College's Educational Technologies Committee is currently working to draft and recommend such a policy. Once approved, this policy will direct OIT on what password capabilities to activate within our mainframe and client/server systems.

Security and password capabilities of our existing systems are herein outlined:

Mainframe:

- The SISS logon does have the ability to be periodically changed; however, no formal policy is established. The concept has been presented to the end-user community but has not been accepted.
- At this time, only the programming and operations staff uses ICCF and there has never been the need to change passwords. If a staff member were to leave, the account and assigned libraries would be disabled, meaning the libraries would be transferred to another staff members' account.
- The CICS sign-on and password scheme is currently being investigated and is being addressed in the migration to the next release of VSE (2.4.1), which has a new security facility, plan and sign on. In the interim, IT is moving from the CSSN sign-on table to the Interactive interface control file to force the users to change passwords on a regular basis
- The Navigant contractors change passwords in VSE/CMS on a monthly basis. These same contractors are the sole owners of the system resources for VSE/CMS.

Oracle:

When a new user is created in Oracle, there is an option to initiate password expiration. The options are Days (the maximum number of days between password changes) and Accesses (the maximum allowed number of sign-ons to applications allowed between password changes). Due to the implementation activities and lack of an approved College password policy, this option has not yet been deployed.

Administrative Systems Access:

- Authorization of system access & password maintenance.
  The Help Desk receives a request from the Department Head or Designee to create an account for the new employee. At that time a call is entered into DKHelp and assigned to the appropriate staff member to create the account. Once the account has been created, OIT notifies the employee and their supervisor, via email, that the account has been created. Account administration is as follows:

    - Mainframe – SISS account and password created by Help Desk, mainframe/CSSN account and password created by mainframe systems programmers (Navigant). Password resets done by Help Desk as requested by employee.

- Novell/GroupWise – accounts and passwords created by on-site campus Network Technician. On-site Network Technician or Help Desk can reset passwords.
- NT – accounts and passwords created by On-site Network Technician. On-site Network Technician or Help Desk can reset passwords.

Finding No. 9:
The College does not routinely use audit trails and logs to aid in the review and investigation of unauthorized access attempts to the College's information resources.

Recommendations:
Due to the previously disclosed deficiencies, in Finding No. 8, regarding password controls and access rights for terminated employees, the College should regularly review access violation reports so that unauthorized attempts to access computer programs and/or data will be discovered timely. If the current security packages do not allow this, the College should consider procuring a security product that could provide the security administrators with such reports. Additionally, the College should review Oracle alerts as a potential source of information to the College.

Response:
The need to monitor unauthorized attempts on the Colleges data and systems has provided the framework for instituting the following security measures:

- The mainframe security system is indeed limited in both recording and reporting either violations or unauthorized access. IBM in the mainframe environment has addressed some of these issues with the release of the newest level of the operating system VSE/ESA version 2.4.1. The College is currently working to develop a plan for migration to this version of VSE/ESA.
- Additional security packages from outside vendors will even further address the College's ability to both monitor the system for unauthorized sign-on attempts and limit access to system resources. Security packages being evaluated are: Top Secret by CA, ALERT by BIM and an updated CSSN package by MacKinney.
- Currently, console logs and CICS journals for unauthorized activity and multiple invalid sign-on attempts are reviewed.
- OIT has instituted a secure network configuration that looks for security breeches both internally and externally. Netsonor, a CISCO network-monitoring product, examines each campus to determine if data or resources are compromised. Additionally, new firewall software is being installed that provides a better safeguard for data or resources.
- Oracle application software does provide a notification workflow component called Oracle Alerts. This product is being used for notification in other module areas, such as purchasing. The College will implement the Alert product for security and password applications as the end-user community gains more familiarity with the system and as the College adopts formal security and password policies and procedures.