JANUARY 2002 REPORT NO. 02-133

AUDITOR GENERAL

WILLIAM O. MONROE, CPA

SPECIAL REPORT ON THE INFORMATION TECHNOLOGY INFRASTRUCTURE OF FLORIDA EDUCATIONAL ENTITIES

Summary

We conducted a survey of the educational entities in the State of Florida, which included all district school boards, community colleges, and universities. The survey was composed of specific technology-related questions. Entity responses to the survey were received between April and May 2001. Responses to selected questions from the survey were confirmed with the entities in July 2001 and used in the preparation of this report.

The survey responses indicated that many varied and, in some cases, potentially deficient information technology (IT) control practices were being followed by Florida educational entities. In addition, constitutional and statutory changes establishing a new governance model for Florida's educational system have created uncertainty as to future information technology requirements. New Federal regulations related to personal health information could also have a significant impact on educational entities, particularly in the area of IT.

The Department of Education (Department) should promote sound IT business practices among the entities, and, where appropriate, facilitate educational system-wide solutions to IT problems. To assist in the formation of sound IT practices, the Department should consider utilizing the State Technology Office (STO) as a resource for information, particularly with respect to enterprise IT practices and solutions. Areas in which the Department is in a good position to promote, encourage, and facilitate good information technology management include:

- *Long-range IT planning*
- *IT security*
- *Use and control of emerging technologies*
- *Acquisitions of application systems*
- *Ensuring compliance with new legal requirements*

We also noted a need for Legislative action regarding certain provisions of Chapter 282, Florida Statutes, as they relate to information technology functions of Florida's education system. Specifically, Chapter 282, Florida Statutes, needs updating to accommodate the governance structure changes provided in Chapter 229, Florida Statutes.

Background:

Florida educational entities, as defined in our report, encompassed the 67 district school boards, 28 community colleges, and 10 universities, for a total of 105 entities.[1] Each educational entity supported a unique technology infrastructure with selected district school boards, community colleges and universities supplementing their technology base through the use of software consortia, regional data centers, and software/data center consortia.

[1] New College was governed by the University of South Florida during the survey period and not considered an independent institution.

In 1998, Florida voters approved changes to Article IX, Section 2 of the State Constitution, mandating the creation of a new public education governance system led by an appointed State Board of Education. On July 1, 2001, the Secretary of Education and the Florida Board of Education (Board) assumed control of Florida's educational system. Under the new legislation, the Department of Education acts as an administrative and supervisory agency under the policy direction of the Board.

Pursuant to Section 229.0073(5)(a), Florida Statutes, created by Chapter 2001-170, Section 11, Laws of Florida, the Office of Technology and Information Services is in the process of being established within the Department. The Office of Technology and Information Services, in conjunction with Chancellors of Public Schools, Community Colleges, and Colleges and Universities, is charged with developing a systemwide technology plan, making budget recommendations to the Commissioner of Education, providing data collection and management for the system, and coordinating services with other agencies, among other things.

Responses to our survey disclosed that information technology structures within educational entities included a diverse set of technologies that performed financial, student, and support services. Data processing equipment ranged from large mainframe units to mini computers to clusters of servers performing individual tasks to support a client/server environment. Educational entities also supported multiple types of operating systems. Entities reported over 13 different production server operating systems. Survey results also revealed entities maintained over eight unique client/workstation operating systems.

Our survey identified, by vendor, hardware and software being maintained by the educational entities. (See Attachment A.) Figure 1 details the machine types used to host production applications and databases (finance, payroll, human resources, and student applications). IBM products have been broken out due to the distinct differences in machine architectures. Figure 2 details the types of operating systems used on the production servers. Figure 3 provides information regarding the client/workstation operating systems. Percentages presented for each individual item in the charts represent a percentage to total hardware or software deployed.

Survey Results

Overall, our survey indicated there is a need for the promotion of best IT practices among Florida educational entities. Survey responses reported many varied, and in some cases, potentially deficient control practices being followed, particularly in the areas of information technology security and procurement.

We believe the Department is well positioned to serve as a resource for educational entities in identifying appropriate business practices in the acquisition, operation, use, and safeguarding of information technology. The Department should, as appropriate, use the STO as a resource for information on enterprise IT practices and solutions. Areas of IT management where the Department should play a role in facilitating improvement are discussed in the following paragraphs.

Planning Framework:

Certain entities did not maintain a long-range information technology plan.

An important tool in the maintenance of a technology infrastructure is the creation of a long-range information technology plan. The plan should include technological direction and migration strategies for the systems architecture. Long-range plans should be modified on a periodic basis to include new technology innovations or internal initiatives taken to change current technology structures.

Our survey disclosed that 11 of the 105 educational entities did not maintain a formal long-range technology plan.

Security Practices:

Numerous entity responses indicated a need for improvement in various IT security practices to enhance the protection of data and information resources from unauthorized disclosure or use.

Systems security can be defined as the safeguarding of all components within a network including data, applications, and hardware resources. Properly implemented and monitored systems security reduces the risk of improper access to system resources and strengthens the privacy, availability, and integrity of data assets. As educational entities have opened their networks with new technologies, the inherent risk of unauthorized access to system resources has increased making the process of securing networks progressively more complex.

Threats to educational entity data assets can originate not only from outside sources (such as unethical hackers), but also from internal sources including disgruntled employees, employees with access rights that do not match their job functions, and mischievous employees exploiting and compromising internal systems and networks. New data system access points (Internet, wireless networks, Web enabled applications) increase the inherent risk of security violations. Another inherent security risk faced by entities is the possibility of unauthorized use of their data processing technology that could result in litigation. Such unauthorized actions include the use of data center assets to spread a computer virus, unauthorized use of data center assets to launch or assist in denial of service attacks directed at external Web sites, and the unauthorized public disclosure of student and staff confidential information. To counter these new risks, entities should maintain a dynamic multidimensional approach to security to provide appropriate security, privacy, and availability of their data, applications, and networks.

A multidimensional approach includes supplementing basic data center hardware and application security controls with increased monitoring of systems by data center personnel, as well as continuously educating end-users and data center personnel on systems security. All users should also be provided with defined and enforced security policies, usage policies, and security procedures.

The System Administration, Networking, and Security Institute (SANS), is a cooperative research and education organization through which more than 96,000 system administrators, security professionals, and network administrators share security alerts and news, research network security topics, and provide certifications for security professionals. Through its research, SANS recommends a security model built upon the following layers:

1. Security policy of the organization
2. Host (individual servers) system security
3. Auditing
4. Router security
5. Firewalls
6. Intrusion detection systems
7. Incident response plan

In an environment where researchers and hackers discover security vulnerabilities in application software, network equipment, and operating system software virtually every day, complacency in actively managing security is something educational entities cannot afford.

Survey responses indicated a need for improved security practices at various entities. Specifically:

- 86 of 105 educational entities did not have a formal written risk assessment of their critical systems or applications running on those systems. Formal system risk assessments of applications and network infrastructure can facilitate better security by identifying security risks, determining their magnitude, identifying areas needing safeguards, and determining methods to safeguard identified areas.

- 19 of 105 educational entities did not maintain current diagrams of their network equipment to assist in developing and maintaining security solutions.

- 44 of 105 educational entities did not maintain current Information Technology Policies and Procedures manuals. Well-defined policies and procedures are essential in communicating management's expectations for all aspects of the information technology function, but especially in the area of IT security. To be most effective, policies and procedures should be documented in writing, disseminated to all individuals to which they apply, and revised as appropriate to maintain applicability in the dynamic IT environment.

- Electronically recorded or physically signed end-user agreements were not always maintained. Specifically:

  - 40 of 105 educational entities did not maintain signed end-user agreements for acceptable use of entity network assets,

  - 23 of 105 educational entities did not maintain signed end-user agreements for Internet usage policies,

  - 50 of 105 educational entities did not maintain signed end-user agreements for authorized E-mail usage guidelines.

  End-user agreements require a written acknowledgment by the users that they understand and agree to comply with policies regarding acceptable use of information resources. For example, well-defined user agreements and policies and procedures on password security can provide a line of defense from social engineering attacks. Social engineering involves the low-tech manipulation of network administrators and end-users to obtain information that can be used to break down network security. Methods include contacting end-users by telephone and impersonating a network administrator, requesting the users verify their ID and password. In the absence of such agreements, management's assurance may be limited that security policies and procedures have been effectively communicated to the users.

- 17 of 105 educational entities did not maintain firewalls at their data centers. A firewall is a device or program designed to filter data traffic into and out of a trusted internal network from an untrusted source such as an Internet connection by the administration of access control rules. Firewalls may also have the ability to control application activities such as the sending and receiving of E-mail, file transfers over the Internet, and Internet access operations. To be effective, firewalls require the creation and maintenance of adequate rule sets that define accepted network activity in addition to consistent and competent monitoring of logs to detect and respond to possible unauthorized activities. Firewalls should be deployed between any connection by an outside source, such as wireless access points, direct connections to outside sources such as city or county data centers, and any access points to Internet service providers. Therefore, a data center may be required to maintain multiple firewalls to adequately protect their internal trusted networks. Failure to secure servers behind firewalls increases the risk of unauthorized access from external sources.

- 27 of 105 educational entities did not maintain host-based antivirus software, while 5 did not maintain client/workstation-based antivirus software. Antivirus software applications are used to detect computer viruses on host or client/workstations and quarantine or eradicate the virus files upon discovery. To protect servers and networks from virus activity, host antivirus applications are deployed on firewall servers, Gateway servers, and E-mail servers. E-mail servers, using a host-based antivirus application, may have the capability of also filtering E-mails for attachments that can contain viruses such as W97.Melissa.A and VBS.LoveLetter viruses and quarantine the attachment, preventing it from reaching a workstation. Workstation-based antivirus programs protect a user's machine from viruses that could be delivered from the network, floppy drive, Compact Disk, Personal Digital Assistant (PDA), or other input device. Failure to provide antivirus software to critical network machines and client/workstations increases the risk of a virus infiltrating network resources.

- 29 of 105 educational entities did not maintain alternate site provisions to provide backup processing of critical applications in the event of a disruption of service in their data centers. Disaster recovery is the ability of an entity to respond to an interruption in services by implementing a plan to restore an organization's critical business functions. Entities may maintain backup processing facilities by contracting for alternate site services with third party vendors, using alternate data processing facilities within the entity's organization, backup plans by regional data centers and consortia, and the use of formal and informal reciprocal agreements. A reciprocal agreement engages two organizations with compatible computer configurations allowing either organization to utilize the other's excess processing capacity in the event of a disaster.

Emerging Technologies:

Educational entities may need guidance in the use of emerging technologies that represent potential new security tools or security risks.

Emerging technologies represent new application and hardware technologies being implemented or under consideration for implementation by educational entities. While some emerging technologies such as Intrusion Detection System software can aid in maintaining system security, other technologies including Internet Protocol (IP) Telephony, wireless networks, and PDAs are creating new challenges for systems security. The new challenges include the need for new policies and procedures to maintain control over these technologies, increased system monitoring by entity management and staff to detect unauthorized access, and physical controls such as additional firewall and encryption technologies to protect entity data.

Examples of emerging technologies that entities were using or planning to employ include:

- 28 of 105 educational entities maintained some type of Intrusion Detection Software. An Intrusion Detection System (IDS) is a software program designed to dynamically detect inappropriate, incorrect, or anomalous activity on hosts (individual servers) and networks. IDS functions include monitoring and reporting user and system activity, auditing system configurations and vulnerabilities, checking file integrity, using statistical analysis and attack-pattern recognition, and auditing user activity for policy violations. A host IDS can be deployed on network servers including firewall, database, and Web servers to monitor network traffic into the host including connection attempts. A network IDS principally operates by monitoring network traffic through a network interface card placed in a particular segment of the network to be analyzed.
- 27 of 105 educational entities had deployed or were evaluating the installation of an IP Telephone system. IP telephony, or Voice over IP (VOIP), is the transportation of voice communications over a data network allowing many educational entities to take advantage of their network infrastructures and the Internet and bypass local telephone services. IP telephone systems can encompass transmission of voice communications within the closed voice and data network of an entity, communication to

other IP telephones on the Internet, or communication to phones on a traditional circuit switched network.

There are three principal security issues concerning VOIP:

- Authentication - When a call is placed, has the call reached the desired destination without being diverted to an unintended receiver?
- Nonrepudiation - When a call has been made, is the connection logged to substantiate the receipt of the call (such that the receiver of the call cannot refute the receipt of the call)?
- Accuracy - Was the call secure from the sender to the receiver of the call without being intercepted and possibly altered before being completed to the intended receiver?

- 63 of 105 educational entities have deployed or are planning to deploy a wireless network system. Wireless Wide Area Networks (WWAN), Wireless Local Area Networks (WLAN) and Personal Area Networks (PAN) provide network connectivity over a limited physical area with the use of radio waves, microwaves or infrared light. Most of the security threats applicable to a wired environment also pose a risk to the wireless environment. Additional threats that are unique to the wireless environment are:
  - Eavesdropping - Current WLANs use frequencies and transceiver powers that allow an unauthorized user the capability to intercept and view unencrypted data transfers outside the building, unless there exists some kind of electromagnetic shielding.
  - Transitive Trust - The ability for a perpetrator to set up a false wireless access point that is used to acquire user IDs and passwords when their wireless device attempts to logon to the unauthorized wireless access point.
  - Denial of Service - Due to the nature of the radio transmission, WLANs are very vulnerable against denial of service attacks. Attackers can jam all the radio communications of a WLAN with a high-powered transceiver or by using incompatible wireless devices in the same area as the WLAN.

  In addition to the unique vulnerabilities presented above, wireless protocols that allow devices such as laptop computers to communicate to a wireless access point on a traditional wired network such as 802.11b and Bluetooth represent relatively new technologies. Since the principal purpose of these protocols was to facilitate the mobility and easy access of users, they were not developed with strong security and user authentication options found in a traditional wired network. Specifically, installing a wireless access point with the default security settings represents a significant security risk to the wired network assets due to the ease in which unauthorized users can breach wireless security.

- 46 of 105 educational entities either officially or unofficially permitted PDAs on network resources. PDAs pose a new threat to network security when users synchronize data between their handheld devices and desktop or laptop computers connected to an entity's network. The synchronization process involves the two-way transfer of data between the PDA and the computer connected to the entity network via a docking station linked to a personal computer or via an infrared connection to the personal computer. PDAs may also access networks through the use of a modem. With the growth of PDAs used to access networks, virus writers and other hackers have begun to direct some of their attention on this comparatively easy unsecured target. Viruses for the Palm Operating System (PalmOS) devices were discovered in September 2000 and this finding signaled a new method to breach network security systems. PDA virus or worm programs could be transmitted by active Web content including ActiveX, Java scripts and executable programs when handhelds are synchronized to a networked computer where significant damage can be done. The large base of shareware and freeware programs for PDAs also increases the chance of obtaining programs with destructive code due to the open source nature of these programs and corresponding lack of controls to prevent alteration of files in the public domain. A current defense against the transfer of destructive material from handhelds to network computers includes the installation of PDA-specific antivirus programs on the networked computer to screen all data transfers from the PDA to the user's computer. When PDAs are used within an entity to obtain or manipulate confidential data, other security issues surface. PDAs operating under certain versions of the PalmOS contain an access back door available to anyone with software applications used by developers to create Palm applications. The developer application allows a person to bypass any password controls to access data stored on the PDA.

Recommendations:

Overall, there is a need for the promotion of best practices on a Statewide basis. The new educational governance model provides an opportunity for the State to create a resource pool which could be made available to educational entities Statewide. The Office of Technology and Information Services has been created to manage technology issues under the Department. Within the Office of Technology and Information Services, an Educational Purchasing and Information Center (EPIC) should be established that would aggregate current entity infrastructure information on all educational entities and provide a basis for promoting and assisting in the establishment of best IT business practices by educational entities. To help facilitate improvements in the areas of concern noted above, EPIC should work with entity management to promote, encourage, and provide guidance in sound IT business practices in the following areas:

- **Long-Range Technology Planning. Future hardware and software technology requirements should be examined and this information used to develop long-range technology plans to guide future technology purchases. Long-range plans should examine the entity's supported technology base to determine if provisions to consolidate the number of supported systems can be accomplished to reduce costs associated with maintaining multiple platforms and operating system software.**

- **Risk Assessment. All entities should maintain a regular risk assessment framework. The framework should incorporate a regular assessment of relevant information technology risks to the achievement of business objectives. The risk assessment should incorporate both a global view and individual system views, including network system diagrams to aid in determining system risks. Entities should use the completed risk assessments and network diagrams to define controls and security measures to mitigate exposure to risks on a continuing basis.**

- **Network Diagrams. Accurate network diagrams, or logical layouts of the network, assist security personnel in determining how to secure access points into their networks.**

- **Policies and Procedures. Information technology policies and procedures should** be created and maintained. It is the duty of entity management to formulate, develop, document, and disseminate controlling policies and procedures (covering topics such as security configuration standards, connection of devices to the network and the Internet, and procedures for granting and terminating users' access to system resources, among other things). The policies and procedures should be reviewed and updated periodically to maintain relevance.

- <u>End-User Agreements</u>. End-user agreements should be prepared and reviewed by legal staff to ensure their completeness. The agreements should cover guidelines for use of entity network assets, the Internet, and E-mail usage. Entities should record user acknowledgement of receipt and understanding by either a signature or in an electronic format. The agreements should be a component of security principles and awareness training provided to end-users.

- <u>Firewalls</u>. Properly maintained and configured firewalls are vital components of a security structure to defend against unauthorized intrusions from outside connections. Since all educational entities maintain connections to external networks, firewall systems should be deployed in all entities to assist in protecting internal trusted networks. Network systems not maintaining firewalls put the data assets of the entity at great risk for unauthorized access and increase the possibility of a disruption of service to users through attacks on system assets by unauthorized individuals or groups.

- <u>Antivirus Software</u>. Due to the easy ability to deliver viruses over the Internet, through E-mail, and over Wide Area Networks, educational entities should fully deploy antivirus software on host and client/workstations to defend network assets. Procedures should also be in place to continuously update antivirus software to maintain current virus definitions that offer a defense against attacks by new viruses. Entities should also examine the use of technologies available to push updated virus definitions and antivirus program updates to client and host machines from a central source in the information technology department. This would eliminate the process of manually updating each machine or relying on the individual user to institute the updates reducing the chances that all machines do not have the latest antivirus configuration.

- <u>Disaster Recovery - Alternate Processing Facilities</u>. Florida had 59 reported hurricane and tropical storm events between January 1994 and December 2000, resulting in over two billion dollars in property damage. Due to Florida's susceptibility to severe weather, all educational entities should maintain adequate disaster recovery plans, including either reciprocal agreements with outside entities, adequate alternate sites within their own campuses, or vendor contracts for alternate sites for processing critical applications. Entities should also conduct periodic testing at alternate sites, as needed, to ensure compatibility of equipment and validation of disaster recovery plan procedures.

- <u>Intrusion Detection Systems</u>. Due to the interconnected nature of entity networks, all entities should examine the prospect of installing IDSs to protect the integrity of network and host systems. While IDSs are reactive and display network attacks in progress rather than proactively preventing attacks, IDSs with properly instituted procedures to monitor, analyze, and respond to alerts, provide an extra layer of protection over critical data center assets in the event other measures such as firewalls are breached.

- Internet Protocol Telephony (or VOIP). Users of VOIP should examine their systems to ensure they provide a secure environment for voice communications. Entities exploring the use of VOIP should make sure their planned installations support encryption protocols to ensure the security of voice traffic, including the use of VPNs or related technologies if voice traffic will be channeled over the Internet.

- Wireless Networks. While wireless networks provide mobility for staff and student users, they also increase security risks for unauthorized access or the delivery of virus type programs to network resources. All entities deploying wireless networks should properly configure their systems to lessen the chance of unauthorized access including the deployment of VPNs and firewalls. Failure to encrypt data transmissions and the absence of a firewall defense provides eavesdroppers and intruders easier access to penetrate production systems over network resources. Entities should also enact security policies that discourage the installation of wireless networks by system users without the approval of appropriate information technology staff or management. Unauthorized wireless networks usually do not have the security measures in place to prevent unauthorized access to system resources including the bypassing of firewalls.

- Personal Digital Assistants. All entities should create policies defining the acceptable use of PDAs on data network equipment. Additionally, entities supporting the use of PDAs should equip all personal computers, capable of logging on an entity's network and used to synchronize with PDAs, with antivirus software to filter the transfer of files between units. The antivirus software should be updated continuously to obtain new PDA virus/worm or trojan definitions. Entities should also explore the use of enterprise software that centralizes PDA management and synchronization with Exchange-based E-mail and other applications. Furthermore, any entities allowing the synchronization of confidential information to PDAs should install appropriate third party security software such as data encryption on those devices.

The Department should, through EPIC, assist educational entities in the creation and maintenance of information security strategies. EPIC could serve as a principal point of contact and coordination for entity security personnel by accumulating and distributing computer security information and alerts, perhaps via a Web portal devoted to security issues. The Web portal could aggregate selected security issues and content similar to the myFlorida.com portal, which centralizes State government activities for Floridians. The security portal would need to be restricted to entity representatives actively managing security for the institutions similar to an internal Intranet.

EPIC could also host a statewide Computer Incident Response Team (CIRT) to react to security breaches and assist educational entities when requested. Duties of the CIRT might include:

- Documenting the priority and sequence of actions to be taken when dealing with an intrusion.

- Developing policy to indicate what types of intrusion response actions require management approval and which are pre-approved.

- Organizing the structure and staffing of the CIRT.

- **Creating policies to guide CIRT actions concerning intrusions, including reacting to the intrusion; communicating the intrusion to necessary parties; collecting intrusion evidence that meets the preservation of evidence required by local law enforcement and the Federal Bureau of Investigation; taking steps to eliminate the ability of the intruder to access system resources; implementing recovery provisions; and reviewing the intrusion to determine if current policies and procedures need adjustment.**

- **Developing responses to handle intrusions, including configuring redundant equipment to preserve the compromised machine for further study and for the preservation of evidence should there be legal proceedings.**

- **Having legal staff review policies and procedures pertaining to CIRT activities to ensure they are legally defensible and enforceable, reflect current overall organizational policies and procedures, and reflect best practices in exercising due care.**

- **Providing constant training to CIRT team members.**

The Department should further consider the following means to assist in the deployment of good IT security practices:

- **To assist the CIRT team, joining organizations such as InfraGard. InfraGard is an information sharing and analysis effort, serving the interests and combining the knowledge base of a wide range of members. At its most fundamental level, InfraGard is a shared undertaking between the United States Government (led by the Federal Bureau of Investigation and the National Information Protection Center) and an association of businesses, academic institutions, State and local law enforcement agencies, and other participants dedicated to increasing the security of critical infrastructures within the United States.**

- **Through EPIC, developing template documents representing security "Best Practices," detailing the process of conducting a risk analysis, documenting network topologies, creating shell end-user agreements, and shell documents for information technology policy and procedures manuals. By converting these items into a database available to all entities, the Department could allow an entity to access the database and create a "living document" that meets the entity's specific requirements. This information could be made available to all entities from the security web portal with provisions in place to keep the content current.**

- **Hosting and moderating a K-20 security discussion group on the Web portal to consolidate security information such that it is available in a seamless fashion to all entities regardless of the type of student they service.**

Acquisitions of Application Systems

As application technologies for student information, human resources, financial, and purchasing systems are implemented, replaced, or updated, there are basic objectives that all entities face in this process. These objectives include creating and maintaining enterprise systems that are secure, robust, intuitive, powerful, efficient, and transparent to users. Trends that will drive this process include not only the ability to provide access and active processing of student information over the Internet, but also the desire to develop and implement Internet accessible human resources, financial, and purchasing services. To accomplish these goals, many educational entities have implemented or intend to implement Enterprise Resource Planning (ERP) software. ERP software represents multi-module applications that support a broad range of activities (finance, payroll, human resources, etc.) using an integrated database to store data.

As of June 2001, Department and Board technology leaders for public schools, community colleges, and universities indicated they did not have a full understanding of the changes that may be dictated by the Office of Technology and Information Services over technology acquisitions within their areas of responsibilities.

Department and Board technology leaders further stated that the independent structures of district school boards and community colleges may limit the type of control the new office will have over their purchasing decisions. State University System representatives were in the process of evaluating a change from State agency to a non- State agency status. A change to non-State agency status would require the universities to manage payroll and other financial functions now performed by the Florida Department of Banking and Finance.

Universities:

The impact of the new educational governance model on the legal status of the universities had not been established. However, all universities were in varying states of acquiring or enhancing financial application systems.

In the university sector, technology purchasing trends may be dictated by the status of the institutions within the State government system. Currently the public universities use the functions of the Florida Accounting Information Resource (FLAIR) Subsystem for accounting and payroll. Additionally, the State continues to maintain possession of all non-local funds managed by the State universities. In connection with the new education governance model, Department and Board officials anticipated that the universities could be legislated as "body corporate," and will no longer be legally considered State agencies. If they become "body corporate," the universities will no longer fall under the State treasury and must assume the accounting and payroll functions now performed by the Department of Banking and Finance through FLAIR. During meetings held for university Information Resource Managers in May 2001, each institution detailed early plans to provide the technology and applications needed to process transactions now provided by the Department of Banking and Finance should their status change. Proposed solutions included the installation of ERP software, expanding the use of software currently deployed, development of solutions within a consortium of institutions, and outsourcing activities. Transactions that would be the responsibility of the universities include, but are not limited to:

- Payroll Processing and Tax Reporting
- Accounting and Financial Reporting
- Treasury Management and Investment
- Bonding
- Insurance and Risk Management
- Employee Insurance Benefits

Any solution provided would have to present a common financial management information-reporting format for budgetary purposes and for reporting as a component unit within the State's Comprehensive Annual Financial Report.

The universities had not received State funding to purchase new systems or system upgrades to process transactions should they be required to provide services performed currently by the Department of Banking and Finance. Section 215.93(2), Florida Statutes, prohibits State agencies from the creation of financial management systems that duplicate the systems provided by the Florida Financial Management Information System (FFMIS). An exemption must be granted from the Financial Management Information Board upon the recommendation of the FFMIS Coordinating Council to proceed with development of any information systems duplicating FFMIS services.

During the FFMIS Coordinating Council meeting in August 2001, a representative from the University of South Florida (USF) presented plans for implementation of an ERP system to provide transaction processing for accounting activities now processed through the State accounting system. After the presentation, a motion was presented and approved by the Council to allow an exemption pursuant to Section 215.93, Florida Statutes, granting USF the right to acquire and implement the required software to perform accounting functions now provided by the State. The Council approved the motion and placed it as an agenda item for the Financial Management Information Board (Governor, Comptroller, and Treasurer). On August 28, 2001, the Financial Management Information Board approved the motion and also delegated authority to the FFMIS Coordinating Council to approve exemptions for the other universities when requests to purchase and install financial management systems are received.

Survey responses and subsequent observations of planning sessions relating to future application acquisitions indicated all universities were in the process of planning, purchasing, or activating software to meet the expected transaction process currently accomplished by the FLAIR Subsystem. Specifically, for the replacement of functionality provided by the FLAIR Payroll Component:

- 2 of 10 universities were in the process of activating modules within currently running application suites.
- 5 of 10 universities were examining ERP solutions
- 3 of 10 universities were creating a consortium to examine a coordinated solution.

For the replacement of financial accounting functionality now provided by FLAIR:

- 1 of 10 universities was in the process of activating modules within currently running application suites.
- 8 of 10 universities were examining ERP solutions.
- 1 of 10 universities was examining multiple software options.

As of December 2001, Board university technology leaders indicated that until the Office of Technology and Information Services is staffed and functioning, it would not be finalized how the Office would affect or participate in university technology acquisitions.

Community Colleges:

The installation of ERP systems continues as a trend for community colleges.

Community colleges are locally based and governed entities with statutory and funding ties to State government, but are not under State agency status. Under the new educational governance system, the Division of Community Colleges, a division of the Board will continue to oversee and execute community college system responsibilities under State law.

The community college system is comprised of six individual consortia. The consortia are structured by grouping the colleges by the type of data processing equipment they maintain, the size of the institution, or the desire to collaborate in data processing functions. One consortium includes all institutions in a distance learning project. Members in most consortia share expenses, data processing equipment, and staff in the development, implementation, acquisition, and maintenance of student and administrative software. Under the new educational governance model, Board community college technology leaders expect the consortia to stay intact. As of June 2001, the colleges were in the process of contracting with a consulting firm to analyze the efficiency of the current administrative data processing systems.

Survey responses indicated that, of the 28 community colleges, half (14) used ERP software suites. Another 12 colleges responded as being in the process of installing additional modules to existing ERP software systems or installing new ERP systems. One community college was in the process of obtaining bids and evaluating a Request for Proposals for the procurement of ERP software.

Colleges continue the process of installing and supporting ERP systems in a carry-over of implementations that began as a solution to the Year 2000 software compliance issues. As legacy systems in colleges, not already using an ERP system, fail to provide required functions for their institutions, ERP systems may possibly provide this functionality driving further purchases of such systems.

District School Boards:

Certain district school boards have encountered difficulties implementing ERP systems.

District school boards are a part of the State system of public education. District school boards operate, control, and supervise all free public schools in their respective districts and may exercise any power except as expressly prohibited by the State Constitution or general law.

As of December 2001, Department technology leaders indicated that a determination of how the public school technology structure would change under the new educational governance model would not be made until the formation of the Office of Technology and Information Services was completed. Like the community college system, public schools maintain their own individual financial information systems outside of the State system, but are subject to State and Federal reporting requirements.

While the majority of larger school districts maintain their own data processing facilities, many of the smaller districts share software development and data processing facilities in one of the public school consortia. The State has encouraged districts with under 20,000 full-time equivalent students to enter into consortia through legislation and the awarding of incentive grants to participating school districts.

The range of computer equipment, participation in consortiums, and disparity in student populations and budgets between districts has created a wide range of software solutions to process student, human resources, and financial transactions. During the push to update applications for the year 2000 concerns, many districts instituted plans to replace applications with ERP solutions. Survey responses indicated that:

- 8 of 67 district school boards were using ERP software.
- 14 of 67 district school boards had a Request for Proposals in process for new information technology projects.
- 27 of 67 district school boards were in the process of installing new application and systems software.

In recent audits of the Broward, Polk, and Volusia county district school boards, we noted several common problems in implementing ERP solutions. These problems resulted in delays and cost overruns in the implementation process and hindered the deployment of ERP software. These included:

- Failure to clearly define requirements in vendor contracts, to enforce timely delivery of a fully functional system that met the needs of the district.
- Difficulties in adequately staffing the implementation project with district staff, due to the need to retain staff in legacy operations to process transactions.
- Districts instituting changes to the development of the systems, resulting in substantial costs above the contracted amounts.
- Inadequate training of end-users on the new systems.

For a more complete understanding of these matters, please see audit report Nos. 01-133, 01-131, and 01-150.

Recommendations:

To support best practices on a statewide basis for purchasing and implementation of information technology equipment and software, the

Department should utilize the proposed EPIC structure to assist all entities. Specifically, the Department should consider including the following features within EPIC to promote the effective and efficient functions of purchasing, installation, and maintenance of information technology products:

- **The EPIC portal should include a Web-based e-procurement component to integrate cooperative purchasing agreements currently in place such as the "Computer Refresh Program," a community college agreement with a major personal computer vendor for the volume purchase of personal computers. Additionally, the e-procurement component should integrate state technology contracts available through the STO and e-procurement initiatives by the Department of Management Services.**

- **The EPIC purchasing component of the portal should serve as an information source for existing and new technology purchasing and maintenance decisions. Using statewide technology information obtained by EPIC, members could access information on other members who have purchased or are in the process of purchasing software technologies. For example, a district school board could search for all entities using, or considering the purchase of, a particular ERP vendor's product and obtain entity and vendor contact names to utilize in their research and possible acquisition of that vendor's product. The portal should also host discussion groups on topics such as ERP solutions, specific vendor product topics including implementation and maintenance, and new technology acquisition and implementation. The members could also use information resulting from the EPIC discussion groups to request vendor improvements for future releases of software used by or under consideration for purchase by the entities and provide the ability to share software solutions to entities with similar platforms and software.**

- **Information on best IT acquisition practices should be made available through EPIC. To help promote these practices, the Department should consider preparing template documents for entities to use when contracting for IT products or services. For example, a 1998 study by the California Legislative Analyst's Office assembled best business practices used by the private sector to develop, acquire, and implement information technology. (See Attachment B.) The Department, through EPIC, could create a similar set of acquisition best practices to meet the needs of Florida educational entities. The template documents could incorporate these practices and be available for use by all entities when procuring information technologies.**

Recommended Legislation:

Chapter 282, Florida Statutes, should be amended to clarify responsibility for information technology functions within Florida's seamless K-20 education system.

Chapter 2001-170, Laws of Florida, amended Chapter 229, Florida Statutes, to provide for changes to the governance structure of Florida's education system. This included, in part:

- Section 229.003, Florida Statutes, was amended to, among other things, abolish the Board of Regents and State Board of Community Colleges and transfer their powers, duties, and functions to the Board of Education.

- Section 229.0061, Florida Statutes, was created, providing guidelines for implementation of Florida's seamless K-20 education system. This includes establishing within the Office of the Commissioner of Education the responsibility for operating Statewide functions necessary to support the Board of Education. Areas of responsibility include data management, education technology, and an education data warehouse, as well as technology and information services.

Chapter 282, Part I, Florida Statutes, which provides legislative expectations for State information resources management, has not been amended to reflect the governance changes. Specifically, Sections 282.005(9), 282.3031, and 282.310(2), Florida Statutes, continue to assign certain responsibilities for the information technology of the State University System and the Florida Community College System, to the Board of Regents and the State Board of Community Colleges, respectively.

Recommendation:

The Legislature should amend the provisions of Chapter 282, Florida Statutes, to pinpoint responsibilities for information technology of community colleges and universities within the new governance model provided for in Chapter 229, Florida Statutes. The Legislature should consider further defining the overall role of the Board of Education in promoting, encouraging, and facilitating the effective use, management, and operation of information technology for the entire K-20 education system.

HIPAA:

District school boards, community colleges, and universities may be subject to significant new compliance requirements related to data interchange, privacy, and security, pursuant to the *Health Insurance Portability and Accountability Act of 1996* (HIPAA), Public Law 104-191.

HIPAA addresses electronic data interchange, privacy, and information security standards for personal health information. HIPAA also provides for civil and criminal penalties for noncompliance. Pursuant to HIPAA, the United States Department of Health and Human Services has published regulations on electronic data interchange standards and privacy, with security regulations expected to be published during 2002.

Provisions include, in part, using a mandated set of transaction codes to classify data, establishing secured methods to transmit data, and having certain security functions in place to protect the data. Provisions to use classification codes set by HIPAA, electronic transmission standards, and audit trail requirements could require entities to convert paper documents to electronic format, subjecting entities to the security provisions of HIPAA. The Federal regulations have staggered deadlines for compliance, beginning on October 16, 2002 for the transaction rule. (See Attachment C for further information on HIPAA.)

Many Florida educational entities could be subject to HIPAA. For example, some district school boards are self-insured entities for employee health coverage. In addition, some colleges and universities are providers of health care services through teaching hospitals, dental programs, and other health care curricula. Because of the significance of these provisions on the handling and transmission of health records, advance planning to evaluate the impact of the HIPAA requirements on district school boards, colleges, and universities will serve to reduce the difficulties in making the necessary transition to comply with these new requirements.

Recommendation:

The Department should serve as a resource for educational entities in their assessment of subjectivity to HIPAA requirements and, where applicable, preparation to implement compliance therewith. This could include disseminating information to applicable entities, encouraging information sharing among entities, and facilitating, where practicable, multi-entity procurements of products and services related to assessing HIPAA applicability or implementing modifications to systems and procedures to provide compliance.

Scope, Objectives, and Methodology:

The scope of this project focused on surveying Florida's educational entities regarding their information technology structures during the period April 2, 2001, through June 15, 2001. Our objectives were to determine the current status of entity information technology structures applicable to financial management functions, and to evaluate the impact of the new governance model for educational entities as provided in Chapter 229, Florida Statutes, as amended by Chapter 2001-170, Laws of Florida.

We administered the survey to the educational entities in an on-line format and verified with the entities the accuracy and completeness of our records of their survey response submissions. However, we did not perform audit procedures to independently test the accuracy of entity representations in their survey responses.

We also communicated with Department officials through interviews and written correspondence regarding the status of organizational and management changes and information technology plans in connection with the new governance model.

Authority:

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of this project.

William O. Monroe

William O. Monroe, CPA
Auditor General

Department Response:

In a response letter dated January 18, 2002, the Commissioner of Education generally concurred with our findings and recommendations. The Commissioner's response can be viewed in its entirety on the Auditor General Web Site.

Attachment A
Hardware and Operating Systems

Figure 1 – Production Server Hardware

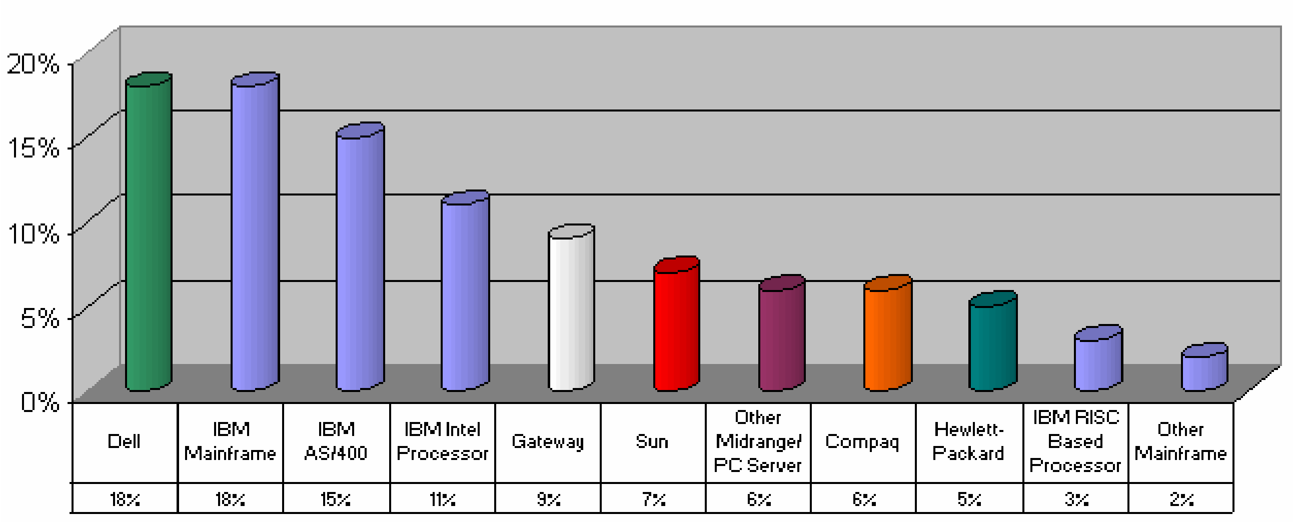


Figure 2 – Production Server Operating Systems

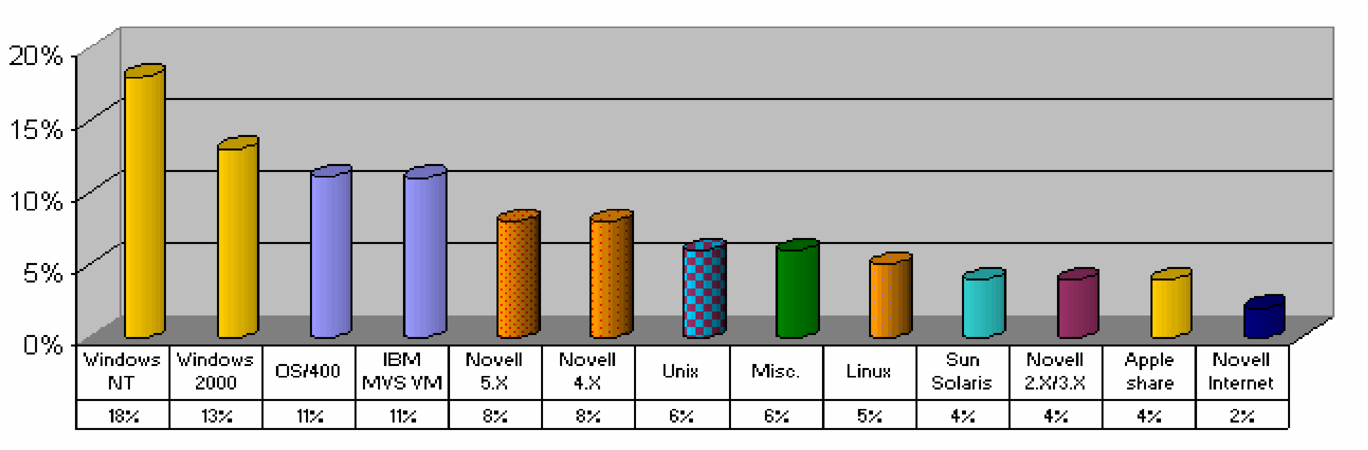
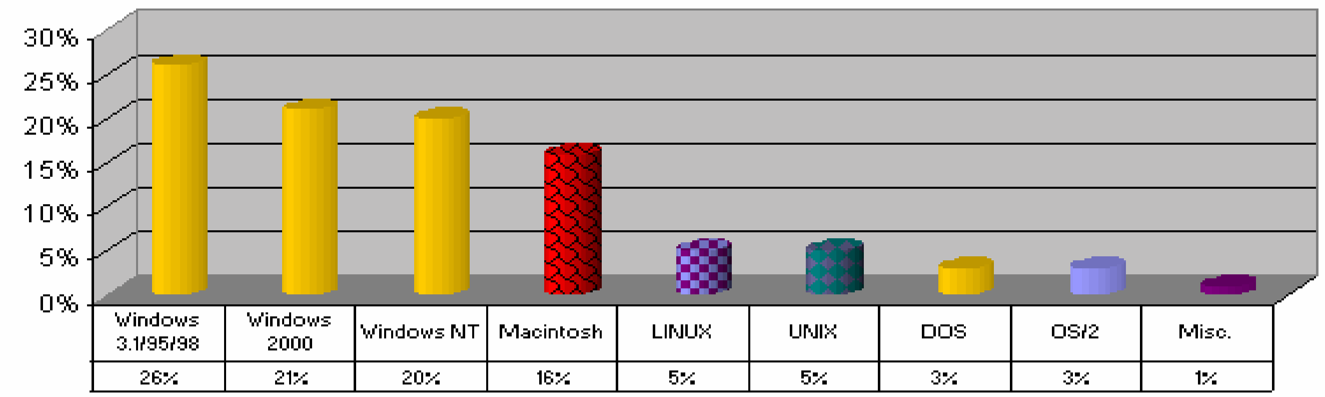


Figure 3 – Client Operating System



Attachment B
Selected Text from
California Legislative Analyst's Office
"Best Practices on Information Technology Projects"
Report

- **Base Procurement on Best Value, Not Lowest Cost** – By using the "Best Value" approach, the vendor's bid is combined with such factors as the proposed technology solution, experience in performing the contracted services, financial strength of the company, experience of the vendor's staff or contracted consultants, and other applicable project components.

- **Outline Business Problem Then Allow Vendor to Propose Solutions** – Rather than proposing a technology solution, entities should present the business processes and have the vendors develop solutions using the vendors' technology.

- **Develop Smaller Projects with Milestones** – Rather than developing large multiyear projects for bid, develop smaller projects with definite milestones.

- **Prioritize Project Elements Up Front** – Each project has three major components: (1) the budget, (2) the schedule, and (3) the functionality of the system. The project manager should have a good understanding of the entity priorities for each of these items. If the priority is the schedule, the project manager should have the ability to commit funds over the budgeted amount to complete the project on schedule. If the priority is budget, the project manager may have to decrease the functionality of the project to complete it within the budget.

- **Establish Measurable Objectives for the Project** – Projects should have measurable objectives to determine if the project has met the objectives of the organization or in defining contracted deliverables for vendor payments.

- **Require the Use of Project Management Methodology** – Project management methodology is a blueprint of how the project will be administered. It provides the components used by the project manager to track the progress of the project to decrease the risk of operational failure or cost overruns. Components include using a competent project manager, developing a strategic plan, use of a cost accounting system, and establishing a dispute resolution process and a process to implement changes to the project when needed.

- **Require Letter of Credit from Vendors on Larger Projects** – Should the project fail, maintaining a letter of credit from the vendor may allow the entity to recover some of its losses. A letter of credit also allows the entity to collect funds in a shorter time period than a performance bond. Because the vendor must maintain higher financial reserves than a performance bond, the cost of the project may be increased.

- **Use a Quality Assurance Contractor** – Quality assurance contractors help entities to identify and assess problems that can occur in a project and propose solutions to the problems. Also known as Independent Verification and Validation vendors, the contractor will assess performance by reviewing planning documents, assessing the quality of design , evaluating computer code written, and performing other project tasks.

- **Pay Vendor Only Upon Acceptance of Tested Project Deliverables** – Specific deliverables should be written into the contract and vendor payment should not be released until the entity verifies the completion of the deliverable.

- **Write Stronger Contracts to Protect the Entity** – Contracts should be written to meet the needs of the information technology purchased including clear responsibilities of vendor and entity, clearly defined liabilities, a dispute resolution process, and terms for payment including specified deliverables.

- **Enforce the Terms of the Contract** – If a vendor is not held to contracted terms during the project, the entity risks losing control of the project and jeopardizes the chance the project will be completed with the contracted functionality it desires.

Source: California Legislative Analyst's Office, December 15, 1998, State Should Employ "Best Practices On Information Technology Projects"

Attachment C
Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Executive Summary

Background

Congress passed HIPAA primarily as a way to allow individuals to carry health insurance from employer to employer. However, the HIPAA requirements are broader, with provisions for the United States Department of Health and Human Services (HHS) to develop electronic data interchange, privacy, and information security standards for the healthcare industry. HIPAA also provides for civil and criminal penalties for noncompliance, including: fines up to $25,000 for multiple violations of the same requirement; and, fines up to $250,000, imprisonment up to 10 years, or both, for the wrongful disclosure of individually identifiable health information with the intent to sell that information.

Compliance Schedule

The final Transaction Rule, which contains electronic data interchange standards and was incorporated as a federal regulation into 45 CFR Parts 160 and 162, was published on August 17, 2000, making the compliance date October 16, 2002. The final Privacy Rule was published in the *Federal Register* on December 28, 2000, but was not effective until April 14, 2001, making compliance required by April 14, 2003. The Privacy Rule was incorporated as a federal regulation into 45 CFR Parts 160 and 164. The proposed Security Rule, 45 CFR Part 142, has not been published in its final form, but is expected to be published during 2002. The law gives HHS the authority to make appropriate changes to the rules prior to the compliance dates.

Information Protected

All medical records and other individually identifiable health information used or disclosed by a covered entity in any form, whether electronically, on paper, or orally, are protected.

Ensure the Security of Personal Health Information

Upon its finalization, the Security Rule will establish the security standards that covered entities must meet to maintain covered records and health information. The current requirements are flexible and scalable to account for the nature of each entity's business, and its size and resources. Entities may be required to maintain:

- Security plans defining the actions required of personnel to maintain security over covered medical records.
- Security training for all employees maintaining, using, or transmitting covered medical records.
- Physical security measures to properly restrict access to covered medical records within the data system(s) and provide verifiable audit trails and monitoring of records.

Equivalent Requirements for Government Agencies

The provisions generally apply equally to private sector and public sector entities. For example, both private hospitals and government medical units have to comply with the full range of requirements, such as providing notice, access rights and requiring consent for routine uses.

Preserving Existing, Strong State Confidentiality Laws

As required by the HIPAA law itself, stronger state laws (like those covering mental health, HIV infection, and AIDS information) continue to apply. In circumstances where states have decided through law to require certain disclosures of health information, the final rule does not preempt these mandates.

**SPECIAL REPORT ON THE
INFORMATION TECHNOLOGY INFRASTRUCTURE
OF FLORIDA EDUCATIONAL ENTITIES**

This project was conducted by Brian R. Rue, CPA, CISA, and supervised by Nancy M. Reeder, CPA*, CISA. Please contact Jon Ingram, CPA*, CISA, Audit Manager, with any questions regarding this report. He may be reached via e-mail at* joningram@aud.state.fl.us *or by telephone at* ***(850) 488-0840****.*

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

**Regulated by State of Florida*

FLORIDA DEPARTMENT OF EDUCATION

CHARLIE CRIST
COMMISSIONER

January 18, 2002

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

Dear Mr. Monroe:

Your report has been reviewed by the Department of Education and education sectors covered in your report. We concur with your general statements that the Department of Education should promote sound information technology (IT) business practices among the education entities. We also concur that there can be areas in the information technology environment where it would be appropriate for the Department to facilitate solutions which could be utilized by the school districts, colleges and universities.

While the Office of Technology and Information Services (OTIS) within the Florida Board of Education has not yet been established, we see the role of this new entity as one of assistance, coordination and facilitation to the local institutions. We clearly recognize that there are expectations for the planning and collecting of data and information, which are required for good management and accountability. However, with the continued emphasis on devolution and local control, we would envision that the Office of Technology and Information Services would recommend IT solutions of varying levels of detail and specificity depending on the IT area involved.

While the current education IT divisions are already doing many things in the areas you discussed, there are always opportunities to strengthen, improve, and expand these practices, and to do more sharing among the local education institutions. We expect to create policies and processes that enable a balance between local flexibility and consistent IT business practices in order to maintain school, college, and university responsiveness to user demands.

We look forward to the opportunity to work with the institutions in developing a meaningful information technology strategy that will support and advance the new K-20 education delivery structure.

Sincerely,

Charlie Crist

Charlie Crist

Florida Atlantic University Tower
220 S.E. 2nd Avenue, #726
Ft. Lauderdale, Florida 33301
(954) 762-5322
Fax (954) 762-5197

The Capitol
Plaza Level 08
Tallahassee, Florida 32399-0400
(850) 487-1785 • SC 277-1785
Fax (850) 413-0378 • SC 993-0378

http://www.firn.edu/doe

University of South Florida, St.Petersburg Campus
POY 248, 140 7th Avenue South
St. Petersburg, Florida 33701
(727) 553-3730
Fax (727) 553-1033