

RAS 12209

DOCKETED
USNRC

September 07, 2006 (3:20pm)

OFFICE OF SECRETARY
RULEMAKINGS AND
ADJUDICATIONS STAFF

**Clalborne County Technology
And
Telecommunications Assessment**

April 5, 2004

TEMPLATE = SECY-038

SECY-02

Table of Contents

Executive Summary	3
General Technological Infrastructure	4
Developing a Enterprise Wide Strategic Technology Plan "A New Renaissance"	5
Establish a local area network and a single Internet assess point	10
Enhance and Standardize IT Security Measures	14
Standardize Computer Workstations and Technology Procurement Options	21
Structure the Management and Use of the County's Information Technology	27
Coordinate the County's Information Technology Support and Service Responsibilities	31
Consolidate and Standardize the County's E-Mail Services	36
Establish and Maintain an Official County Web Site	40
Ensure all Critical County Data are Secure	49
Improve the County's Telephone System	53
Improve the Management of County's Electronic Records and Data	55
Improve the Administrative Functions of Public Works Department	61
Sheriff's Department	63
Increase the Efficiency of the Sheriff Department's database software	63
Increase Sheriff Efficiency with Mobile Computing Technologies	70
Claiborne County Fire Department	74
Emergency Operations Center and E-911	80
Department of Information Technology and Public Safety	81

Administration and Planning Office
88

Streamline Workflow in Chancery, Circuit Clerk and Tax Assessor Office
90

Improve the Management of the County's Electronic records and data
91

Parks and Recreation
96

Road Management Department
97

Improve the Municipal Court's database Software
98

Internal Controls
104

Claiborne County Hospital
111

Claiborne County School District
112



BOARD OF SUPERVISORS

James E. Miller
County Administrator

DEPARTMENT OF ADMINISTRATION & PLANNING
jamesmiller@ccmsgov.us • www.ccmsgov.us

P.O. Box 689
510 Main St.
Port Gibson, MS 39150



Office: (601) 437-5216
Fax: (601) 437-4430
Cell: (601) 415-5713

Executive Summary

In September 2003, the Board of Supervisors of Claiborne County, Mississippi asked Delta Communications to perform a technology and telecommunications assessment of the information technology (IT) and electronic infrastructure of the county. Delta Communications reviewed the county's IT infrastructure during several on-site visits conducted in September and October 2003. In addition, Delta Communications staff included an appendix focused on proper internal controls. An assessment is not an audit and is not designed to detect errors or fraud.

The assessment's objective was to assess the county's current IT infrastructure, recommend improvements and provide an IT infrastructure that will eventually enable the county to offer e-government services. The review focuses on the county's general technological infrastructure, which crosses all county departments and offices. Additional specific entities include, the Administrative office, the Sheriff's Department, E-911, Chancery Clerk, EOC/Civil Defense, Claiborne County Road Department, Tax Assessor Collector and Justice Court. This document is based on information obtained during interviews with County department heads, staffers, and software vendors.

It is evident county officials realize the importance of IT as a tool to help provide efficient government services. The county has made commendable efforts to introduce and implement many aspects of IT. Such efforts include using specialized software applications in the Sheriff's Department, Justice Court, Chancery Clerk, Tax Assessor Collector, E-911, Road Department and Administrative office. Also, by creating a fixed assets inventory list and organizing the county's IT service for support and maintenance agreements has proven to be a step in a positive direction.

The County's 2002-2003, 2003- 2004 approved budget contains the necessary information. It has prior-year, actual and budgeted data. The Board approved the budget by resolution, and the Clerk has sworn it as the official budget document approved by the Board. Overall, the budget is easy to read with adequate descriptions; however, the document lacks sufficient detail, which does not give department heads sufficient flexibility. This problem may result in requiring the Board, Administrator, and Financial Officers to bring budget amendments and transfers to the Board of Supervisors frequently to avoid overspending and or to acquire services and equipment.

This report lists 50 recommendations or options that the County may consider for improving the IT infrastructure. Some major recommendations include Drafting an Enterprise Wide Strategic Technology Plan and establishing a Department of Information Technology and Public Safety. The installation of a local area network (LAN) utilizing a centralized redundant file server for cross-departmental access with a Geographical Information System (GIS) Repository will improve the security of the county's workstations and equipment, including uniform data backups and off site storage. In addition, addressing IT administrative and control issues, establishing a presence on the World Wide Web (WWW), standardizing the county's-mail accounts and e-mail address domains, e-fax consolidation, and upgrading critical county software applications will assist in the migration of Claiborne County into the twenty-first century. Delta Communications anticipates the Claiborne County Board of Supervisors will find the recommendations useful. Ultimately, the decision to implement these recommendations rests with the Board and the affected elected officials.

General Technological Infrastructure

At the time of the assessment, the Claiborne County maintains 30 personal computer (PC) workstations in eleven distinct departments or offices. The county has 38 printers and 11 fax machines. A few offices have access to the Internet (either cable broad band or telephone [dial-up] connections) communicates through Mississippi State University County Extension backbone that is not a County controlled asset. The County does not have an official electronic mail (e-mail) domain or server; however, department heads and staffers have personal e-mail accounts that are not secure or protected from foreign virus attacks. The departments/offices are not totally networked, and the County does not have an official Web site.

There was a standard networking cable that connects the WYSE workstations of the Justice Court, Circuit Clerk, Chancery Clerk, Tax Assessor/Collector to the IBM AS400 mini mainframe of the Court House. These networking cables in various areas are not installed with the proper appliances and hardware. This has made areas in the Court House and the Administrative building trip hazards and out of compliance according to Occupational Health Safety Standards (OHSA) standards. The Administrators office is the only department that can share files over an inter-office network this allows the four pc workstations to communicate and share electronic files.

The County's workstations use four different versions of operating systems (Windows 95, 98, Windows 2000 and Windows XP) and different office software applications. Windows 95 is not Y2K compliant. Some Departments or individual employees use

specialized software applications to perform their jobs. These applications include, but are not limited to: MS Roma, CAMEO, MARPLOT, Amaxtrom, and SCATS.

The County does not employ a full time, dedicated IT administrator. Instead, each department assumes responsibility for the service and support of its information technology (IT).

The County accounts for IT expenditures by line item in each department's supplies and operational expenses budget. The County also budgets for training, maintenance, service and support separately.

Some of the County's current IT capital needs that are covered include the acquisition of a new central file server and a local area network (LAN), new computer workstations, an updated and enhanced PBX telephone system and an official County Web site and County wide E-Mail.

There is a need for physical upgrade in the public utilities that serve the County telecommunications needs. As we understand it, there is only one main trunk that serves the County campus of (Court House, Administrative Building, Sheriff Department/Detention Center, Central Fire Station, E-911). The history of this one trunk has proven that if there is a natural disaster or an accident that this main artery will cut all out going and in bound calls to the campus. This is a tremendous liability for the Provider as well as the County when emergency operations depend on this utility. A back up plan must be devised to support the County's Enterprise Wide Strategic Plan. The County must request that the utility provider design an alternate routing system to compensate for this out dated public utility plan.

Developing a Enterprise Wide Strategic Technology Plan " A New Renaissance"

Background

Effective organizations, whether public or private, develop specific missions, establish goals that support these missions and implement strategies to reach these goals. Organizations frequently use strategic planning and budgeting process to develop and achieve their missions, goals and strategies. A strategic plan gives an organization a unified vision of its future by focusing on priorities developed by reaching a consensus. A comprehensive strategic plan highlights potential risks and enables decision-makers to

make informed decisions. Furthermore, strategic planning can help an organization measure its progress toward its goal.

In general terms, a strategic plan provides a status of the organization, its desired future direction and the actions necessary to achieve stated goals. The typical strategic plan covers three to five years, but some cover longer periods.

Successful strategic planning requires an ongoing, systematic process that becomes permanently intertwined with the organization's routine operations. The components of a strategic planning process may vary among organizations, but virtually all involve several basic components. These include a "plan-to-plan," an "environmental scan," the creation of broad organizational policies and detailed departmental goals and objectives, training for all participants, participation from the entire organization, involvement of a facilitator or coordinator, a direct link to budget decisions and daily operations and performance evaluation.

A plan-to-plan should be the first activity undertaken by any organization developing a strategic plan. As the name suggests, a plan-to-plan is literally a plan for the planning process itself. It details the steps involved in developing the strategic plan so that the entire organization can understand the process.

A plan-to-plan defines the steps, lists the people involved in each step, outlines decisions to be made for each step and identifies the people responsible for those decisions.

The plan-to-plan also lets outside interests know when their input is necessary. The planning steps should be organized so the completion of one step leads to the beginning of another. Without a comprehensive plan-to-plan guiding the strategic planning process, key players or activities at various stages may be overlooked.

An environmental scan is a detailed assessment of the organization's current circumstances—normally follows or parallels the plan-to-plan phase. The scan closely examines the current organization, its structure, its strengths and weaknesses and external factors and trends that affect it, such as customer expectations. The environmental scan identifies issues that the organization should address in the strategic plan.

Creating board organizational policies and detailed departmental goals and objectives are important to ensure full and standardized cooperation throughout an organization. This process also helps decision-makers prioritize separate departments' needs.

Organizations may use consultants/plan coordinator, steering committees, administrator's office or a combination of these groups to manage the process. Without effective coordination and leadership, strategic plans tend to drift and lose momentum. The consultant/plan coordinator should keep the plan current and ensure that all schedules are followed. The organization's leadership also should provide a common point of contact for planning information and progress reports. To be successful, an organization's

leadership must enthusiastically support the planning process and make this support highly visible to the rest of the organization.

The planning and budgeting processes should remain distinct, because a comprehensive strategic planning process covers a much longer time period than an annual budget. Nonetheless, the priorities set forth in the strategic plan should be used to guide annual funding decisions and priorities. For example, a department may present two proposed projects for the coming fiscal year or two departments may each present a proposed project, but the organization only has funding available for one. The organization should then evaluate both projects and prioritize or determine which best fulfills and advances the organizational goals defined in the strategic plan.

Finally, effective strategic planning involves measurement and evaluation. The strategic plan must identify how performance will be measured and specify evaluation standards consistent with the plan's goals and objectives. With such yardsticks, the county can evaluate its progress and modify the plan based on new information and experience. Due to the multitude of issues and decisions that should be addressed when acquiring, implementing and managing an IT infrastructure, the county needs the guidance of a well-developed IT strategic plan.

The benefits of effective IT planning includes:

- Improved communication and consensus building among stakeholders;
- Effective use of available funds through open technology software systems, the blending of existing equipment within a multi-vendor approach and more efficient buying practices;
- Increased access to technology resources within the county boundaries and beyond, via telecommunications;
- A clear picture of equipment needs that improves the county's ability to secure appropriate funding and prioritize needs;
- An adequate number of effective training workshops for staff members;
- Improved access to and use of governmental information to assist decision-making;
- Improved operations, enhanced working environments and more effective management; and
- The elimination of redundant data entry and other inefficient practices.

At a minimum, the county's IT plan should include:

- Evidence of wide involvement by staff and community stakeholders, including a representative from each department;
- Support from executive leadership, including all elected officials and appointed department heads;
- Support for overarching organizational goals including the future introduction of e-government solutions through the Internet;

- An assessment of internal and external users' technology skills, knowledge and comfort levels;
- An asset management system that contains IT hardware and software inventories with sufficient detail to support informed decision-making for the future, compatible technology purchases, including tracking, scheduling and auditing policies;
- A compilation of technology expenditures over the past three years;
- An infrastructure design and the capacity needed to support the county's communication and information needs;
- Common technology standards for software and hardware, including update and replacement schedules;
- Software and hardware service policies and procedures, including a centralized process for requesting service;
- A three-to-five year implementation plan for expenditures tied to specific goals and budgets to ensure that a general IT budget is available for service and general maintenance, support and end-user training costs; and an IT capital improvement budget set up for long-term IT networking, hardware and software expenditures;
- Training and support plans for users;
- Standard data backup and recovery policies, schedules and procedures, including backups for each department, as well as the central server;
- Disaster recovery and contingency planning;
- Data privacy/integrity policies, especially important when introducing online or e-government services like account and payment information;
- Data retention and scheduled purging;
- IT network security policies and procedures, including user access and password policies, both for on site and remote access to the network;
- Policies and procedures for the Web site content changes and updates;
- Dispositions plans for old or unused hardware; and
- An evaluation and revision process.

As the county's develops the IT plan, it must be sufficiently flexible to manage rapid changes in technology. The plan should allow new technologies to be introduced at the appropriate times.

Findings

- **Claiborne County does not have a formal IT committee.**

Each department submits IT request on an as-needed basis during the budget planning process and randomly throughout the year. This process does not address all IT concerns, nor does it allow for consolidated orders, and it represents a reactive approach to acquiring and managing IT resources.

Claiborne County does not have a documented IT strategic plan.

The County does not have a unified vision of where it expects its information technology to be in five years. Again, this represents a reactive approach toward IT rather than a proactive approach.

The Assessment conducted by Delta Communications for Claiborne County Can serve as a foundation for the county's environmental scan, which is an Essential step in the IT strategic planning process.

Every strategic plan should include an environmental scan. A scan provides County with a snapshot of its IT infrastructure, which provides a starting point For planning. The county should include the IT required in all departments in The environmental scan.

Recommendations

Develop and maintain a long-term vision for the county's information technology.

A. Create a countywide IT planning committee.

Effective IT plans and strategies usually are derived from a committee that represents each of an organization's major operations or departments. Representatives should know about their departments or operation's current IT infrastructure and future IT goals and needs. At the beginning of the planning process, the committee should designate an IT coordinator to manage the process, prepare the plan, oversee its implementation and serve as the central contact for IT information requests.

The coordinator should be a full-time county employee and have the authority and the independence to report directly to decision-makers. The individual filling this position should have superior communication, financial analysis and research skills, the ability to manage projects and an understanding of IT and its applications. Depending on the coordinator's IT experience, the county also may need to hire a consultant to guide the planning process.

B. Devise a five-year IT strategic or master plan.

A formal IT strategic or master plan will help the county make appropriate IT acquisitions and agreements for services, provide a way to prioritize all city IT related projects and communicate the county's vision to county officials and employees so they can accurately formulate expectations.

When creating this plan, the committee should consider the potential number of IT users in the community, their present access to technology and their current skill levels. To gauge these factors, the committee should survey the county employees as well as external users to gather the data needed to perform a cost-benefit analysis of every proposed element of the plan.

While the plan should focus on establishing internal IT policies and procedures that will help the county achieve its desired goals and objectives, it should also incorporate opportunities to use common technologies and share resources among local organizations. Committee members could consider collective purchases of software, hardware, cabling, Internet service and communications equipment when such purchases could generate savings for the county.

Establish a local area network and a single Internet access point

Background

A local area network (LAN) consists of individual computer workstations that are connected and confined to a single building or group of buildings. Workstations can be connected or networked with physical cables, wireless antennas or a combination of the two. The primary benefit of a network is that it allows users on individual workstations to access, share and communicate data. Most LANs use a central computer, referred to as a server, to direct network traffic (data transmission) between the workstations connected to the LAN. A LAN is most commonly used to transmit e-mail messages, to share data files and to browse the Internet.

Network architecture refers to the manner in which workstations are connected. Networks can use either peer- to- peer or client server architecture. In a peer- to- peer network, data flows between two or more workstations, but there is no central server or single workstation controlling the others. In some peer- to- peer networks, one user may have access to other user's hard drive for easier file sharing. With client-server architecture, each computer or workstation on the network is either a client or a server. Servers are primarily dedicated to managing network traffic among workstation, and clients are simply the workstations connected to the network.

There are several types of servers, but by design, all servers, no matter their specialized function, pass information across a network. The most common type of server is a basic network server. As the name implies, a network server passes information from one workstation to another and helps manage the resources of a network. Similar to a

network server is a file server, which also moves information across a network but is primarily used to store large amounts of data. File servers are used as a central storage point for much of an organization's data, and from this point users on the LAN can access, search and share the information stored in the file server. Organizations rely heavily on file servers to support and store their data because loss or corruption of that data could be costly. For this reason, a file server is outfitted with a special type of data backup system, referred to as a redundant array of independent disks (RAID). RAID disk drives are used frequently on file servers as a means to ensure that important data is duplicated or backed up.

A LAN will vary in complexity. Every LAN is an aggregate of computer servers, workstations and other components that connect them. These components include hubs, switches and routers, and they serve as a common connection point for workstations on a network. A hub is a hardware device that contains multiple ports that are used to connect the cables of a network. Hubs serve as a conduit for cables that enable the transfer of data packets from one workstation or segment to another. Hubs are comparable to traffic intersections because they serve as junctions where packets of information, like automobiles, can pass through toward their intended destination. In small networks with minimal data traffic, a hub is usually adequate. In larger networks, it is advisable to use a dedicated hub, commonly referred to as a switch. A switch adds the level of functionality needed by reviewing and directing the data as it passes through the hub. Another similar device is a router, which basically is a hardware appliance that connects any number of networks. When data packets originate from within one LAN and are destined for another LAN, the data must exit the network through a router. As the name suggests, a router simply routes traffic that is leaving or entering a LAN.

Modern organizations increasingly depend on internal LANs for communication and data sharing. The resources dedicated to the management and maintenance of an organization's LAN should reflect that. A network or systems administrator is a general title used to describe an individual dedicated to the management of an organization's LAN. A network or systems administrator addresses issues such as hardware layout, security, performance and reliability. Hardware layout refers to the workstations, servers and cables that are run throughout a facility to connect the organization's LAN components. Security refers to the measures taken to ensure that the LAN is protected from unauthorized users. Performance refers to the handling of bottlenecks in the network, and reliability refers to making the LAN available to users and responding to hardware and software malfunctions. Depending on the size of an organization or its dedicated IT budget, the task of a network or system administrator may require one part time individual or a large staff. Some organizations may choose to outsource all network maintenance.

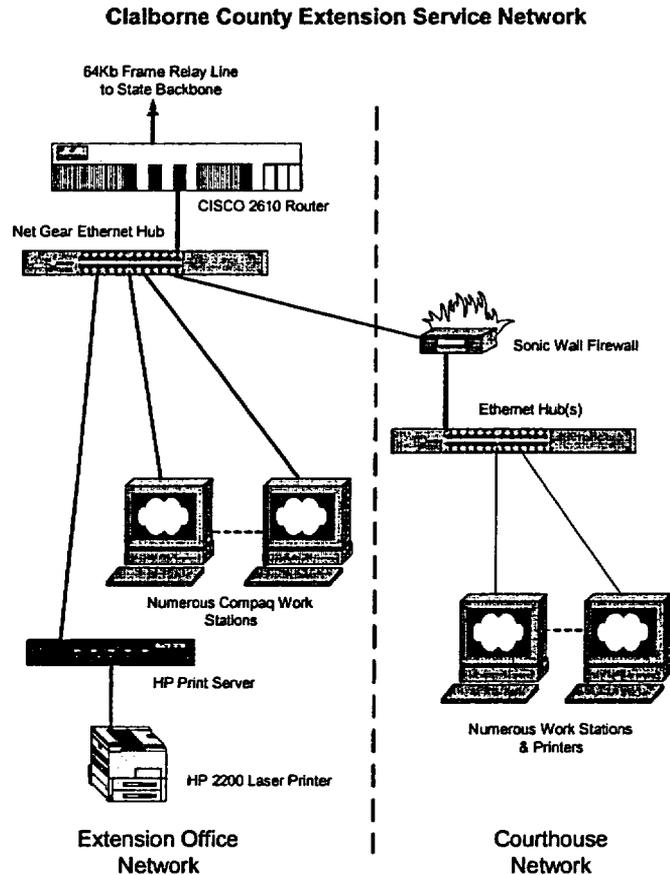
When an organization's LAN is connected to the Internet, a wealth of information is available to its employees. Most organizations connect their LANs to the Internet using broadband, satellite dish and dedicated circuit. For the purposes of this report, a broadband dedicated circuit refers to an Internet connection that is continuous, does not require telephone (dial up) access and allows a high volume of user traffic and

information to pass through. Although it is beneficial for an organization to connect its LAN to the Internet using a broadband connection, some organizations still maintain workstations that are fitted with telephone (dial up) modems.

There are three primary reasons why organizations prefer to connect to the Internet using broadband dedicated circuits, rather than telephone (dial up) modem connections: performance, cost and security. First, workstations using broadband connections are perpetually connected to the Internet and do not need to dial (call) to connect, thus providing users instant access to the Internet. Once connected, a conventional telephone modem can only transfer information at 56 kilobytes, which is considered inconveniently slow for a modern business environment, and only about one-fifth the speed of the slowest broadband connection. Data transfer speeds are extremely important when transferring (downloading/uploading) large amounts of data, such as documents or digital photographs over the Internet. Additionally, the cost of business class broadband services has steadily decreased within the past few years, making broadband more affordable. Finally, telephone (dial up) modem connections are more vulnerable to security problems than broadband connections.

Findings

Currently, the only existing network resides on a frame provided by the Claiborne County Extension Service (see diagram below).



This network has provided adequate, but limited resources for such functions as internet access, shared printing, and file distribution for multiple users at a fraction of the cost. However, this network structure is not sufficient to achieve the intended goal of efficient IT communication for the entire County. The current network infrastructure may serve as foundation example for satisfactory upgrade specifications to be met. Ultimately, the recommendation is to establish a self-contained network infrastructure owned and housed by Claiborne County. This in turn gives executive control of the network's maintenance and enhancements to Claiborne County.

Enhance and Standardize IT Security Measures

Background

A local area network (LAN) consists of individual workstations connected and confined to a single building or a group of buildings. Workstations can be connected or networked with physical cables, wireless antennas or a combination of the two. The primary benefit of a network is that it allows users on individual workstations to access, share and communicate data. Most LANs use a central computer, referred to as a server, to direct network traffic (data transmission) between the workstations connected to the LAN. A LAN is most commonly used to transmit e-mail messages to share data files and to browse the Internet.

When a LAN is connected to the Internet, a wealth of information is placed at the user's fingertips. This same connection, however, also invites potentially harmful elements into the network, such as unauthorized access to data, computer viruses and data destruction. Any of these issues could have a devastating affect on operations.

A breach of information security could range from harmless network access to malicious corruption of an organization's records that could disrupt basic administrative processes. Organizations are especially vulnerable to such incidents if adequate funding is not made available to implement sound security measures. Many smaller organizations have been victimized by network intrusions, which can have far-reaching legal implications for those organizations and can reduce public confidence. It is in the best interests of an organization to develop and include reasonable, proactive security measures in its strategic plan.

The first layer of defense in preventing Internet intruders is a firewall. A firewall is a system that functions as part of a network and is designed to prevent unauthorized access to an organization's private computer network. All the messages entering or leaving the LAN pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. Firewalls allow an organization to filter content, manage virtual private networks (VPNs), monitor network resource requests and share Internet access. Although a firewall is a necessary tool to protect from network intrusion, it only protects the network from external threats.

Another layer of protection, anti-virus software, is located on each individual workstation on the LAN. Unlike firewalls, which are designed to detect intrusions to the network, anti-virus software scans the data disks including the hard drive, floppy disks and compact disks of each individual workstation to detect the presence of viruses. Viruses can be introduced into individual workstations through e-mail messages, Internet download or infected media such as floppy disks and compact disks. Anti-virus pro-

tection is usually offered as a software application, which is generally loaded on each workstation. Because of the dynamic nature of computer viruses, the anti-virus software should be updated routinely. Anti-virus software companies offer downloadable updates, which increase their products' ability to detect and eliminate computer viruses. These updates are generally offered at specific time intervals, or are updated in response to a specific threat. These updates should be included in an organization's IT strategic plan.

One of the easiest and least expensive ways to prevent unauthorized access to an organization's LAN is the use of the user IDs and passwords. A user ID, also referred to as an identification string, identifies the user attempting to access the network or workstation. A user ID can be an individual's name or a series of identifiable numbers. This is especially helpful when more than one individual routinely uses, or has access to the same workstation or LAN. A password enables a user to access a data file, computer workstation, software program, LAN or centrally shared server. On multi-user networks, each user must enter his or her user ID and password before the workstation will respond to commands and allow access to the network.

Sometimes passwords are easily determined. An organization should have control measures in place to ensure passwords remain confidential. Many organizations use an expiration schedule, which forces users to re-establish new passwords after a given period of time. Without these safeguards, entire networks can be vulnerable. For this reason, the use of passwords should be monitored, and employees should understand the guidelines for choosing and implementing passwords. Finally, organizations should maintain comprehensive policies outlining procedures for the use of passwords and stress the importance of keeping passwords confidential.

Most organizations connect their LANs to the Internet using a broadband, dedicated circuit. For purposes of this report, a broadband dedicated circuit refers to an Internet connection that is continuous, does not require telephone (dial-up) access and allows a high volume of user traffic and information to pass through. Some organizations still maintain workstations that are fitted with telephone (dial-up) modems. Telephone modems use standard telephone lines to directly connect to the Internet, thus bypassing the protection of an organization's firewall. Such connections are a major vulnerability for an organization because there are no tools to filter and protect users from security threats, such as computer viruses or hackers, and hackers often target telephone modem connections because they are often easier to compromise than an organization's firewall. Moreover, it is more difficult for an organization to adequately monitor and regulate Internet usage of those who use a modem versus those who connect using a LAN connection. An Internet connection that goes through an organization's server and firewall are generally monitored to ensure that employees abstain from unauthorized Web sites or questionable content. For these reasons, many organizations that have a functional LAN will not purchase standard workstations with telephone modems.

Maintaining a secure LAN is a multi-layered process that encompasses numerous technologies and documented procedures. While none of these precautions can completely protect an organization's network, the combined use of firewalls, anti-virus

software and user IDs and passwords will help maintain a secure and cost effective network.

Findings

- **The county uses multiple telephone (dial-up) modems to connect to the Internet, which poses a security risk.**

The county uses at least two telephone (dial-up) modems to connect to the Internet. Workstations, like those used by the county that are connected to the Internet using a telephone (dial-up) modem are more likely to inadvertently download a virus or experience an intrusion.

- **The county secretary receives Internet access through a cable modem.**

Since the on-site review, the county has acquired cable broadband Internet access for the county's secretary's workstation. The county secretary, however, has the only workstation that was connected to a cable modem for the broadband Internet access.

- **The county's workstations are not networked, so they are unable to Access the Internet through a single server or cable router, and this situation can pose security risks.**

The county has five workstations that are used every day, and because The workstations are not fully networked, they each have different access points to the Internet, which makes them vulnerable to a security breach. To enjoy the security benefits of using a single location such as a LAN Server or cable router, are connected to a firewall appliance that filters Internet traffic as it leaves or enters.

It also is more difficult to regulate and monitor employees' Internet usage When they access the Internet using a telephone (dial-up) connection, as opposed to those who access the Internet through a network server. Network Servers equipped with the proper software tools can regulate, monitor and record employee actions while on the Internet.

- **The county does not have adequate firewall protection.**

The two workstations in the county's administrative office are equipped With a free software based firewall application, known as Zone Alarm, But the county's remaining workstations connect to the Internet through Telephone (dial-up) modems so they have no firewall protection.

- **The county is vulnerable to virus and worm attacks because the anti-virus software is not routinely updated.**
- At the time of the on-site review, there were numerous workstations in the county hall that did not have ant-virus software installed, or the installed anti-virus software was outdated. Given the changing nature of computer virus threats, it is critical that versions of the county's anti-virus software are routinely updated. Additionally, the county has no specific procedures or policies to address computer virus threats.
- **There are no documented policies and procedures, or standards processes that address the use and control of computer access and authentication.**

Although some county staff has user Ids and passwords, the county does not maintain a comprehensive policy outlining procedures for the use, administration or control of user IDs and passwords.

County employees or council members can access any computer without logging on, thus the system cannot identify who is using the computer or track what they are doing. Without security policies and proper oversight, the use of user IDs and passwords becomes ineffective.

- **The county does not have any workstations or Internet enabled terminals located in the common meeting area of the municipal building.**

The county does not have workstations or terminals located in the common meeting areas of the municipal building that would allow access to the Internet. Consequently, some county staff members or elected officials are compelled to use the workstations located in the police office or administrative office when they need a computer. Not only is this an inconvenience for officials and staff members, it is a security concerns as well.

Recommendations

Enhance and standardize IT security measures.

- A. **Discontinue the use of telephone (dial-up) modems to connect to the Internet**
- B. Workstations in the courthouse will be less vulnerable to network intrusions and viruses if the county stops using telephone (dial-up) modems. This change would have some county offices unable to access the Internet, so they should choose between two different options to secure broadband Internet access for all of the county's workstations. These options are outlined below in recommendations B and C. The county should continue to use the telephone modems until it installs a

LAN and central server, or until equipment is installed that will allow all employees to leverage the county's broadband connection. Implementation of either of these recommendations will negate the need for telephone (dial-up) connection.

B. Connect each of the county's workstations to the Internet through a central LAN server that works in conjunction with a firewall appliance.

This recommendation is congruent with a recommendation outlined in Issue 1.2 Of this document, which notes that the county should install a LAN. A LAN Server could be fitted with a router and firewall appliance, providing a single and protected point from which all county workstations could access the Internet. There would be substantial costs associated with establishing a LAN, which are also covered in Issue 1.2. The county has other Internet connectivity options. The installation of a LAN, however, is the preferred option because it provides **the best reliability and security.**

Once a LAN is in place, a firewall device could be installed on the LAN. This cost would include a standard firewall hardware appliance and software sufficient to serve the needs of up to ten workstations.

C. Connect each of the county's workstations to the Internet through a single cable modem that works in conjunction with a firewall appliance.

In the absence of a central LAN server, the county should consider expanding the availability of cable broadband Internet access so that each of the county's workstations have a secure broadband connection from one source.

XXX Cable, the county's broadband Internet service provider (ISP), can arrange for each workstation to have broadband Internet access. Attaching an eight-port cable nub to the county's existing cable router would allow up to eight of the county's workstations to slave off the county's single broadband connection, which is currently used only by the county secretary. Additionally, the county could incorporate a standard firewall appliance to the configuration, and this change would ensure all of the county's workstations would be provided with the same level of security and broadband Internet access.

The initial charge for a router, firewall appliance and installation of five additional workstations connections, commonly referred to as drops, would cost approximately \$750. Recurrent monthly fees would increase approximately \$70 to approximately \$200 per month. The increase in recurrent monthly fees would stem from additional bandwidth needed to facilitate additional users, as well as nominal per user licensing fees for the connection XXX/Roadrunner connection software. Compare to the current \$70 monthly charge for a single broadband connection in the county administrative offices providing six work-

stations with the same broadband connectivity for approximately \$200 per month would be cost effective. More importantly, the cable modem hub would allow broadband Internet connections for all employees, while directing Internet traffic through the safety of a firewall device.

This recommendation should be used in lieu of, or prior to the installation of the Proposed central LAN. A broadband connection passing through a shared cable Hub with firewall protection would satisfy most of the county's security concerns, however, a cable hub would not function as a true LAN.

C. Install anti-virus software on all of the county's workstations and the proposed LAN server and ensure that the software is routinely updated.

Anti-virus software is an expensive way to protect against the threat of computer Viruses. A licensed and uniform version of anti-virus software should be installed on each of the county's workstations, as well as the LAN server.

Once installed, it is important to update the anti-virus software routinely. Employees are not generally responsible for downloading anti-virus software updates to their workstations; instead the task should be regulated to a designated person, such as the IT coordinator (see Issue 1.6). Once all workstations are networked to a LAN, updating anti-virus software on all workstations can be accomplished from the LAN server. Assigning a specific individual to perform anti-virus software updates ensures that the downloads are performed in a timely and uniform manner. Some software vendors recommend updating anti-virus software about once a week, however, monthly updates should be sufficient for the county of Claiborne. Many anti-virus software programs offer automated update schedules that enable the anti-virus software that is installed on a LAN to automatically perform periodic software updates. This feature relieves the IT coordinator from having to perform periodic updates manually.

Issues such as who is responsible for installing and updating the anti-virus software as well as how often the updates should be performed, should be outlined in the county's information technology policies and procedures. For additional information about IT policies and responsibilities, refer to Issues 1.5 and 1.6.

D. Document and distribute policies on user IDs and passwords.

The county should develop and maintain comprehensive policies outlining procedures for the use of user IDs and passwords. The policies should encompass what end user operations employees will be expected to know, such as how to establish and modify their computer passwords. Passwords should be a combination of letters and numbers, valid for a given period of time, such as three to six months. In addition, control measures should be clearly defined to ensure passwords remain confidential.

Administrative aspects of the user ID and password policy should cover issues such as general procedures for using passwords, training, password expiration schedules, general security, who can grant, reset and provoke passwords and possible disciplinary actions for those who fail to comply with noted policies. The administrative aspects of the policy are generally the responsibility of a designated systems administrator, or smaller organizations an IT coordinator (see 1.6) . In addition to administrative duties, the designated employee should be able to track and issue temporary passwords to employees who have forgotten theirs. The county's designated employee should be able to discontinue password access for terminated employees.

F. Ensure only appropriate staff members have keys to access any IT equipment or the storage areas where IT equipment is stored, such as offices and IT closets.

In the case of a small county, such as Claiborne, only appropriate staff such as office employees should have access to any IT equipment during, and especially after, business hours. Limiting access to areas where IT equipment is stored or housed will significantly reduce the likelihood of data corruption, theft or physical damage to equipment contained in these areas.

The county should implement a process to document when personnel have entered an IT storage area. A basic log should be kept in each area noting the name, date and reason for access. This process may seem unnecessary; however, if the county acquires a LAN server, the IT closet should be more secure.

G. Install an Internet-enable workstation in the common meeting area of the municipal building (city hall).

As a matter of convenience and security, the county should place one or more Workstations in the common area of the municipal building. The workstations could be used by the county officials, county contractors or even citizens to prepare documents, take minutes or notes, check e-mail or have general Internet access. This addition would also allow county officials to access county systems without having to use an employee's computer. Again, only persons with the proper user ID and password should be allowed to access the computer or use its tools, such as access to the Internet.

Administrative rights and other access controls could be placed on the common area workstations so that the terminals would not jeopardize the security of the county's workstations, LAN or central server. These security controls could be established regardless of whether the county uses a single cable hub for Internet access or purchases and installs a network server.

Staff noted that the county had planned on purchasing new workstations for administrative staff during the next fiscal year. At least two of the workstations

that are currently used by the county staff could be reallocated to the common area.

Standardize Computer Workstations and Technology Procurement Options

Given the rapid rate of technological change, it is difficult for any organization to have the most current hardware. As the sophistication and power of software applications increase, they require better performance from computer hardware, specifically the workstations that support them. This diminishes the useful life of the computer hardware and presents a challenge for IT or systems administrators or coordinators who determine when and how to upgrade or discard older workstations.

Keeping workstation inventories current involves many steps but begins with a comprehensive inventory of the computer hardware currently in use by the organization. An inventory of workstations should be conducted at least once a year and the process should be documented in the organization's comprehensive IT strategic plan. With a comprehensive inventory, organizations find it much easier to anticipate general hardware needs and form strategies to minimize costs.

It is important that an inventory contain references to internal components such as random access memory (RAM), processors, bus speeds, port configurations and hard drive capacity. Noting only factors such as the brand, model and serial number will provide information about the functionality of the workstations. In evaluating workstation hardware, there are many factors to consider; however, the three most important performance-related attributes of a workstation are the RAM, hard drive storage capacity and speed at which the central processing unit (CPU) operates.

The CPU is the brain of the entire computer. In terms of computing power, the CPU is the most important element because it performs all the computer's calculations. The speed at which the CPU processor performs calculations is measured in megahertz (MHz). In general, the higher the CPU speed, the faster the CPU can perform calculations, which results in better performance of a workstation. Leading computer manufacturers currently offer basic workstations with CPUs that operate at 2,500 MHz, or 2.5 gigahertz (GHz).

RAM is the most common type of memory found in computers and other devices, such as printers and servers. The way RAM works is complex, but as a general rule, the more RAM memory, the faster the workstation can execute tasks simultaneously. For this reason, it is important that workstations are equipped with sufficient amounts

of RAM. Many leading computer manufacturers currently offer basic workstations with a minimum of 128 MB of RAM.

A workstation's hard disk drive, often referred to just as the hard drive, serves as a computer's long-term memory and is where software and data files are stored and retrieved. A hard drive has a given capacity that is measured in gigabytes (GB). Leading computer manufacturers currently offer basic workstations with 20 GB of capacity.

There are hardware aspects of a workstation that should be noted, but are not directly related to performance. For example, most workstations come with a network interface card (NIC), a device that allows a computer to be connected to a local area network (LAN). A workstation cannot be connected to local area network without a NIC, so it is important to confirm that a workstation has a NIC. It is also advisable to inventory the port configurations of a workstation. Ports are simply the different connection points, generally on the back of a workstation, in which peripheral devices such as printers, a mouse, monitors or LANs can be connected. It is advisable to note the type, number and layout of each port.

When establishing the hardware needs for an organization, it is necessary to understand the nature and complexity of tasks a workstation will be required different software applications, and each software application requires a certain level of computer hardware support in order to perform properly. It is the task that determines the type of software used, in turn; the hardware needs are determined by the level of computing support required by the software. For example, geographic information systems (GIS) are complex software applications designed to transform raw data into maps that can be used for a number of purposes. Police and fire departments may use GIS software to plot destinations, design emergency routes and locate landmarks and hazards. However, GIS software requires a substantial amount of RAM to function properly. Some professional GIS software applications will not operate without a minimum of 256 MB of RAM. A software application will not function correctly or at all if the workstation is not equipped with the minimal hardware support as recommended by the software manufacturer.

It would be easy for an organization to simply purchase the most powerful and highest performing workstations available; however, purchasing workstations with excessive computing power for routine tasks would be a poor use of financial resources. Instead, it is important to strike a balance between the organization's need and its requests.

An organization should have a solid understanding of its workstation needs. A comprehensive computer hardware inventory of the county's workstations and printers make it easier to determine when equipment may need replacement. Once an organization identifies its workstation needs, it must determine which workstations are adequate and which should be upgraded or replaced. Organizations use different methods to upgrade or rotate workstations. Some organizations use a first-in, first-

out rotation schedule. Using this method, the oldest workstations are simply replaced as new workstations are purchased. Another common method is the department-level request. Using this method, funds are made available at the department level and the old workstations are rotated out at the behest of department managers. No matter which method an organization implements, the procedure that encompasses the inventory, purchase, upgrade and disposal of all computer hardware equipment should be documented within an organization's IT strategic plan.

Findings

- **The County has performed a basic computer hardware inventory in the past 12 months.**

The county maintains a hardware inventory that includes references to factors found in traditional equipment inventories such as make, model, serial numbers and internal hardware components. The county's inventory, however, does not include all the recommended performance-related information found in a comprehensive computer hardware inventory such as processor type and speed, the amount of RAM in each system, hard drive capacity, type of NIC and other factors.

- **The county maintains active workstations that require hardware upgrades or replacement.**

One of the recommendations outlined in Issue 2.1 is to move the county's data into centralized databases on a central file server. To access, share and distribute information in a database, the county's workstations must possess sufficient internal hardware components to perform these functions. Of the workstations reviewed, some require hardware upgrades or replacement. Additionally, court staff said the county has budgeted for five new workstations in the 2003 budget.

- **The county has received at least one price for computer workstations within the last twelve months.**

In August 2002, the county received a proposal (quote) from a local vendor to install basic networking hardware and cabling that would facilitate broadband Internet connections and provide four new computer workstations. The workstations that were noted in the quote contained sufficient performance hardware to meet the county's current needs.

Recommendations

Standardize the county's computer workstations and technology procurement options.

- A. Perform a comprehensive hardware inventory of all the county's computer hardware, including all current desktop workstations and a future network server.**

The county should perform a comprehensive inventory of the workstations and printers that are currently used by the county. Issues such as allocation of computer hardware resources, potential purchases or budgeting cannot be accurately developed without first performing a comprehensive inventory of computer hardware.

Unlike traditional hardware inventories in which the focus is on asset control, a comprehensive computer inventory will provide performance-related information about the computers as well. The inventory should be conducted on each workstations and should include a range of performance-related aspects for each. The county should conduct an inventory of hardware at least once a year, and the process should be clearly documented within the county's overall IT strategic plan. Maintaining an accurate and comprehensive hardware inventory, especially of workstations, is essential.

An inventory can be developed using a basic spreadsheet application or one of numerous software applications that have been developed specifically for inventory management. It is recommended that the county research software applications options.

- B. Establish minimum computer hardware standards for workstations.**

Each software application requires a minimum level of hardware support to perform adequately. The type and sophistication of a software application determines the level of hardware support required.

The county should review all of the software applications it uses and any software application the county plans to introduce over the next two years, which should be identified in the county's overall IT strategic plan. Each software application provides information about recommendation hardware support requirements, and these minimum standards are generally noted on the packaging or are available from the software manufacturer. By establishing the current and projected hardware support needs, the county's staff should be able to develop minimum hardware for all the workstations currently used by the county.

Determining which workstations the county replace or upgrade is easier when a minimum standard for hardware is established. To make this process easier for

the county's IT coordinator, the outline below has been provided as a general guide for establishing a minimum hardware standard. It recommends that any workstation that does not contain the attributes listed below should be scheduled for upgrade or replacement over the next fiscal year.

Each of the listed hardware components is contained within a standard PC-compatible workstation and is listed next to a set of performance-related attributes. These attributes should reflect a minimum performance standard for each workstation.

<u>Workstation Hardware (individual components)</u>	<u>Performance Attributes (description of performances)</u>
Processor (CPU):	At least Pentium 4 Architect
Processor Speed: also referred to	At least 2000 Megahertz (MHz), to as 2.8 Gigahertz (GHz)
Hard Drive Capacity:	At least 40 Gigabytes (GB)
used as primary	(especially if hard drive is storage)
RAM Memory: of random	At least 512 Megabytes (MB)
Compact Disk (CD_ROM): compact disk media	Memory Must be equipped with
Compact Disk (CD-RW): primary backup.	read-only If CD media is used as
Disk Drive: read/write	Must be equipped with 3.5" diskette drive
Modem:	Not needed if connected to
LAN	
Ports: least two USB	Must be equipped with at ports
Connectors: least one RJ-45	Must be equipped with at connection
Networking: 10/100 NIC or better	Must be equipped with
Monitor: CGA or EGA	Must be at least VGA – No monitors

A monitor is considered a peripheral device but is primary tool used to view computer output. Any monitor that is not considered a video graphics array (VGA) monitor should be scheduled for replacement. The outline includes two video display formats: EGA format, which uses an enhanced graphics adapters, CGA format, which uses a color graphics adapter. Both EGA and CGA formats use obsolete color adaptor technology that does not provide adequate resolution for newer software applications. CGA and EGA monitors are no longer manufactured.

It is recommended that the county establish a minimum hardware standard to assist in the scheduling of hardware upgrades or replacement of workstations. The specific standards listed above have been provided to help the county develop a workstation standard, but is meant only as a general recommendation. Special circumstances may dictate a need to deviate from timetables developed to implement the minimum hardware standard.

These recommendations have been compiled with the knowledge that the county of Claiborne currently maintains a hardware formal based on IBM/PC-compatible systems, which tied to a platform that encompasses a computer industry standard for hardware developed by IBM.

C. Implement a purchasing plan dedicated to optimizing the existing budget so desired hardware standards can be attained and maintained.

An approved IT plan provides documented purchasing guidelines, allows organizations to forecast hardware needs accurately and prepare a budget that will meet anticipated needs. Additionally, an organized purchasing process will allow the county to devise purchasing strategies to maximize the county's IT budget. For example, most computer hardware is sold with optional service and support contracts of varying degree and cost. Understanding the needs of the organization will ensure the county makes purchasing decisions that do not exceed or fall short of the anticipated support needs. The process of computer hardware acquisition, related service contracts and the rotation of technology should be clearly outlined in the county's IT strategic plan.

The county of Claiborne is considering the purchase of additional desktop workstations within the next year. There are factors that should be considered when weighing the option to purchase or lease required equipment. Leasing can be advantageous because it allows the cost of technology to be evenly budgeted Over a given period, and technology hardware tends to depreciate rapidly. Leasing also assures a scheduled rotation of technology, assuring an organization will have the newest technology available. Purchasing can offer just as many advantages as long as the hardware that is purchased can be upgraded as needs and technologies change. The decision whether to purchase or lease should be weighed with each major purchase.

Whenever possible, it is advisable to supplement purchases with grants. The Grant process is rarely easy; however, there are numerous organizations and consultants dedicated to assisting with grant request preparations.

Structure the Management and Use of The County's Information Technology.

Background

Policies are approved standards that guide operations and include the rules and regulations that govern an organization. Procedures are the standardized implementation of established policies. Policies and procedures guide employees through daily operations and determines how an organization should achieve its goal. Documented policies and procedures specify how tasks should be performed to comply with organizational guidelines and standards as well as applicable federal, state and local laws.

Policies not procedures can serve as training aids for new employees and as an organization's performance benchmark, once training has been completed. Policies and procedures also help ensure that workers who rarely perform a certain task can do so competently and consistently. Policies and procedures also can serve as a management tool because they illustrate management's expectation.

Written procedures should clear and succinct and allow operations to continue if one or more employees are unavailable for an extended period or leave employment. Procedures are especially valuable if an employee has sole knowledge of a particular responsibility, and that employee is not available. When a department experiences the loss of one of its key employees, the remaining staff faced with the tasks normally completed by the absent employee or the task is postponed or goes undone entirely. If employees assume a responsibility and do not have experience in the area, it is an ineffective and insufficient use of their time. Written procedures help these employees to perform the task without wasting valuable time.

Procedures provide detailed instructions on the job duties and responsibilities of a department and can be used to help set job performance standards for individual employees. Effective organizations incorporate employee input when developing, adopting or updating procedures, because they are the ones most familiar with the processes.

An organization should properly document policies and procedures. Documentation is a formal and permanent means of conveying information. Documented policies protect an organization from lawsuits and claims by staff who say they misunderstood or were unaware of policies. Documentation incorporates policies, rules and information that must be distributed to all employees so their efforts can be directed and coordinated correctly. Policies and procedures aid an organization in holding staff accountable, ensuring that employees understand and use an organization's resource appropriately.

Every organization that uses information technology (IT) should have documented policies and procedures outlining the use, access, storage and security of all hardware, software and information maintained or passed through an organization's computer network and system. "Acceptable Use" policies Address IT equipment, e-mail and Internet access and provide general guidelines for their use. Among the issues addressed should include approval procedures for mass e-mailings and external network connections. Employees also should be informed of unlicensed or shared software policies.

The following list represents general IT policy categories that should be addressed as organizations grow and become more technologically sophisticated:

- IT hardware and software acquisitions;
- desktop and network management, which should include security and user authentication;
- training for end-users and IT support processes, which should include onlining reporting processes for state agencies. Also, training includes equipping users with the knowledge of security risks;
- IT hardware and software service and maintenance;
- e-mail and Internet acceptable usage policies;
- data integrity, which should include file backups, as well as access and retrieval procedures. Archival copies are important for security, disaster recovery and recovery retention requirements. A data policy should convey the manner in which personnel in the organization create, access, manipulate and save data;
- data retention and destruction schedules. Legal and local requirements for documents including e-mail storage and retrieval should mirror the Public Information Act requirements,
- IT hardware and software inventories and asset management;
- password and access code requirements;
- security, which should includes privacy and "confidential by law" records versus open records. Privacy includes safeguarding individuals' personal or sensitive information;
- Web site posting and content updates/changes submissions should meet the goals and expectations of the organization as a whole. Care should be taken to ensure

that content also stays within the confines of state and federal laws, including copyrights;

- shared software requirements. Software licenses should be either specific to machine or a site license should support multiple machines. Audits to ensure compliance with copyright and property laws should be regularly scheduled and enforced;
- consistently using tested software updates and periodically reviewing human processes and procedures; and
- consistent revision and distribution of policies and procedures. For example, Senate Bill 694 of the 2002 Legislative Session requires confidentiality of e-mail addresses for members of the public, meaning that a city cannot give out or sell citizens' e-mail addresses.

These policies and procedures should be viewed as a starting point and not a final list. They should be regularly reviewed to make sure they accomplish the organization's IT goals. Over time, they should be revised as necessary.

Policies and procedures should be disseminated to all employees either on paper or posted electronically on an internal employee Web page. Whichever the method, the policies and procedures should be updated and distributed to each employee regularly. Even the best procedures manual cannot prevent problems from arising. Well-written procedures, however, can prevent legal problems from arising.

Findings

- **The county does not have formal, documented policies and procedures related to its use of IT equipment.**

The county was unable to produce comprehensive IT policies or procedures that address the proper use of IT throughout the county; including access, usage, storage and retrieval. Even though different services, there are standard parameters that departments should use as guidelines. The guidelines should ensure compatibility with automated systems and cost efficiency. Without IT policies, the county does not have a documented and approved strategy for addressing IT issues as they arise. As a result, the county can only react to IT related problems; it cannot prepare for them.

- **The county does not have an IT manual or an internal Web site for posting policies and procedures.**

Currently, the county does not distribute any IT policies or procedures to its staff. Departments use their own discretion on whether or not to create and follow policies and procedures. Failure to document and distribute policies and procedures can lead to miscommunications and misunderstandings.

Recommendations

Structure the management and use of the county's information technology.

A. Develop written IT policies and procedures.

The county develop comprehensive policies and procedures addressing IT-related Issues. To accomplish this task, the county should designate a technology committee or team of employees that includes a representative from each department to research and formulate comprehensive IT policies and procedures.

The county's comprehensive IT policies and procedures should address the fundamental list of topics included in the background section of this issue, including Web page content and instructions for doing business with county. The counties of similar size to compare and leverage applicable aspects of their IT policies.

B. Disseminate documented IT policies and procedures to all staff.

The county should distribute the completed policies and procedures, and subsequently revisions, in a comprehensive manual, similar to the county's personnel manual. This manual should be a flexible tool to address a number of possible scenarios.

If all county departments are connected to the proposed LAN (see Issue 1.1), an internal electronic version stored on the central county server will allow employees quick and easy access to the information.

Implementing this recommendation will require staff time; however, the costs of developing a policy and procedures manual for technology in the budget as a part of long-term planning.

C. Assign an employee to oversee any updates, maintain a master copy and disseminate changes to the county's IT policy and procedure manual.

A comprehensive IT policy and procedures manual must be maintained and updated once it has been developed, documented and disseminated. Organizations should expect changes and additions. Staff should review the county's policies and procedures every six months to ensure the contents are current and accurate.

The task of maintaining the county's IT policy and procedures manual should be assigned to a designated employee; however, it does not have to be an IT employee. While only the designated person should physically amend the manual, all departments and employees should be encouraged to submit changes and additions. Maintaining the manual should not increase the county's IT costs.

Coordinate the County's Information Technology Support and Service Responsibilities.

Background

Information technology IT is part of the basic infrastructure of today's organizations. The ability to collect, store, search, analyze and distribute information is vital to efficiently conduct essential operations. IT plays an ever-important role in managing information as the amount of information increases. It, however does represent a significant and recurring expense to any organization.

The average enterprise issues as much as 12 to 30 percent of its information technology budget due to poorly managed IT assets. Specifically, this loss is due to poorly monitored and maintained software licenses, maintenance and support agreements. In recent years, compliance enforcement agencies such as software auditors have charged businesses and government agencies with the improper use of software assets. The settlements of those charged have ranged from \$30,000 to \$50,000 and beyond . Actual costs of these problems average four to six times the cost of the settlements alone. The goal of managing the IT assets of any organization should be to become a well informed information technology buyer and to negotiate agreements that strategically match inventory to user needs. Therefore, asset management requires reviewing and monitoring purchases and maintenance and support agreements.

Efficiency demands that an organization have a clear understanding of the size, condition and value of its assets. In June, 1999, the Government Accounting Standards Board (GASB) issued statement number 34 regarding basic financial statements for state and local governments. In this statement, "capital asset management inventory is essential to realizing the true costs over the useful life of the asset. Additionally, asset tracking helps in planning for future purchases and improvements by examining the age, maintenance and support of equipment.

In addition to managing asset inventory, IT administrative tasks often include:

- desktop or workstation support
- network management;
- database management;
- software application integration or development;
- e-mail and messaging management;
- e-commerce (e-government) management
- web site maintenance;
- installation;
- configuration;
- service and support;
- hardware and software upgrades;
- system settings modifications;
- training;
- security (including management of user authentication processes);
- controlling and documenting software licenses; and
- final disposition of outdated hardware.

Organizations have three basic options when deciding how to provide service and support for IT. Under the first option, an organization can employ a full time, dedicated in-house IT or systems administrator and, depending on size of the organization, support staff. IT administrators handle the day-to-day management and operations of automated systems within an organization and respond to technology related problems. At a minimum, responsibilities should include evaluation, installation, configuration, repairs, general maintenance, upgrades and security measures, including data integrity and network problems. This employee also serve as the organization's IT coordinator or point-person for technical help.

Full-time, dedicated IT administrators earn salaries that average between \$75,000 to \$95,000 annually. Although this is an expensive commitment, organizations benefit by saving time by eliminating outsourced, service-related expenses. In a majority of organizations with more than 15 computers, hiring an IT or systems administrator is the most cost-effective long-term solution for regular maintenance needs. Older computer systems with a mix of hardware also may be easier to maintain with regular system administrator.

Before hiring a dedicated IT administrator, an organization should determine if a current employee could be trained to handle this position. Reallocating an existing staff person allows the organization to take advantage of the employee's familiarity with the organization itself as well as its IT infrastructure and equipment. In many small entities, an existing employee may be trained to perform simple computer-related tasks and rely on individuals from outside the organization with special expertise for higher-level, IT operations and service. It is then incumbent upon the

organization to prioritize the employee's duties and functions to limit any reduction in the efficiency of overall operations.

As a second option, an organization can contract, or outsource, the IT service and support responsibilities. Requests for support can usually be accommodated over the telephone, and often this support is included as part of hardware or software purchases. Service, however, usually requires on-site work or assistance from contracted IT professionals. A local vendor who charges an hourly rate or a contracted subscription of service time provides the most cost-efficient, outsourced service arrangements. Organizations should be wary of service vendors that must travel long distances, because the organization will be billed for travel time.

Small organizations often engage outside vendors for IT service and installation rather than pay the high cost of employing a full-time IT administrator. It is important, however, for the organization to assess the value of a third party vendor and ascertain whether the vendor can offer benefits above and beyond what your in house staff can provide." With a new focus on security issues, the private sector has the expertise and capability for innovative technologies and implementations. Problems may arise, however, due to a contractor's lack of experience with an organization's existing IT infrastructure and systems. This situation might result in unexpected add-on costs. It is important to negotiate an IT service contract that clearly states a desired performance or service level standard using a simple billing structure. There are many examples of failed partnerships with vendors, usually because the organization did not define its requirements and expectations properly.

If an organization chooses to outsource service responsibilities, it is important to establish an internal IT coordinator to handle all service requests. An IT coordinator should be responsible for all IT service support contracts and service as the only employee authorized to call for outside service. Designating an IT coordinator who is already a member of the organization offers the advantages of previous experience with the IT infrastructure and the organization's operations. Increased duties, however, may strain the individual's ability to work effectively and could require additional compensation.

The third option suggests pooling resources with private companies or other public organizations to share the services of a professional IT administrator. Sharing an IT administrator can save an organization the cost of a full-time IT administrator. Job expectations, should be negotiated in advance to avoid miscommunications of the person's availability. Many public entities are establishing local community networks to share IT resources and help retain dedicated IT administrators. Options including sharing with other surrounding public entities such as cities, counties or school districts.

Federal and state grants are more readily available for communities that consolidate their needs. Such partnerships enable government entities to expand user access,

organize local information, improve communications, promote economic development and otherwise take advantage of advanced technology.

The Commerce Department's National Telecommunications and Information Administration (NTIA) grants awards through the Technology Opportunities Program (TOP) to extend economic opportunities, including e-Government, to non-profit organizations and state and local governments.

Many universities are willing to assist local communities with its technology development. A nonprofit community development group report released in November 2002 said, "few community development groups used technology innovatively but when they did, it was through university partnerships." The report went on to define the variety of roles offered, which including consulting, designing and service.

Deciding how best to service and support an organization's IT operations involve analyzing the costs and benefits of these three basic options. Issues to consider when determining an IT service and support arrangement include:

- the size of the organization and the number of workstations and service used;
- the IT service and support budgets;
- the willingness of surrounding entities to share resources;
- the amount of service and support needed; and
- the trade-off between immediate service availability and cost.

Local governments should always budget for IT administration from their general fund. Better still, they should use a dedicated IT capital fund, because service and support will always be necessary.

Findings

- **Claiborne does not employ an IT administrator/coordinator on a full or part-time basis.**

Many Mississippi counties do not employ a systems or network IT administrator and often rely on county employees who possess knowledge about computer systems or networks. Often, these employees provide assistance in addition to their primary job which may or may not be associated with IT functions.

Although the county, demonstrates versatility by using existing staff for informal IT support without formal training, it is not an optimal way to address the county's increasing IT support needs.

- **Each county department requests IT service independently.**

The county does not have a standard, formal or consistent process for requesting IT assistance from outside vendors. Each county department independently calls IT service as needed, resulting in service calls that are not coordinated or consolidated. This situation could result in numerous and unnecessary on site service calls. As identified IT coordinator could efficiently consolidate and reduce service requests.

Recommendations

Coordinate the county's information technology support and service responsibilities.

- A. Formulate the specific IT support and service needs of the county's IT coordinator.**

The county council should organize a small committee of stakeholders to review the IT administration and coordination needs of the county. The core group should include individuals familiar with the technological systems of their respective departments.

The committee should determine the roles and responsibilities of the proposed Claiborne IT coordinator and recommend a current employee to be in charge of IT related issues, including asset inventory control and supervising data backup and updates of virus protection for all departments/offices. The job responsibilities also could include consolidating IT purchases and requests for service and monitoring IT maintenance agreements and inventory reports. Moreover, the county should assign the IT coordinator to monitor and seek technology resources available through the state and federal government. In essence, the committee should define the coordinator's authority and responsibility to provide county employees a single point of references for IT issues, including service requests and purchase.

Individual departments should continue to be responsible for contacting their respective software vendors for general phone support that accompanies individual purchases. The IT coordinator should only be responsible for maintaining and coordinating on-site IT service requests.

- B. Evaluate support and service options that would satisfy the county's needs.**

Consolidate and Standardize the County's E-Mail Services

Background

Although electronic mail (e-mail) has only been widely available for just over a Decade, it has become critically important in the modern office environment. E-mail offers organizations a fast and relatively inexpensive way to communicate within the organization or with external clients or constituents. Given the increase in e-mail traffic during the last decade and the subsequent reliance on e-mail, many organizations no longer use standard network servers to pass and restore e-mail traffic. Instead, even smaller organizations are turning to dedicated e-mail servers to transmit, store and monitor the sheer volume of e-mail messages generated by their organizations. Unlike network or file servers, e-mail servers are designed to store, monitor and control the flow of e-mail messages that are passed through the organization's local area network (LAN).

Smaller organizations that do not have the technical staff or budget for a network or systems administrator may choose to outsource network-related responsibilities, such as e-mail. When a vendor stores and maintains e-mail accounts for an entire organization, it is referred to as e-mail hosting. E-mail accounts hosted by a vendor are commonly referred to as Web-mail accounts, but for purposes of this report, all such accounts will be referred to as hosted e-mail accounts. The vendor that provides these services is referred to as an e-mail hosting services provider (HSP). Using an HSP for e-mail services can help an organization to avoid the costs of owning LAN-related hardware such as an e-mail server. Instead, individuals within the organization can access their e-mail accounts by logging onto a server that is owned, housed and maintained by a vendor. Issues such as server maintenance, reliability and security are handled by the HSP.

Smaller organizations that do not have the technical staff or budget for a network or system administrator may choose to outsource network-related responsibilities, such as e-mail. When a vendor stores and maintains e-mail accounts for an entire organization, it is referred to as e-mail hosting. E-mail accounts hosted by a vendor are commonly referred to as Web-mail accounts. The vendor that provides these services is referred to as an e-mail hosting services provider (HSP).

This method may raise concerns about the privacy and integrity of an organization's data. E-mail traffic between two points contained within a building is usually on the same local area network (LAN), and operates behind the relative safety of an organization's firewall, a device designed to protect data and

contained on a LAN. An e-mail sent or received over the Internet must leave the security of the LAN and is more susceptible to a host of security threats. In the case of hosted e-mail accounts, the actual server that stores an organization's e-mail accounts may be hundreds of miles away from the organization. For a user who is attempting to access their e-mail account, however, the physical location of the organization's server is irrelevant and, in general, has no bearing on performance.

There are legitimate security concerns and risks associated with transferring data outside the relative protection of an organization's LAN. To address these vulnerabilities, an HSP vendor may wrap a layer of security software and hardware around an organization's e-mail data that is referred to as a virtual private network (VPN). A VPN is constructed by using publicly shared wires (Internet) to connect one organization to another, and then introducing security measures that create a protected environment, which allows the confidential flow of e-mail traffic between organizations. There are numerous ways to build a VPN that can provide protected networks using the Internet for transporting data. These ways use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

An HSP can provide remote storage and administration e-mail accounts, but not all can or will provide a VPN for hosted e-mail accounts. In the scenario, an organization's e-mail traffic may not be afforded adequate protection from intrusion. For this reason, it is important that an organization identify security priorities and options when considering a vendor to host e-mail services.

For about \$3 per month for e-mail account, an organization that wishes to have 100 hosted e-mail accounts could expect to pay approximately \$300 a month, just to have an adequate number of uniform e-mail accounts. Some organizations may be unable or unwilling to pay this recurring monthly fee for general e-mail services, but there are public agencies and private organizations that provide free e-mail hosting services. For example, the County Information Resources Agency (CIRA) provides Mississippi counties with free, secure e-mail accounts to any county government that is a member of CIRA.

Organizations generally use a Web domain name (Web address) as a foundation for their e-mail accounts, which are often established for each person within an organization. For example, if John Smith was an employee for Claiborne County, Mississippi, his address should be similar to john.smith@co.claiborne.ms.us. Most commercial organizations use a similar format as well, for example, if John Smith were employed by a fictitious company such as Acme Sprockets, his e-mail address could be john.smith@acmesprockets.com. An e-mail address can be broken into three segments: an individual's name or title, a domain name that usually reflects the name of the company or organization and the suffix that usually indicates the type of organization (i.e., .com, .org, .net, .gov., .us). An individual's name and the organization's name are separated by the ":"@"" (at) sign to signify

that an individual's named in the first segment is part of the organization or company named in the domain segment of the e-mail address <FirstName.LastName@OrganizationName.com>.

Some public entities use e-mail accounts offered through their local Internet service provider (ISP), (i.e., hazard.county.judge@aol.com) or they may use free e-mail accounts offered on the Internet (i.e., hazard.county.commissioner2@hotmail.com). Both of these practices are strongly discouraged because constituents may view this as less secure or less professional. Additionally, all public entities such as cities and counties are discouraged from using the, com and .net suffixes in their Web sites addresses or e-mail addresses because they are reserved for commercial entities. The IANA/CORE (Internet Assigned Numbers Authority/Internet Council of Registrars) is the authoritative body that develops e-mail formats for public and private entities, and they have developed a specific format for Mississippi cities and counties: john.smith@ci.CityName.tx.us and john.smith@co.CountyName.tx.us. The IANA/CORE acknowledges that the newer e-mail address formats public Entities is more obscure, however the protection and uniformity will make the new format the de facto standard for public entities within five years.

Findings

- **The county has different e-mail formats because each department in the county uses a different (dial-up) or cable broadband Internet service.**

The county uses e-mail accounts with multiple ISPs and each has a different type of e-mail addressing format (i.e., <personal.account@msn.com>, employee.name@rr.roadrunner.com and <county.department@juno.com>). Some constituents may perceive the lack of uniformity among the county's email addresses as confusing or unprofessional.

- **Name of the e-mail accounts currently do not reflect the county's domain name or comply with IANA/CORE naming convention standards for governmental entities.**

None of the county's current e-mail addresses comply with the e-mail naming conventions outlined by the IANA/CORE, the authoritative body that has established specific e-mail address formats for Mississippi counties.

Recommendations

Consolidate and standardize the county's e-mail services.

- A. **Install a dedicated e-mail server for county-wide use.**

The county should abandon the use of multiple/personal e-mail accounts.

Recommendations

Consolidate and standardize the county's e-mail services.

A. Use the services of a single e-mail host service provider in lieu of purchasing and supporting a dedicated e-mail server.

The county should abandon the use of multiple e-mail service providers (ie: MSN, Juno, etc.) and secure e-mail services through a single HSP. Using a single e-mail HSP ensures that each of the county's e-mail accounts has the same level of reliability, security, uniformity and also provides the county with a single point of contact for service, support and billing. The use of hosted e-mail accounts also would be beneficial considering that the county departments are not yet networked. Hosted e-mail would enable employees to remotely access e-mail accounts whether they are connected to the Internet through cable broadband or telephone (dial-up) lines. Securing e-mail accounts through a single HSP is recommended regardless of whether or not the county purchases a network server. The county could secure e-mail hosting any number of e-mail HSPs for about \$300 per year. This generally includes about 20 hosted e-mail accounts, and the e-mail accounts would reflect the county's Internet domain name (employee.name@ci.claiborne.ms.us). Additional cost saving could be realized by using the same company for both ISP and e-mail hosting, and this recommendation is specifically addressed in recommendation B of this issue.

Purchasing and maintaining a dedicated e-mail server in house has some advantages, such as enhanced security because e-mail messages can be exchanged behind the relative safety of the county's Internet firewall. Storing (hosting) and maintaining the county's e-mail accounts on its own server is preferable to the e-mail HSP option if any entity has the network infrastructure, funding, volume and on site resources to provide an acceptable level of e-mail support. Claiborne would be better served to acquire the services of an e-mail HSP.

B. Secure free or reduced e-mail services through Vendors, or county's current cable Internet service provider.

The county receive cable broadband Internet service through an alternate service provider. As part of the broadband package, the county is eligible for ten free e-mail accounts. At the county's request, the ten hosted e-mail accounts could be configured to reflect the county's registered domain name<firstname.lastname. By using Time Warner as the county's ISP and e-mail HSP, the county would be able to receive uniform and IANA/CORE compl@ci.claiborne.ms.us>. In addition, the county would be eligible for additional ten e-mail accounts for \$10 a month, bringing the cost of the twenty e-mail accounts needed by the county to approximately \$10 a month.iant e-mail addresses at the substantially reduced rate of \$10 per month for 20

hosted e-mail accounts. The county should contact Barry Watson, sales representative at Time Warner, to discuss rates and available services.

C. Adopt an e-mail address format that complies with the IANA/CORE standards for municipal entities.

The county should adopt a unified format for all e-mail accounts that would reflect the IANA/CORE standard (<employee.name@ci.claiborne.ms.us>). The IANA/CORE recommends a standardized format for public e-mail accounts modeled after its recommended public entity domain format. For example, the e-mail address for an individual employee in the county of Claiborne should be john.smith@ci.claiborne.ms.us; a county officer may choose to use a title and name, such as judge.smith@ci.claiborne.ms.us; an entire department can be identified by name, such as police.department@ci.claiborne.ms.us. As these mock examples demonstrate, the <@ci.Claiborne.ms.us> portion of the address must be a part of all county e-mail addresses.

Since the IANA/CORE format is reserved for all local government entities, it can be used with any HSP that hosts county e-mail accounts. Establishing e-mail that reflects the IANA/CORE standard should result in minimal cost and can be arranged through any e-mail HSP. In the case of Claiborne, the county's current cable broadband ISP (Time Warner) may be willing to offer the e-mail HSP services described above. See recommendation B for additional information.

Finally, it is recommended that all county documents containing e-mail contact information, including business cards, should eventually be amended to reflect the county's new e-mail format.

Establish and Maintain an Official County Web site.

Background

The Internet is a global network connecting millions of computers in more than 100 countries, which form a web of computers designed to share information. Unlike some computer networks that store everything on one central computer, the Internet is not centrally controlled but rather decentralized by design.

A web site is a virtual location on the Internet, each Web site is owned and managed by

an individual, company or organization. A Web site generally contains content, documents and files that pertain to the organization that owns the site. Each Web site contains a home page, which is the first document users see when they enter the site.

It is becoming standard business practice for both public and private organization to maintain an Internet Web site because it offers local governments new efficient ways to serve their citizens. A Web site offers governments a means to communicate effectively with employees, customers and constituents. A county's official Web site also serves as a window into the operations of county government. The proliferation of the Internet during the past decade has created citizenry who are comfortable purchasing goods and services and searching for general information from online sources. A natural progression for governments is to offer similar services to its citizens.

Each Web site has an address known as a uniform resource locator(URL). Much like An address on a letter and sent through the mail, proper address must be provided or the letter may not reach its intended destination. A URL is the global address of documents and other resources on the Internet. As we noted previously, the terms Internet address, Web address and URL are often used synonymously. Unlike a street address, URLs are contained in just one line of text, but are segmented into sections and each of the URL serves a distinct purpose.

An example, though fictitious, of a segmented URL is www.acmesprockets.com. The first part of the address allows the computers involved to establish a protocol, or manner in which they plan to exchange data. The second segment specifies an Internet protocol (IP) address, more commonly referred to as a domain name where the resource is located. In the example provided, the Internet domain name of this Web site is acmesprockets, and infers that the Web site is owned by the Acme Sprockets Company. The third portion is the top level domain(TLD), which refers to the suffix attached to Internet domain names. Using the example, we see that the TLD for the URL is .com. This simply implies that the organization that is registered at that URL is a commercial entity, thus the suffix.com.

There are a number of predefined suffixes, and each represents a TLD. Current TLDs, include the commonly seen .com for commercial business, gov which is delegated to U.S. Federal government agencies, .edu which is delegated to educational institutions such as universities, .org which is delegated to organizations (mostly non-profit), .mil which is generally delegated to U.S. and NATO military entities, .net is generally delegated to network organizations and there are many more. Some TLD suffixes refer to the country in which a particular organization is headquarters such as .ca for Canada, .th for Thailand and .us for the United States. These TLD suffixes are established by the Internet Council of Registrars(CORE), and are established as general guidelines only. The types of TLD suffixes increases continually to accommodate the large number and types of organizations establishing a Web presence.

Unfortunately, these Web site address standards were not in place when public entities began to establish their Web presences in the 1990s. This resulted in numerous Web site addresses formats for cities, counties and state governments. To alleviate problems associated with these inconsistent government Web site addresses, new standards were set, in principle, by the Internet Assigned Numbers Authority (IANA), and the Internet Council of Registrars(CORE). The protected, de facto address format for city entities became; www.ci.city-name.state-abbreviation.us. For example, in this newer format The official Web site for Dallas, Texas, would be found at Internet address;www.ci.dallas.tx.us. The IANA acknowledges that the newer addressing format is more obscure; however, the protection and uniformity will make this new format the standard within five years.

Most organizations lack the in house expertise to create and maintain an official Web Site, so most companies outsource Web site services. Web site services vendors generally provide three types of services; development, hosting and maintenance. Web site development, sometimes referred to as Web design, is the most expensive aspect of Web site services because it involves transforming information that an organization would like to have on its Web site into a format that can be viewed by Internet users. Some Web sites may contain 500 individual Web pages, all of which must be prepared with general text, pictures, graphics and hyperlinks.

Web site hosting refers to storing the contents of the Web site on an Internet server, so that anyone on the Internet can access the organization's Web site. In essence, the county is renting space on an Internet server.

A county's official Web serves as a window into the operations of county government and allows a county to provide to a myriad of information to better communicate with its citizens. For this reason, once a Web site is up and running, it must be maintained so it continues to operate correctly and it must be routinely updated so that information contained on the Web site is current. County governments routinely post contact information for each department, meeting schedules, agendas and minutes. Keeping this type of information on the county's Web site current requires frequent modifications. Changing the content on Web pages may require the services of a Web maintenance professional. Web site changes generally require familiarity with special coding languages, such as hyper text markup languages (HTML), which is most common Language used to create and display content for Web pages. For this reason, making numerous changes to an organization's Web page can be expensive.

Some organizations have attempted to circumvent the expense by providing staff members training in HTML so that members of the organization can make changes to the Organization's Web site, not a Web services vendor. Other organizations use one of many Web content management software applications available. As the name implies, the Web content applications are designed so that users can make changes with little or no Web coding experience, using a more familiar desktop publishing (DPT) format similar to a word processing software application.

No matter which option an organization uses to make changes to its Web site, there should be a process in place to ensure that any information posted to an organization's Web site has been reviewed and approved by a dedicated Web content manager. The best way to ensure that Web content meets with the organization's approval is to establish policies and procedures regarding an organization's Web site content.

Historically, Web site content included primarily static information about an organization; however, over the past few years, electronic transactions through Web sites have become commonplace. Some Web sites contain more than just informational content and move into the realm of e-commerce or e-government when referring to financial/business transactions that take place between citizens and government entities. E-government refers to the practice of providing government services through the Internet, one of which is to collect different types of taxes, fees and entities offer citizens the option of making payments over the Internet.

To receive payments over the Internet, a Web site must be fitted with a payment engine, specifically designed software programs that allow individuals to perform financial transactions via the Internet. A payment engine allows an organization to accept electronic credit card or checking account payments via the Internet, process these transactions and settle the funds within the organization's existing financial systems. Payment engines are developed with different levels of security to ensure that customer and citizen information that is provided during the transaction is protected.

Providing government services on the Internet increases the level of customer service by offering options to citizens, such as the convenience of paying for services without leaving their homes. The acceptance of online payments has many long run cost advantages for governments as well. Online payments afford government the opportunity to process transactions at their discretion, unlike an office environment, where staff must be dedicated to accommodate customers as they arrive. There are three primary methods an organization can use to accommodate the use of online payments.

The least expensive method for implementing online payments is the use of a third-party Vendor who collects online payments. In this example, customers visit a county's Web site to pay a particular fee, such as building permits. The customer clicks on a payment option, and is immediately forwarded to the Web site of an authorized vendor who will collect money on behalf of a county. Once at the Web site, the customer is prompted to provide information about the fee, fine or tax they wish to pay. The customer provides the fee-related information, as well as payment information such as a credit card or checking account number. Once processed, payment is electronically transferred to the county's financial accounts. This method uses a payment engine that does not have any specific information or records about the individual paying a fee, raising the possibility that a customer could place incorrect information into the window's provided on the screen, which could result in an improperly recorded fee. The use of a generic payment engine has advantages for smaller organizations because it does not require additional back-end technology, or the sharing of data with a third-party vendor to accommodate the online payment transaction.

A second, and less common, method incorporates the use of electronic transaction software that interacts with an organization's financial database. This method differs from the previous example in that payment engine software has the ability to gain access to a portion of a county's financial database. A customer who wishes to make payments using this type of payment engine would be required to provide authentication information, such as a password. Once an account is open, an individual can view limited versions of records that pertain to the individual, such as home values and property taxes. If a customer desires to pay their property taxes over the Internet, they could review their tax information and make payments using a credit card.

This type of payment engine is sophisticated and uses the software that can retrieve an individual customer's account records, provide immediate feedback to online customers, accept payments, post transactions to correct accounts and provide receipt information. For this reason, a software vendor is generally used to develop a custom fit payment engine for an organization, as well as maintain the payment engine. Even with a vendor providing maintenance for this type of payment engine, a dedicated IT staff would be required to support the databases for the transactions. Cities and counties that prescribe to this type of method often subscribe to these services through Mississippi Online (www.mississippionline.com), the state's e-government portal.

The third option is primarily for large organizations includes using software vendor to develop a custom-made payment engine, and then using their own IT staff to maintain it. Given the complexity and the sophistication of payment engines and transactional software, this option is only plausible for organizations with a large IT staff.

No matter which method is used to accept online payments, customers often pay the cost of this service through a small convenience charge that is added at the time of the transaction. The amount of the convenience charge varies depending on the type and amount of payment received, but is generally nominal. A majority of Mississippi cities and counties do not operate the volume of transactions that would make such a method economical; however, citizen expectations are changing as more people become comfortable with the use of the Internet to perform financial services. It would be beneficial for local governments to adopt a proactive attitude toward the acceptance of online payments and make this an option for citizens.

Findings

- **The county does not have an Internet Web presence.**

The county does not have an official Internet Web site. An official Web site would be a convenient way for the county government to provide a host of information and services to Claiborne constituents and businesses.

- **The county has not registered a Web domain name, would serve as the the county's official Internet address.**

By establishing a domain name, the county will have a specific Web site address, which is a virtual location on the Internet. Although no one except the county would be allowed to use the county's Internet Web site address (www.ci.claiborne.ms.us), the county still has to go through the process of registering a domain name, which involves contacting a domain registrar or a company that registers the domain name on behalf of the county.

Recommendations

Establish and maintain an official county Web site.

A. Register the domain name www.ci.claiborne.ms.us as the county's official Internet address.

Prior to establishing an Internet Web site, the county must register a domain name that will serve as the county's virtual location on the Internet. The county should contact a domain registrar to register its domain name so that no other entity, public or private, can trespass on the county's Internet address. The services of a domain registrar are relatively inexpensive, and governmental Entities can register a domain name for about \$50 per year. Most Web site vendors or ISPs will register a domain name for a nominal fee. Time Warner Cable of Jackson, the county's current cable broadband Internet service provider, may be willing to serve as the domain registrar at no cost.

The specific domain name www.ci.claiborne.ms.us complies with the recommended format www.ci.county-name.state-abbreviation.us for county government prescribed by the IANA/CORE. Additionally, this format facilitates the proper IANA/CORE e-mail format for county employees, which is firstname.lastname@co.countyname.ms.us.

B. Contact with a Web site services vendor to develop and host an affordable County Web site.

The county should establish an official Internet Web site, which will require the county to use the services of a Web site vendor. There are three primary services that are associated with establishing a Web site; development, hosting and maintenance. Most Web site vendors can provide all three services, and it is recommended that the county use only one vendor to provide all three, if pricing and service levels are compatible. As we noted in recommendation A, the county may request the Web site vendor to handle the domain registration process. A Web site must be stored on a Web server in order for it to be viewed on the Internet. Since the county does not have the capacity or resources to store the Web site in house, the county would need a vendor to host the county's Web site. Web hosting fees are generally less expensive if they are purchased from the same vendor that provides other Web services. Using one service vendor is

significantly easier than contacting multiple vendors in the event of a problem.

There are dozens of Web site designers in the Claiborne County area, so the county is encouraged to obtain bids from at least three separate vendors. The cost of content development varies drastically from vendor to vendor, so it is important that the county carefully outline its expectations by developing lists of what information it would like to be placed on the county's official Web site (see recommendation C). Reviewing other County Web sites will help the county to determine the appropriate content the county should have posted on the official Claiborne County Web site.

The market for Web site services has only developed within the last ten years; Therefore, many Web site service vendors have a short business history. For this reason, it is important the county obtain a list of clients from prospective Web site vendors, review some of the active Web sites developed and maintained by the vendor and contact clients to gauge their level of satisfaction with the vendor. The county is encouraged to learn from the experience of other similar-size counties to identify potential vendors.

When discussing cost options with potential Web site vendors, it is important that authorized county employees have the option to make minor changes and updates to county Web site. This helps reduce Web site maintenance costs and ensures that small updates and maintenance can be performed immediately. Some vendors may be opposed to this idea because it reduces potential maintenance-revenue. Even if the county chooses to have all of the Web site maintenance performed by the vendor, it is advantageous for the county to have the option. This recommendation is explored in greater detail in recommendation D of this issue.

C. Determine the specific content to be posted on the county's official Web site and establish policies and procedures for Web site maintenance and the introduction of new Web site content.

To ensure that information posted on the county's official Web site is accurate and has been approved by the appropriate county authorities, the county should implement general policies and procedures that outline the manner in which Web site content is submitted, approved and posted. The policies and procedures should identify which county employees are authorized to post or make changes to Web site content. As a quality and control measure, many counties delegate one or more individuals or a single department to oversee the process of posting Web site content and updates. The specific manner in which Web site changes are made is of secondary importance to having a general policy and procedure in place to address these issues.

Developing policies and procedures for the county's official Web site should be a collaborative effort, and it is recommended that all county offices participate in the process. A Web development/content team comprised of representatives of

each county department should be assembled to determine the specific information or content that will be posted on the county's Web site. For example, each department should have its own Web page that provides specific information about its department, such as names and titles of employees, contact numbers and e-mail links, general summary of services provided, hours of operation and other pertinent information. When attempting to develop a content outline, it is recommended that team members review other official county governments and state agencies Web sites to obtain ideas and learn best practices.

D. Determine ways to make Web site maintenance costs affordable for the county.

The county should consider delegating the task of Web site maintenance to a specific county employee, department or even a county official. Using the county staff to make routine changes to the county's Web site is an inexpensive way to reduce the cost of the services of a Web maintenance professional. In addition, a staff member responsible for Web maintenance serves as a quality control measure because the number of individuals assigned to update the Web site is limited.

In order for staff members to modify the county Web site, they require the proper software tools. In the past, making modifications required familiarity with special coding language such as HTML, however, now Web page content management applications have been designed that allow users to make changes with little or no Web coding experience, using more familiar desktop publishing (DTP) format. Most importantly, the content management applications eliminate the need for employees to learn complex Web coding languages. Using a DTP software application would be especially beneficial to the county, given the limited IT/Web maintenance skills of the current staff. DTP software would allow staff to make changes without a professional Web developer, or at least reduce the frequency in which the services of a Web developer are required.

Web content management software applications vary considerably in price depending on the sophistication of the application. However, there are standard per user site licenses available for as little as \$500.

Even with the more user-friendly DTP applications available, staff members may still require training before they reach a level of competency that is adequate for the county. IT training for Web site maintenance comes in many forms; formal classes; teach-yourself publications or even Web-based tutorials provided via the Internet. While teach-yourself publications and Web-based tutorials may provide sufficient training for some, others may require formal classroom instruction. Web page design and maintenance classes are provided at most technical and trade schools or local community colleges and universities.

The county could also use student interns to assist with routine Web maintenance and other IT functions. Student internships are offered through most universities, community colleges and vocation/technical schools in the Claiborne County area, and they offer a cost-effective way to secure expertise and help. The county should actively seek to participate in a formal internship program such as those offered through local schools such as Alcorn State University, Copiah-Lincoln Community College and Hinds Community College. The county should also consider the Port Gibson Public School District and Claiborne County School District. The county needs to seek if the district has a school-to-career program, that is a formal work-study program for high school students.

E. Explore the possibility of offering e-government services to citizens, specifically the payment of taxes and fees via the Internet.

Although this option may seem progressive, the county should research and eventually offer e-government service options to the county residents. Such services could include submitting forms or applications via the Internet and accepting electronic payments. The county should eventually adopt one of the outlined methods noted in the background section of this issue and implement Online transactions to accept payment for county taxes, fees and fines. These recommendations should be explored, however, only after the county has developed more experience maintaining a static Web site.

Because the county does not have a dedicated IT staff, the simplest way to offer an online payment process would be a third-party vendor who provides generic payment engine services. The generic payment engines provide a platform in which citizens can input information about the tax or fee they are attempting to pay through the county's Web site. Only citizens that choose to use this payment option would have to pay a small convenience fee for the service.

Another option requires the use of a customized pay engine designed by a vendor specifically for the county. The initial cost for a payment engine that is actively integrated with the county's financial information varies greatly, but would be substantial. In an effort to recover these costs, the county could charge a service fee for each transaction.

To avoid such a large initial capital layout, the state of Mississippi provides a portal, or window of services, in which local governments can become a participating member and use their Web applications. The county should investigate these options and choose the option that best fits its needs, which is most likely the use of an online, third-party payment vendor.

Ensure all Critical County Data are Secure.

Background

As organizations increase their reliance on technology, accessing and storing data becomes increasingly important. Data backup simply involves copying files to a second medium as a precaution, in case the first medium fails. All computer users should back up their files regularly. Without a backup, data stored on a server or an individual computer workstation may be lost after a system failure, human error or natural disaster.

On many networks, data are stored in two locations; individual computer workstation hard drives and central file servers. It is difficult for organizations to ensure that individual users backup their workstations consistently and properly, unless there is direct supervisor.

Central file servers manage network resources and provide a large data storage appliance where all users can store critical data. With a central depository, Organizations can back up data on a central server to ensure proper, regular and reliable access to data.

An organization can use many different methods to back up data. The primary Difference between the methods is the device and medium used to store the backup. Different media have different characteristics, such as capacity, speed and ease of use. The backup method chosen should be able to expand as the organization and its need for data grows. Government must balance the cost, capacity and performance of the various options.

Data storage strategies include:

- diskette (3.5 inch) are the most common storage media, and they are readily available and inexpensive. The storage capacity however is limited to 1.44 megabytes (MB) of data. Zip Disks, a type of diskette; most commonly come in 100MB and 250MB;
- CD-R and CD-RW (CD read only and read write) are easy fixes to back up large amounts of data and they allow easy restoration. CD-R and CD-RW disks can hold up to 640MB. CD “jukebox” (also known as libraries) filing systems are gaining popularity as a way to store and distribute data over a network;
- magnetic optical (MO) is a removable storage technology for files up to 2.6

gigabytes (GB), MO also uses jukeboxes, but stores about half as much data as CD-R, and disks are more expensive. MO, however, can read, write and erase more information faster;

- tape drives' strongest feature is capacity, ranging from a few hundred kilobytes to several gigabytes. Accessing data on tapes, however, is much slower than on disks. Technology advisors recommend using a reputable manufacturer to avoid early obsolescence.
- a redundant array of independent disks (RAID) offers the highest level of protection because it simultaneously makes identical copies on two different storage, checks for errors and allows a technician to replace a "bad drive" without shutting down the system. With costs typically starting at more than \$10,000, such a system may not be reasonable for constrained budgets;
- network attached storage (NAS) servers relocate data from servers to physically separate boxes and can be plugged into a network where needed;
- a storage area network is a separate dedicated network that avoids any traffic bottlenecks between clients and servers that can arise in using NAS systems;
- Internet storage involves outsourcing storage for a fee and allows a pre-programmed backup of the entire hard drive of a PC or server on a daily basis; and
- digital versatile discs (DVD) may help solve data storage problems. Although similar to a CD in appearance, DVDs can store almost 5GBs and the drives can read CDs. The price difference for the same system with a CD-ROM drive ranges from \$30 to \$200, though laptops have more expensive drives. Upgrade kits for older computers are available for \$100 to \$700.

Electronic data backup and recovery processes should be approved by an organization's IT administrative or governing body and documented in its IT strategic plan. Backup schedules and the type of backup process used in each department should be documented and disseminated to every department. The approved schedule should require every department to back up information at the same time.

Once backed up, the physical storage of the media should be addressed. Backup storage should not be in the same location as the original data source. Off-site storage protects an organization against physical disasters such as fires and hurricanes. A secure off-site facility is ideal, but as a minimum, backups should be secured in an Organization's vault. Regardless of the storage location, an organization should have documented storage processes. The organization should also exercise caution when restoring user files from untested backups and instruct all users to check for any unexpected changes to their restored files.

Data integrity requires file backups, as well as access and retrieval procedures.

Archival copies are important for security, disaster recovery and record retention requirements. But even the best procedures manual cannot prevent problems from arising. Clearly written procedures can reduce the legal ramifications when problems do arise. Additionally, without IT backup policies and procedures, the organization does not have a documented and approved strategy to address data integrity issues as they arise. As a result, the organization can only react to possible problems; it cannot prepare for them.

Findings

- **Each department in the county is responsible for establishing storage and backup processes.**

While departments in Claiborne County back up their data, there is no consistent Or documented countywide policy or process regarding data backup. Each county department is individually responsible for backing up its own data. The county does not have a local area network (LAN), and throughout the county, backup schedules and storage methods vary in sophistication and effectiveness.

For example, in the county administrative office, the water bill information is Backed up onto computer diskettes daily, and the entire hard drive is backed up monthly. The county secretary indicated, however, that she has not backed up the information on her hard drive since she has began work at her current position. In the Sheriff's department, backup processes were unclear. The municipal court backs their system about once a week, or when time is available, but no formal procedures are in place.

- **Problems have occurred trying to recover needed information.**

In early 2003, a system failure in the Municipal Court Records System causing data loss and corruption. The software vendor was able to retrieve most of the information, but the court lost some correspondence to defendants. The result was a loss of productivity and the incurred minimal retrieval costs. Without a recent backup of data, the office had to spend valuable time recovering the county's court information from the software vendor.

- **The County Courthouse has experienced water and rain damage.**

County hall is situated in an older building experienced in water and rain damage. A backup of the county tax billing system and information is stored in a fire safe, but the safe is located on the same floor as the computer. With electronic records and information backups stored on site, even disaster recovery data is at risk. The municipal court stores its backed up copy in the same server.

Recommendation

Ensure all critical county data are secure by establishing and implementing consistent countywide backup processes.

If individual departments continue to back up their own hard drives data, then a consistent countywide backup schedule, method and process should be developed, documented and enforced. Although backup processes may seem burdensome and an inefficient use of staff time, their necessity will become apparent when an unexpected disaster or malfunction deletes critical county data. Insufficient or inconsistent backups could result in a permanent loss of data.

The policies and procedures should be as comprehensive as possible and should be developed as a flexible tool to address a number of possible scenarios. They should state the employee responsible for the backup, the backup media, the schedule of when to back up data, short- and long-term storage strategies and purging instructions.

The county should look to the county secretary for help in developing policies and procedures for a consistent countywide data backup process. This should include selecting the method of backup, developing a backup schedule, locating a secure off-site backup storage facility and documenting the process. An audit process also should be devised to monitor compliance and ensure each department has a clear understanding of the process.

County departments should have the option to regulate their department's data backup responsibilities to the county secretary if both parties agree. This agreement should be documented and signed by both the individual department head and the county secretary.

If the county acquires a central server and LAN (as discussed in Issue 1.1), the designated IT coordinator (see Issue 1.5) should routinely back up the server. If the county does not migrate to a central server and LAN for all county departments, the designated IT coordinator employee should supervise the backup of each department's workstations, especially for the municipal court, police and water billing administrator.

Whether the county migrates to a central server, or the individual departments continue to back up their own hard drive data, a consistent countywide backup schedule, method process should be developed, documented and enforced. The policy and process should part of the IT policies and procedures manual.

Improve the County's Telephone System.

Background

Telecommunication refers to all types of data transmission, from voice to video. The original and most prevalent use of telecommunications technology is the standard telephone system, which serves as the primary means of communications for many modern organizations. Even with the advent of complex computing systems, most organizations would be unable to successfully conduct business without a functional and reliable telephone system.

During the last 20 years, the communications industry has been the biggest beneficiary of technological advances, allowing modern telecommunications system to provide highly reliable voice, data and digital services across the globe. These advances in telecommunications, often simply referred to as telecom, have dramatically affected the modern office environment. Features, such as, voice mail, automated telephone attendants, call transferring, call forwarding, three-way calling teleconferencing, paging, cellular phones and numerous mobile office services, are common place today, while just ten years ago, these were considered luxuries.

Telecom services are critical to support the mission of an organization, therefore, documented telecom policies and procedures are important to guide employees on how such services and equipment should be used. Portable equipment and wireless devices can expose organizations to potential security vulnerabilities, as these devices can be easily lost or stolen. Telecom policies and procedures should include instructions on the proper use and protection of equipment such as telephones, printers, fax machines and mobile technologies (satellite and cellular phones, pagers and mobile Internet devices).

Telecom policies also should address personal versus business uses of resources, such as the use of calling cards or collect calls, personal phone calls, use of 900 numbers, fee-based directory assistance and international calls. Policies and procedures that outline the specific privileges and restrictions of telecom tools helps organizations avoid incorrect use or abuse of their telecom systems. Finally, all policies and procedures should contain a contact person for general questions and general billing inquiries, effective dates, modification processes and to report policy violations.

When acquiring telecom systems and resources, decision makers should consider the benefits and costs of updating existing systems, as opposed to purchasing entirely new system. There are numerous examples of organizations that attempted to revamp existing telecom systems in lieu of purchasing entirely new systems, only to find that the older

technologies could not be successfully integrated. Therefore, the Ms Dotson has made an excellent decision on the selection of the Avaya phone system. It is important for organization to make these critical acquisitions that are upgradeable and expandable for the Organizations mission. This system affords the county to have Voice over Internet Phones. This type of equipment selections gives the County the capabilities to communicate on state and federal level with seamless effort during emergencies disaster. The existing telephone system does not cover the entire county offices. Given the reduction in telecom costs over the past four years, replacing the organization's outdated units is less expensive.

Findings

- **Portions of the county's current telephone system are not adequate for the county's needs and mission.**

The county has had the same telephone system (Avaya) in place since the early 2000s. Since that time, the size and scope of the county's mission has substantially changed.

The county uses five telephone lines; one for the Sheriff's department, one for the municipal court, one for the county fax machine and two for the administrative offices. The current system's primary shortcoming is that users cannot efficiently transfer call s from one department to the next, which many consider a business necessity. Other shortcomings of the current system include that the telephones in all of the county offices will not work if there is a power outage; not all telephones have intercom or hands-free capability; and the telephone system does not support conference calling throughout the county.

- **The county's current telephone system does not include a battery backup system in the event electricity is unavailable to the municipal building.**

The county's telephones will not function properly in the event of a power outage because there is no emergency (backup) power system for the telephones. Modern office telephone systems generally require power to function, which is why many of them have an emergency system which includes a battery backup.

- **There are no policies that specifically address the use of the county telephone system.**

The county does not have a set of policies and procedures that outline use of telecom equipment such as land lines, cellular and radio telephones. Nor does the county have a contingency disaster recovery plan covering the use of the county communications.

Recommendations

Improve the county's current telephone system.

A. Determine which telecom features/services the county needs to function more effectively.

The county should develop a list of the current system's shortcomings, such as inability to transfers call, no voice mail and no auto-attendant to help direct calls. Once shortcomings have been identified, the county should specify the ways in which county staff and officials would like the telephone system to work and which features they believe are necessary. By preparing a list of shortcomings and possible solutions, potential vendors will be aware of the county's needs and expectations. Or, establish a help desk for all incoming calls.

B. Secure bids from multiple vendors to expand the county's current telephone system.

The county should actively pursue bids to update the municipal building's telecom systems. Within the past four years, there has been a drastic reduction in the price of business-class telecom systems. This reduction presents an opportunity for organizations, such as the county, to secure high quality telecom equipment at a relatively inexpensive price. It is important the county entertain at least three bids for a telecom systems so the county, as the consumer, is provided with an accurate picture of the available products and potential costs.

The quotes should included upgrades that would provide up to six multifunction lines for additional capability in the event the county was to obtain additional lines, remote access and retrieval of voice mail for up to 100 employees and council members, an integrated automated attendant to direct calls, an emergency battery systems in the event power is unavailable to the facility and the ability to transfer calls internally or to off-premise locations. The new telephones would include number displays (caller ID), hands-free/intercom operations. The figures quoted included the complete installation of any hardware telecom patches/boards.

As always, it is recommended the county actively negotiate any vendor so the county receives the most cost-effective system for its investment.

C. Develop and distribute official, documented telecom policies and procedures.

The county should standardize and document telecom policies and procedures so employees understand the county's expectations concerning the use of telephones, cell phones and pagers. The telephone policy should address issues such as use of voice mail , toll call restrictions, proper use and protection of equipment such as telephones, printers, fax machines and mobile technologies (satellite and cellular phones, pagers and mobile Internet devices) and the related conduct while using any of these tools.

The county should assign the county-secretary or administrative assistant to oversee the development of telecommunications policies and procedures, and this employee should receive assistance from appropriate county personnel. Once completed and approved by the county council, the county, should ensure all personnel receive the documented policies and procedures, either in the county's comprehensive policies and procedures manual, a personnel handbook or simply in memo form. Personnel should be made aware of any possible disciplinary actions that could result from violations of these policies.

Improve the Management of the County's Electronic Records and Data.

Background

Collecting, sorting and storing data have become easier with the proliferation of powerful, low-cost computers. Once considered a luxury item used only by large corporations, today even the most modest organization can afford the basic information technology (IT) necessary for management electronic files.

Electronic documents or files either "born electric" or are converted from a hard-copy to an electronic format. Word processing, spreadsheets, correspondence (email), forms, Web site content, workflows and customer management files are just a few examples of the electronic documents and data created and maintained in today's organizations.

One way to manage electronic files is to store them in a database; or an electronic filing system where electronic files are placed in a specific format for quick and easy retrieval. By placing information in a database; a user can perform queries, which is a request for a single record or for specific information within a record. Users can search thousands, possibly millions of records of data to find a specific request. For this reason, databases have become invaluable to many organizations.

Many organizations would prefer to have all their records and documents in an electronic database; however, they may have to contend with years of legacy documents in storage. Legacy documents are historically printed (hard copy) documents (i.e., reports, receipts, ledgers, photographs). Depending on the time Requirements for legacy documents, an organization could fill an entire warehouse. Electronic documents or records storage requires considerably less space. For example, one compact disc can hold a four-drawer file cabinet of about 10,000 pages. In addition, many organizations often file legacy documents by a single category, such a name or date. This makes retrieving information from legacy documents an arduous task. Maintaining legacy documents on paper is not an ideal situation for any organization.

One solution is to use an electronic document or records management system (RMS). RMS can be categorized in two ways; the first refers to the use of records management software to catalogue printed records. Even if an organization's records are primarily paper documents, they can still benefit from the use of a records management software application. For example, a public library may contain thousands of paper documents, but a software-based system is the most efficient way to maintain an index of these documents or identify their physical location. In the case of public organizations, such as small counties, records management software applications are beneficial because they automatically alert records custodians when to purge or destroy legacy records.

The second type of RMS uses electronic records management software with a document imaging system, in which the documents/record are no longer maintained in printed form. The best known, decades old standard for legacy documents is the use of microfiche. Microfiche is storing photographed paper documents on small filmstrips. Microfiche is a relatively inexpensive way to store and manage entire warehouses of paper documents. Microfiche is a static medium, however, and does not allow searches or queries. For that reason, microfiche is not the recommended solution for an organization's RMS.

Within the last decade, the cost of digital records, management tools such as optical scanners and high-speed copiers has dropped significantly, making them affordable for even small organizations. One of the fastest growing forms of document storage and retrieval technology is digital imaging. Digital imaging refers to storing documents as an electronic file or record. The newest digital imaging systems use special software programs that recognize and index document content, which enables users to search the content of thousands of documents.

One of the most common digital record formats is a portable document format file (PDF). A PDF captures information from scanned copies of documents or directly from a desktop publishing application, making it possible to send formatted documents and have them appear electronically exactly as they appear on the original hard-copy document. PDFs can be static or automatically imbedded with digital search information, which provides both real imaging and

database functionality. The largest benefit to storing data in a PDF format is that it requires minimal space on computer hard drives. For example, a 100-page document that has been prepared using a standard word processing application may require as much as 1 megabyte (about 1000 kilobytes) of storage capacity. When this same document is scanned into PDE format, it requires less than one-tenth the space (about 100 kilobytes). Organizations may process a million separate documents or records during a year, and the ability to compress such a large amount of data may eliminated the need for additional storage hardware. Costs for industrial-grade PDF record systems less than \$10,000 PDF is just one of many searchable image formats in which information can be stored.

Another technology that has become commercially available within the past few years is the Web-enabled e-form (electronic form). Now that most modern organizations are connected through a local area network (LAN), standardized forms for nearly any purpose within organization can be made accessible to all employees connected to the LAN. E-forms are completed and submitted using a workstation, and are generally paperless. Once posted, e-forms can be used by employees to submit vacation requests, time cards, maintenance requests or anything that suits the needs of the organization. Using e-forms eliminates the need to create an electronic image of printed documents because the record or document will retain an electronic form, from its creation until it is purged.

It is incumbent on an organization to have a process for comparing the value of various types of information management tools and the cost of maintenance. The primary factor to consider within this process is whether the costs of maintaining information are reasonable and appropriate. Planners should research initiatives at the federal level and in other states and communities to see if any other entity has developed technology that may be adapted for local use. Moreover, in researching records, management applications, the organization should consider:

- connectivity needs (compatibility of different information systems)
- duplication of information (similar collected multiple times);
- validity of the information (information which is accurate and useful)
- timeliness of the information (ready access)
- accessibility (difficulty of access); and
- ownership (confidentiality/security and proprietary considerations).

An organization should learn about the types and availability of information to properly assess the type of management system it requires. This process requires the adoption of standards for the organization and categorization of government information and records. The organization should evaluate any management process by evaluating;

- time constraints and information turn-around;

- the appropriate level of detail;
- ease of use and understanding; and
- the reliability and completeness of the system.

Finally, an organization should include all ongoing projects, in the records/data management strategy. It is also should review and assess current problems and opportunities. An entity should be as precise as possible in quantifying the benefits and resources, both current and long term.

Findings

- * **The county maintains departmental record/files in a decentralized and hard-copy format.**

County departments store their own individual hard-copy records, which does not facilitate file sharing or database development. Moreover, each county department's storage space is limited.

For example, the county has a hard-copy file for each physical address in the County. The assistant county secretary maintains these records in county hall and files building permits by address. The county secretary maintains a Binder with a handwritten log of the files. The information stored in the files and binder is not electronically tracked, so information requests require a manual search. Therefore, any type of summary report requires pulling each file and checking for the needed information.

Official minutes of various councils, committees, boards and work group meetings are taped and documented. The documented minutes are entered into the computer, and the electronic versions are saved as word processing files. The official signed copies are stored in a binder in the county secretary's office. The electronic documents are saved by date. Each electronic document file allows word or term searches, but only within that document. Without access in an electronic format, searches or queries are not available and information must be manually researched.

Another example is the maintenance requests completed by the county public staff. The administrative office pages the county maintenance worker, who responds to calls as they come in. The county does not have a formal process for processing and documenting service calls. Therefore, the maintenance history on equipment, fixtures and improvements are not

recorded or useful for long-term planning. In addition, maintenance staff effort and effectiveness is not quantifiable. As the county grows, it will be easier to justify staff salary and performance evaluations when the work products are detailed.

- * **The county does not have a formal, documented policy for records storage, retention and destruction.**

Although each county does an adequate job of hard-copy records management, the county does not have countywide documented policies and procedures that outline when records should be transferred from the county's workstations to a storage facility, or when they should be purged from the storage facility.

- **The county has used outside assistance with its record management.**

Recommendations

Improve the management of the county's electronic records/data.

- A. Acquire a central file server that can be used by all county departments.**

The county should centralize its departments' electronic records/data files department level databases onto a single file server. The server may contain multiple databases, possibly one for each department or major functions within each department. Centralized electronic records and information are easier to maintain and protect and allow a uniform manner for implementing security measures, correct and consistent backup procedures and effective file sharing).

- B. Establish policies and procedures for the county's electronic records and data management.**

Policies and procedures should be developed that detail the management of the county's electronic records and data. A countywide, official effective date should be established on which employees should begin using electronic records and following the new records management procedures. Since some records and information are more critical than others, each department should classify its types of records and manage them according to its classification. Other topic that should be a part of records management policies and procedures include (at a minimum):

- responsibilities for data entry;
- specify report/records recipients (internal and external);
- access, security and privacy issues;
- record and data backups;

- long-term storage; and
 - retention and destruction of records
- C. Consider options for training and assigning responsibility for records management.**

The county should assign responsibility for records management to the county secretary or administrative assistant. Although the former county secretary will perform records management services for the county on a part-time basis, a current staff member should be responsible for ensuring records management requirements are completed as required by law and county policy.

The Mississippi State Library and Archives Commission has adopted administrative rules establishing standards (including classifications) and procedures for state records management. It also has analysts and resources, specific to electronic records storage, available for local governments.

Improve the Administrative Functions of the Public Works Department

Background

One of the best ways an organization can stay competitive is to routinely evaluate the methods and processes it uses to deliver goods and services to its customers. By identifying efficiencies, an organization can improve service, cut operating costs and ensure the organization's success. This model is true for both public and private sector organizations seeking to increase their effectiveness. Many organizations are looking to technology to increase efficiency. As the cost of hardware and software technology continues to decline, the trend to find efficiencies through technology increases.

Many organizations, public and private, have turned to work orders management systems, which are designed to help track an organization's routine service and maintenance requests. Smaller organizations, such as private service companies and smaller municipalities, which provide critical services such as water, telephone or electricity, are usually adept in restoring critical services when disruptions and outages occur. These same organizations, however, often fail to properly document and track routine service and maintenance issues that lead

to such outages. For this reason, work order management software offers substantial benefits for critical services providers.

An electronic work order management system is made up of both hardware and software components. Work order management hardware can refer to any electronic tool, computer workstation or hand-held device, that works in conjunction with the work order software. For purposes of this issue, hardware primarily refers to electronic hand-held devices, also referred to as personal digital assistants (PDAs). Among other benefits, a PDA allows maintenance staff to document service-related information while at a service location. This system removes the need to re-enter the same information when a staff member returns to the maintenance office. Most software companies that sell work order software programs also offer integrated PDA devices, and these devices enhance a work order system, but the cost may be prohibitive for smaller organizations.

Work order management software is designed to help track routine service and maintenance requests. The requests could include something as simple as changing inoperable light bulbs, or as complex as tearing up streets to repair an underground water line. Depending on the size of an organization, such requests could number into the hundreds per month. Work order systems are beneficial because they provide a uniform format in which work order requests can be processed. For example, many work order software applications provide reporting templates, which allow employees to prepare work order requests in a standardized format. Preparing work order requests using a template makes documenting such requests easier, and it also provides uniform record of requests. This system makes it easier for an organization's public works supervisor to schedule and prioritize daily work and improves record keeping. By tracking and documenting such requests, management can account for the time and activities of their respective staff, quickly search and query histories or work performed to help identify areas requiring additional attention and project future needs to allocate necessary resources. Work order software applications are offered by numerous companies, and they can range in price from about \$450 up to more than \$100,000 for custom-made applications.

Findings

- **The county's public works department does not have an automated work order system.**

The county does not have an automated process to receive, track or record work order requests. The department, comprised of one full-time employee, receives maintenance requests or general work order requests in person, by telephone or by alpha-numeric pager. Often, the county secretary will accept requests for service from citizens and then forward the requests to the employee, who then performs the requested tasks. The current process is functional; however, it makes it difficult to access historic information on the county's work order

requests. Proper documentation of requests can help management determine the frequency and type of requests received, schedule workload and provide an accounting of staff activities. Most important, better documentation can help create service performance baselines and related measurements, which can be used to determine how efficient the department's operations are. Proper documentation of requests also reduces the risk of liability by demonstrating that the county maintains concise maintenance records, and this is especially important in the event of discrepancies.

Recommendation

Improve the administrative functions of the public works department by purchasing (for developing) and implementing a work order management system to help process, track and record work order requests.

The county should purchase and use an electronic work order system. A work order system has many advantages. Not only can information be quickly retrieved, work orders tracked and requests categorized and prepared in a uniform format, but staff can generate periodic reports more easily and accurately assess actual work order costs.

A work order management system sufficient for the county's needs would cost as little as \$500. Many software companies offer software applications designed for smaller companies and municipalities. These applications are designed so employees can easily document, categorize and process requests. Like many customized applications, most of the information placed into the work Order record is menu driven, thus saving time and effort. The estimated cost would include installation of the software and a support agreement.

A similar option, which costs less than \$450, is to create a work order system using off-the-shelf software applications that are already licensed to the county. For example, the county currently has licensed copies of MS-Access, a common database application and MS-Excel, a common spreadsheet application. Both of these software applications are routinely sold with most Windows operating systems. Local software companies will customize (configure) these applications so the county can use them as their work order database, complete with menu driven options and report generation capabilities. Support agreements for this type of arrangement varies greatly from vendor to vendor.

These are two of the more cost-effective options the county should consider. The specific type of software selected is not as important securing a system that meets the county's needs and is properly supported. Before purchasing any software, the county should consult with several software vendors that provide public works software, as well a other Texas cities of similar size for advice.

Sheriff's Department

The Claiborne County Sheriff's Department consists of thirteen officers. The department maintains two stand-alone personal computer (PC) workstations. One workstation runs the Uniform Criminal Reporting System (UCRS) database software for incident reports, collision reports, etc. The department has a maintenance contract allows for phone support.

Some of the department's current IT capital requests include an upgrade of the radios placed in each patrol vehicle to an 800-megahertz trunking system and the installation of mobile data terminals and new video cameras in each of the department's patrol vehicles.

This review of the Claiborne County Sheriff Department's It infrastructure included an interview with the Sheriff.

Increase the Efficiency of the Sheriff Department's database software.

Background

One way to manage a large number of electronic files and reports is to store them in a database. A database is the best described as an electronic filing systems in which files are placed in a format that facilitates the quick and easy retrieval of specific records. Databases require specific software applications that allow users to perform functions within the database, such as viewing, adding and if authorized, altering or deleting a particular file or record.

Software applications and programs dedicated to managing databases are referred to as a database management systems (DBMS). There are many different types of DBMS, ranging from small systems that run on personal computers to massive systems that run on mainframe computers. DBMS and generally all software programs can be divided into two broad categories; DOS-driven and Windows-

driven. For purposes of this document, Dos-driven refers to older and more cumbersome programs that require users to type commands using only keyboard commands, and windows-driven refers to the more familiar programs of screen menus that are navigated by using a mouse and keyboard. Because of ease of use and generally flexibility, the windows-driven programs are considered superior.

A database can only be effective if the information is accessible to all users. One of the easiest ways to make information accessible is to centralize it in one location. Most organizations do this by placing their databases on a file server. File servers are computers used as a central storage point for an organization's data. Individuals with workstations that are connected (networked) to the server can assess the database information stored on the server. When two or more workstations can extract information from a file server, it is referred to as a local area network (LAN).

The degree to which an employee can use an organization's database is referred to simply as the access rights. There many different access levels, which each organization can establish as deemed necessary. Most organizations divide access levels into four distinct categories; read-only access, modify-access, delete-access and create-access. For example, an employee may be granted read-only access to database, which allows that employee to only view the information contained within the database but will not allow the employee to make changes. Some employees may be granted modify-access, which allows employees to make changes to files within the database. A common control measure for those employees with modify-access, delete-access and create-access rights is to track the user ID or user authentication of the person who is modifying, deleting or creating a file/record.

The task of protecting and maintaining the integrity of information contained within a database falls a database administrator (DBA), and the administrator should be the only individual with access to tracking information. A DBA, in conjunction with management, assigns employees levels of access. By regulating the types of data that can be viewed or modified, an organization decreases the likelihood that important data is compromised, lost, corrupted or deleted. This ability to establish access levels for different employees is referred to as administrator rights. A DBA grants different levels of access to different employees, generally based on the type of task the employee performs within the database. Within the computer industry, the terms administrator rights and administrative controls are synonymous. The information contained in an organization's database is usually valuable socontrol Measures are important characteristics of any database. Depending on the size of an organization, a DBA can be a single person with multiple other duties or a team of experts dedicated to maintaining one single database. For smaller entities, the DBA could be the IT coordinator.

Findings

- **The current configuration of the Uniform Criminal Reporting System (UCRS) database software.**

The sheriffs department uses the UCRS database software to generate incident Reports, call-for-service reports, collision reports and to track the issuance of traffic citations. When preparing reports that involve a vehicle collision, sheriff officers currently prepare two separate reports, an incident report and a vehicle collision report. The ICRS database software, as currently configured, does not have report templates that automatically post information from one report to another related report. For example, once an officer enters information into the UCRS incident report template, the officer must then re-enter much of the same information to complete a UCRS collision report. Because the database software, as is currently configured, will not export or auto-populate fields to other reports, the officer cannot shift information that has already been entered into another related report. This situation results in duplicative efforts and is an inefficient use of officers' time.

- **The sheriff department uses a windows-driven version of the UCRS data base software.**

The UCRS database software is window-driven, which makes it less compatible with the DOS-driven Municipal Court Reporting System (MCRS), database software. While this does not restrict officers from completing specific reports, it does impede the general flow of information between the two departments.

- **Transfer of data between the UCRS and MCRS is difficult because the sheriff department and the municipal court are not networked.**

Even if the UCRS and MCRS database software were more compatible, the County would have difficulty sharing data because the workstations do not share a common database. In any systems environment, it is far more difficult to share data when there are no established and easy paths, such as properly networked workstations. Although the county would be able to copy the data onto a disk and transfer (export) the data from one software program to the other, it would not be as efficient as if the data could be automatically exported to the other database. Currently, the information has to be hand written and placed in a shot gun envelope and hand carried to each department

- **Sheriffs records/data are stored on a workstation hard drive located in the County's sheriffs department.**

The county does not have a central file server, therefore, police records/data are contained on a workstation hard drive in the police department. Although sheriffs personnel are diligent about performing regular data backups, a workstation hard drive is more vulnerable than a file server because it does not have as many data integrity tools as a standard file server. Additionally, each workstation may be loaded with varying degrees of software security,

and this circumstance can be a vulnerability if an inadequately protected workstations contain a department's database. Finally, controlling physical access to a central file server is easier than controlling access to multiple workstations.

Recommendations

Increase the efficiency of the sheriff department's database software.

A. Discuss concerns about the UCRS database software with the UCRS software.

The county is encouraged to share its concerns about the UCRS software with the county's UCRS database software vendor. Before contacting the vendor, the sheriff department should write down a list of concerns it has about the UCRS database software. Daily users of the program should carefully note questions and concerns they have about the UCRS database software because they are the ones most familiar with it. Users will have an opportunity to learn practical solutions to problems they confront in their daily use of the UCRS database software. Such a list could include perceived functional shortcomings of the software with specific examples cited. For example, police officers noted that they are unable to leverage information that was entered into an incident report; they would prefer not to have to enter the same information on another report, such as a collision report. Vendor representatives said that the automated exporting of data from one report to another, such as the exporting of information from an incident report into a collision report, is within the capabilities of the software. Such discrepancies underscore the need for the UCRS vendor and the county to meet and resolve these issues.

Since the UCRS database software should be compatible with the Municipal Court Reporting System (MCRS) database software, the municipal court and sheriff's department should share concerns and determine what functions they desire before contacting the vendor. Preparing a detailed list of concerns before contacting the vendor increases the likelihood that issues and concerns can be adequately addressed. The software vendor will either be able to help the county reconfigure the database software applications over the telephone, or county staff may have to attend training at the vendor's offices, or a vendor representative could provide on-site training at county hall (see recommendation B).

Sheriff staff concerns about the functionality of the UCRS software; however, some of the issues may be related to proper end-user training. The current UCRS annual software maintenance agreement does not cover software refresher training. For this reason, the county is encouraged to carefully review training options with the vendor before contracting for another year of UCRS software maintenance. The renewal of the UCRS contract will provide an opportunity to negotiate for Free training as part of the renewal contract.

In the meantime, the sheriff department is encouraged to maximize the use of telephone support that is included as part of the annual software maintenance agreement. To the end, the sheriff department should address concerns it has about the limitations of the UCRS software with the vendor. For example, police staff said they were unable to export data from incident report templates into collision report templates. The fact that the data are not being automatically exported to the collision report template should be addressed with Software vendor telephone support representatives.

The county should not invest in additional UCRS refresher training if the county decides to purchase a new police records management software system from another vendor.

As with any business relationship, there are costs associated with terminating the relationship with a current vendor to obtain the services of another. Therefore, the county should make every effort to work with the current vendor.

B. Train county staff to maximize the benefit of the UCRS database software.

There are some functionality issues that likely could be resolved if county staff were afforded additional (refresher) training with the UCRS database software. The vendor offers additional UCRS database software training for \$400 per person four-hour session. Because this is a significant cost to the county's training budget, the county should make sure the training would specifically address its concerns.

C. Consider all vendors who provide sheriff reporting software.

Should the current UCRS vendor fail to provide the necessary assistance, the county should explore buying new police reporting database software. Numerous Companies offer windows-driven software applications dedicated to documenting and reporting police activities. As part of the process for reviewing other software vendors, the county should first review its relationship with the current vendor and assess issues such as actual software applications costs, service and support agreements and overall customer satisfaction. If county officials decide to actively

pursue other vendor options, they should consider factors such as the prospective vendor's general support policies, new software's ease of use, amount of training necessary for employees to use the newer software and the ability of the prospective vendor's software to perform required tasks.

Sheriff records software should be compatible with the county's municipal court records database software because much of the information contained in a county's Sheriff report and citation records database, such as citations or arrests will eventually be exported to the municipal court's records database. For this reason, software developers will create both sheriff records management software and municipal court records management software to work in conjunction with each other, especially since both software programs will probably draw information from a common municipal database. As a matter of functionality these two types of software applications are often purchased from the same software developer, at the same time. Although not imperative, it is advisable that the county purchase police reporting software and municipal court reporting software that is developed by the same organization. Moreover, purchasing two software applications at the same time may offer leverage to negotiate a better price for the city.

When considering other software vendors, the county should clearly understand that prospective vendors may need to recode the county's existing data. Recoding, also referred to as rewriting source code, is the process used by a prospective vendor to migrate the county's existing database records into format that can be used with the prospective vendor's software. Recoding is a critical issue when considering vendor options and unless negotiated otherwise, it may not be incorporated as part of the software price. For this reason, it is important that expectations of the county and the potential vendor are usually understood when discussing data support.

The purchase of software is a large capital outlay, and county is encouraged to actively negotiate prices for licensing, installation and support.

D. Transfer all sheriff records, data and reports in the UCRS database to the county proposed file server.

Unlike the current process, in which the police records, and data are maintained on a single workstation hard drive located in the police records, the proposed file server should be equipped with data mirroring fault tolerance systems and automated backup procedures. Maintaining this information on the proposed file server will be a more stable option and is preferable to maintaining UCRS database records on a workstation hard drive.

The sheriffs department may have concerns about the accessibility and vulnerability of UCRS database records if they are stored on the proposed file server. Sharing space on a file server, however, does not mean shared access or

reduced level of confidentiality. In fact, using a file server will increase the security and integrity of the police department's UCRS database records. Newer file servers are equipped with built-in data integrity systems and methods that can be used to monitor and restrict access to court records, such as passwords and user IDs. A server is generally fitted with software and hardware tools to protect it from external and internal threats such as hackers or computer viruses. This recommendation is predicated on the assumption that the county will purchase a file server and install a LAN, regardless of where county hall is located.

Increase Sheriff efficiency with mobile computing technologies.

Background

Since the first large scale introduction of radios in police vehicles in the late 1930's, law enforcement has come to rely on mobile technologies to help them perform their primary mission, protecting the public. Within the last 10 years, mobile data terminals (MDTs) have become a common feature in patrol vehicles, at least within larger urban areas.

MDTs are similar to standard laptop computers, but they are fitted with tools specifically used in law enforcement. MDTs use wireless FM (frequency modulator) radio/modern systems to access local law enforcement databases, which allows patrol officers in the field instant access to law enforcement information, such as vehicle registration, criminal warrants and all points bulletins. MDTs enable patrol officers input (type) requests directly into the law enforcement databases, thus bypassing the police radio dispatcher who manually checks information requests that are traditionally sent to the dispatch center via radio. This system increases safety because officers have quicker access to information on potential threats. MDTs also improve customer service because they substantially reduce the time citizens must wait before being approached by officers when being detained, such as during a traffic stop for a driving infraction.

In addition, most MDTs serve as word processors for preparing incident reports, collision reports and even the issuance of traffic citations. MDTs allow officers to prepare reports in the field, thus reducing the frequency that officers must return to a police station or precinct to prepare reports on traditional typewriters or a

computer workstation. This equipment means police spend more time in the community and less in the police station which increases police visibility, an important aspect of patrol duties.

The hardware and software that support MDTs are referred to as MDT system backbones. MDT systems are more than just computers mounted in patrol cars, and they require supplemental software programs and hardware devices to operate such as wireless modems and radio repeaters. MDT systems require regular technical support to operate, such as wireless modems and radio repeaters. MDT system require regular technical support to operate properly. For this reason, it is not uncommon for a complete, turnkey MDT system to cost as much as \$8,500 per vehicle. Traditionally, MDT systems have been too expensive for many smaller municipalities and rural counties. Within the past five years, however, MDT technology has steadily dropped in price while grant opportunities to purchase such equipment has increased.

Findings

- **County officers return to department to prepare incident and collision reports.**

County officers must return to the station to prepare reports, which reduces the amount of time they can patrol. In addition to being an inconvenience, sheriff visibility, one of the most important aspects of policing, is reduced.

- **During peak times, Claiborne County sheriff officers are forced to wait long periods before radio dispatch requests are fulfilled.**

Due to its small size, the county uses Claiborne County dispatch services, and during peak periods when the volume of "wants and warrants" requests are at their highests, Claiborne County Sheriff's radio dispatchers require additional time to respond to requests. All things being equal, the county sheriff officers operate under the assumption that Claiborne County dispatcher, on occasion, will prioritize radio calls which come from Claiborne County Sheriff's deputies ahead of calls coming from Port Gibson police officers and also have additional duties of E-911.

During times of excessive delays for radio dispatch responses, county patrol officers may choose to approach a vehicle before receiving a formal report about the vehicle's occupants or license plate. Claiborne County officers generally conduct patrol alone, so this combination of factors increases concerns for officer safety.

- **Excessive delays can negatively affect customer service.**

When a patrol officer detains a motorist for a possible infraction, it is recommended that the patrol officer wait for clearance or permission from a police radio dispatcher before proceeding toward the detained vehicle. When Clearance is delayed for excessive periods of time, vehicle operators, already subject to increased level of stress during traffic stops, can become easily agitated.

Recommendations

Increase sheriff efficiency with mobile computing technologies.

A. Actively gather information from vendors and other sheriff agencies about mobile computing technologies and their related costs.

MDTs are beneficial because they allow officers in the field instant access to law enforcement information, which saves valuable time, thus increasing officer safety and customer service. With the word processing capabilities of MDTs, officers can prepare documentation in the field while maintaining visibility.

Because MDTs provide such a large range of benefits, the county is encouraged To research mobile technology options, which should include entertaining bids from multiple vendors for MDTs and other related technologies, such as portable citation devices.

The county is encouraged to seek the advice of similar-sized sheriff departments in the area that have already completed the purchase process. The county is encouraged to contact these sheriff departments to leverage their experience and lessons learned fro undergoing the purchase, implementation and continued use of MDT systems.

In the past, \$8,500 per vehicle cost of MDT systems has been too expensive for many smaller municipalities and rural counties. Within the past five years, MDT technology has steadily dropped in price while grant opportunities to purchase such equipment has increased. The \$8,500 per-vehicle cost can be reduced substantially depending on the number of patrol/municipal vehicles that are outfitted with MDTs. Before accepting bids and negotiating with vendors, it is important the county have a rudimentary understanding of the services and hardware infrastructure it will need for a functional MDT system. This information will reduce the likelihood that the county will purchase equipment that may be unnecessary or not useful.

As with any large purchase, the county should entertain detailed bids from multiple vendors. The purchase of an MDT system is large capital outlay, and the county should closely scrutinize bids and vendors. To that end, the county

should negotiate with vendors to obtain the best price for products and services. As with all large capital purchases, the county should plan to ensure funds are available either in one year or over several years.

B. Explore ways to purchase mobile computing technology through government or private foundation grants.

The county should research methods and funding options that could reduce the cost of acquiring and maintaining mobile computing hardware, such as MDTs. Many federal grant programs have expanded their base of eligible recipients to include local law enforcement agencies. For example, the Domestic Preparedness Assessment Grant Program was recently enacted to assist small municipalities, like Claiborne County in obtaining mobile technologies.

In addition to the information contained within the Resources Boxes previously in this issue, the county may work with vendors who will help potential customers prepare grant information.

C. Reassign the E-911 operators and locate them within EOC facilities

The current location of E-911 places the county with a great liability. Current problems with the back up generator and hostile situations within the detention center level overwhelming distractions on the emergency operators as well as leaving them ineffective to the department and the entire community.

D. Acquire Mobile Command Post and Bomb Response Vehicle with full access to emergency response Apparatus to include biological and chemical, satellite, TV, phone, radio Data/voice communications, interoperability, video surveillance, marine radio(communicate with Coast Guard) and etc...

E. The electric generator at the Detention Center must to be certified by the maker or technical supporters as its ability to perform as stated or mandated by federal/state regulations.

F. Computer Evidence Processing and Potential Law enforcement liabilities

Computer evidence has become a 'fact of life' for all law enforcement agencies. Personal computers, the Internet and the use of word processing and spreadsheet programs, have changed the way the world does business. It is amazing that this has taken place over the span of just a few years. It is sad but true.....Those agencies that don't yet have the capability to deal with computer evidence issues, may not be fully capable of providing law enforcement services to their citizens. Now that documentary 'best evidence' has moved from sheets of paper to disk, it is important for all law enforcement agencies to evaluate their readiness and the ability to deal with computer evidence. Currently, it is all but impossible to investigate a fraud, embezzlement or child pornography case without dealing with

some sort of computer evidence. In the 'computer age' it is not uncommon to find evidence in a homicide or narcotics case buried deeply within a computer hard drive. It is extremely important that the Counties computer specialists get proper training from accredited training source. Increased exposure of law enforcement agencies to computer evidence also brings with it potential hazards tied to legal liabilities. By way of example, if your department happens to seize the computer books and records of an ongoing business, it is probable that such an occurrence will have a negative financial impact on the operation of the business involved. It gets worse if the records are accidentally destroyed 'on your watch'. If it can be shown that the business records or property was destroyed through through negligence on the part of the law enforcement agency involved, legal problems may turn a criminal investigation into 'the civil law suit of the century'. Training is the key.

- G. **New software for law enforcement administration, jail, booking etc.. current system has too many lapses of integrity. GIS software for reporting Megan's Law (sex offenders).**

Claiborne County Fire Department

Background

The Mississippi State Rating Bureau with the City of Port Gibson holding a class 8 rating currently rates Claiborne County class 10. The Claiborne County Fire Department is responsible for providing fire protection for the county and support for the Grand Gulf Nuclear Station in the event of a fire requiring off-site response. This summary discusses the state of current levels of protection, trends, and options for improving the fire protection in Claiborne County including Port Gibson. Included are increased capabilities in certain population centers, improving communications in emergency response situations, better preparing for hazardous material incidents, and attaining lower insurance rates for portions of the county and Port Gibson.

Findings

The Claiborne County Fire Department central station is located in the City of Port Gibson near the Court House. The department houses a rated, commercial chassis, 1,500 GPM pumper, a rated, commercial chassis, 1,250 GPM pumper, and will soon house a quick response vehicle with a 1,000 GPM pump and a dual dry chemical / foam system. This equipment is manned by three shifts of two personnel with no replacement if one of the shifts is sick or on vacation. This means that one or two pieces of fire apparatus is sometimes operated by only one shift person and the fire chief. The personnel are well tenured with two ready to retire. A veteran in the department who also is eligible for

retirement leads the department. There are a total of twelve employees. The off duty shift personnel work second jobs and are generally unavailable for back-up response. There are no building codes or National Fire Protection Association codes adopted by the governing bodies.

The Claiborne County Fire Department came into existence with 125 personnel and a new 1,250 GPM rated pumper, fully equipped, and a charter to provide fire protection to the Grand Gulf Nuclear Power Station, then under construction. Since that time, the tax funds from Grand Gulf have been divided between other counties by the legislature and the level of manning of the fire department has dropped dramatically. The fire department has more equipment than it has personnel to operate, even if off shift personnel respond. One 1,250 GPM pumper can easily require 4 firefighters on each of five 2 ½ hose flowing 250 GPM to manipulate the hose stream during firefighting activities. These firefighters are in addition to those needed to provide forcible entry, ventilation, search and rescue, water relaying, and such essential parallel firefighting activities. The recent re-rating of Port Gibson from a class 7 to a class 8 was attributed primarily to a lack of personnel responding to fires. The overall reduction in personnel (from 125 to 12) is detrimental to any organized fire protection program and may violate grant provisions if it can be shown that equipment was purchased where insufficient manpower and training are provided to adequately utilize the equipment in its intended emergency role.

The Port Gibson Fire Department has a part paid fire chief and a volunteer fire department whose members are paid a fee per response. The average response is about six members, of which several are city employees. The members mostly come from the city maintenance department. The city recently purchased a 1500 GPM rated, fully equipped, commercial chassis pumper. The fire truck is housed and maintained by the fire chief on private property. In the event of fire or other emergency requiring the fire truck, the fire chief responds in the truck, meeting members of the department at the scene of the event. The city has access to one other privately owned piece of firefighting equipment through a lease arrangement. The fire chief owns this piece of equipment.

Recommendations

A deputy sheriff who is not assigned to arson investigation as a primary duty investigates fires. The first personnel on the fire scene are the ones who notice unusual odors, color of flames, or flame patterns. These same personnel are the ones who may destroy evidence by the very nature of having to over-haul the fire scene after the fire to prevent further fire and water damage to the building or contents. Further, any evidence collected after the fire department has vacated the fire scene no longer meets the chain of evidence. Anyone can tamper with the fire scene once all fire and law enforcement officials have left.

The fire department personnel can be trained in arson detection and evidence gathering. Any suspicious fires could then have a preliminary investigation performed by the fire

department personnel along with any evidence gathered following the chain of evidence rules. The evidence along with any other arson findings could then be turned over to the sheriff's deputy for follow-up criminal investigation with the chain of evidence being intact.

Additional County Volunteer Departments

Volunteer Fire Departments have a long history of community service and proud tradition. The City of Port Gibson and the communities of Hermanville, Pattison and perhaps Alcorn and others have adequate core population to support volunteer fire departments. If the volunteer organization can be founded not on only protecting the community from the danger of fire, but on community pride, then a volunteer fire department can become a civic group that binds a community together, building trust and confidence between it's members.

The number of personnel needed to respond to fire or other emergency events in a volunteer organization is not standardized. In a rural area with one piece of apparatus, a first response of six personnel and a second response of a tank truck with a crew of two for tanker relaying of water may be adequate. This response level would be available day and night and includes male and female firefighters. Also, an alarm system is needed to alert the volunteer firefighters. Normally, this is accomplished using beepers, automated telephone alert, or both.

Traditionally, volunteer firefighters raised money and paid for all their own equipment, including fire trucks and training. With the federal and state funds available today, equipment should be readily available. The training for volunteer firefighters is the same as that for paid firefighters. The Mississippi Fire Academy provides training to nationally recognized standards at little or no cost. Training is also provided for volunteer groups at various locations around the state. Additional volunteer firefighters working together with the existing County Fire Department could be a cost effective and labor effective way to increase the number of personnel responding to fires within the county. As the longevity of these departments grow and the memberships sustain, then the rating bureau will look at the fire records for the number of personnel responding, training records for the volunteers and maintenance records the equipment and water supply and will give credit accordingly. Maintain any training, vehicle maintenance, and water supply records for review by the rating bureau.

In rural areas, *investigate* a water district, a legally defined district with definite legally defined boundaries under administration and authoritative political control of a municipality, county or the state or political subdivision thereof, as provided in (1) Section 21-25-21 and following or (2) Section 19-5-151 and following or (3) Section 19-5-215 and following of Mississippi statutes. *If a water district allows the use of a private water system to fill storage tanks then the rating bureau will allow credit for the storage tanks as an alternate water source.*

The Mississippi State Rating Bureau in its evaluation of fire protection facilities allows credit for alternate water sources. There are various water supplies that may be used to support a water

shuttle or relay process. One of these methods is via placing storage tanks throughout the area that can be used to fill tankers.

The Rating Bureau will recognize these tanks as a water source if the following conditions are met.

- A minimum storage capacity of at least 5,000 gallons. The rating bureau recommends at least 10,000 gallons.
- The tank must be capable of being filled from a water system by either automatic control or a manual valve that can be turned on while tank is in use.
- Proper precautions must be made to prevent valves and tank from freezing. This can best be accomplished on above ground tanks with an electrical element. It should be installed such to guarantee a water temperature of 32 degrees Fahrenheit with an outside temperature of 0 degrees.
- A visual device must be installed to indicate the water level in the tank.
- An audible device (siren, horn, etc.) must be installed to assure tank water level is adequate.

If a storage tank meets the above criteria, it may be considered as an alternate water supply point. A minimum, uninterrupted flow of 250 GPM for 60 minutes (15,000 gallons minimum) must be demonstrated for an alternative water supply to be acceptable. This requirement can be met using tanker truck relay. There are also accessibility, travel, and freezing requirements.

Water districts with approved water supplies and adequately staffed, trained volunteer fire departments can get reduced ratings from the rating bureau.

Hazardous Materials Response

Compressed hydrogen, carbon dioxide, oxygen, and nitrogen in varying size containers pass through Claiborne County routinely. Many of these gases are used at Grand Gulf in daily operations and maintenance functions. Identifying and knowing the characteristics of these and other hazardous materials passing through the county is crucial to effective and successful outcomes from emergency hazardous materials response events. Pre-planning and training for these events with other agencies is the key to minimize losses.

Most often, local fire departments are called upon in cases where hazardous materials response is needed. Law enforcement officials are usually first on the scene, particularly when the incident involves vehicle transportation. All who may be involved need specialized training in Initial Assessment of Hazardous Materials Incidents. The first several minute's activities can be the difference between a minor incident and a loss of life or worse. Often, it is the first responder, unknowingly rushing onto the scene to help, who becomes the first victim.

Law enforcement vehicles usually do not carry the volume of materials sometimes needed to successfully conclude hazardous materials incident so local fire departments with their hazmat vehicles and fire trucks are summoned. With money available from many sources, agencies, including Claiborne County Fire Department, received new equipment specifically for use with incidents involving hazardous materials. Much of

this equipment requires special training in its use because its misuse can result in injury or death. For instance, using the wrong type of protective clothing can allow gas to permeate through the clothing and absorb into the skin. Another example is certain types of facemasks are approved for use in oxygen deficient atmospheres and using one that is not can be fatal. When providing new and different equipment to your agencies, follow-up and be sure that the agencies have properly trained and have been certified in the use of the equipment. Maintain the training documentation for review by the rating bureau. Ensuring that all agencies receive and maintain training credentials for all personnel allowed to use equipment requiring special training helps insulate the local government from liability lawsuits resulting from lack of proper training and use of this specialized equipment.

Communications

Emergency events require clear, uninterrupted communications between units and a central station. This communication is essential to set up initial fire ground command and tactics when more than one unit is involved. Also, it is necessary to communicate to central station any information relevant on a larger scale (hazmat, propane tank, telephone trunk, etc.) so outside agencies can be notified as needed.

The communication cycle begins with reports to E911. The rating bureau may look at how E911 is staffed, training of personnel, distractions of personnel, maintenance of equipment, interruptions of service, logging of calls, dispatching of responses, adequacy of equipment, and identification of callers. They may how the emergency communication is transmitted to the fire department. Is there a dedicated system? How are alarms handled if electric power is lost or if the phone lines go down? If the answer is no or I don't know, then there is a serious flaw in the E911 communication with the Fire Department.

Given the number of miles of rural roads in Claiborne County, how is each building known to the E911 operator and how is that information make known to the fire truck driver? With the coordinate system used by many counties, navigation has become nearly impossible unless the driver knows the location of the property involved. More and more emergency response vehicles are resorting to GPS (global positioning satellite) system to assist them in finding more direct routing to the correct location. The maps can also assist in providing alternative routes, evacuation routes, and terrain information useful in HAZMAT events, water sources, and perhaps other valuable information otherwise unavailable to the firefighters. The GPS system could also provide location data about the fire department vehicle in case of an accident saving valuable time in getting medical attention to the occupants.

Grand Gulf

Grand Gulf provides specialized training annually for members of offsite groups who might respond to emergencies on site or support Grand Gulf's Emergency Plan. The Claiborne County Fire Department has made good efforts to attend this training but circumstances such as not enough personnel on duty, fire alarms, and other events has prevented the members from staying qualified. This limits their response capabilities to areas outside of the protected area (protected area - the area inside the fence where

security clearance is required). Also, a fire truck with one person would be of little assistance.

Flooding proved that Grand Gulf could be isolated from the Claiborne County Fire Department and other county services. All weather access to this facility and to the port facility would benefit both. The port could be designed with reservoirs to provide suction for fire pumps for automatic fire protection for building on the port site. This would be cheaper than building and maintaining an elevated tank. The reservoir could also provide suction for fire truck pumps to augment automatic fire suppression equipment.

Summary

The Claiborne County Fire Department has provided quality fire protection to the people of Claiborne County. However, over the past few years, the number of personnel has declined from 128 to 12. The department is at the point where they're too few personnel to operate the available equipment. The recommended minimum firefighters on a first response fire truck are four. This minimum number allows the crews to only operate one 1-½ inch hose line, have a truck operator/equipment person, and a fire ground leader/utility person. Today, the response vehicle is manned with two personnel when the shifts are fully staffed (no sick leave or vacation) and supplemented by the Fire Chief. This is considered very under-manned and can place the firefighters in a more dangerous environment.

The Mississippi State Rating Bureau indicated that the recent change in the City of Port Gibson's insurance classification from class 7 to class 8 was due in large to the reduction in personnel in the Claiborne County Fire Department. This affected the rating because it reduced the average number of personnel responding to fires within the city limits. Since the Claiborne County Fire Department responds to those fires, those personnel count along with the City of Port Gibson fire fighters.

Creating new volunteer fire departments within the county is one method of increasing trained manpower to support the existing core county fire department. These new departments could create new community identity, commitment, pride, and unity. These areas would enjoy quicker response time to fires and provide a greater knowledge of fire prevention and fire safety to their neighbors. If these volunteer departments can be established in legal water districts, then other advantages may also be available.

Claiborne County Fire Department has some hazardous materials response equipment on hand. Although the railroad no longer passes through Claiborne County, Highway 61 still has traffic carrying hazardous materials. Diesel fuel, gasoline, compressed hydrogen, compressed oxygen, chlorine, laboratory chemicals, swimming pool chemicals, hospital supplies, UPS, FedEx, and surprise locations offer everyday exposure to hazardous materials incidents. Given the range of hazardous materials and the limitations of much of the HAZMAT response gear, special training is required in the use of the equipment and response gear. For instance, some types of protective clothing look very similar but are very different in their intended use. Some protective clothing is safe to use in oxygen deficient atmosphere with an inert gas but not in an oxygen deficient

atmosphere with poison gas. All personnel who might respond to a hazardous materials event or otherwise use this equipment should be trained in its proper use. The training should be documented and maintained to protect the county from liability.

The fire department has limited communications between department vehicles and a base station. Communication between the fire station and E911 are more precarious. It seems that when the electricity is off, there is no way for the E911 dispatcher to communicate with the fire station. During weather emergencies, when electricity is likely to be lost, is when emergency calls might be highest. Direct communications should be a high priority. GPS devices in fire response vehicles could be lifesavers. They could eliminate trips to the wrong address, shorten routes, locate a fire truck in the event of an accident, and provide topological information at the incident scene.

Currently, Claiborne County is capable of providing little, if any, fire protection support to Grand Gulf Nuclear Station. Again, this is because of a lack of personnel to operate its equipment. The county has a good inventory of pumpers and supporting equipment. Properly staffed and trained, Claiborne County would have a formidable fire fighting capability, able to provide excellent support to Grand Gulf should the need arise.

In addition to the following:

- * Hazmat Response Vehicle is needed within this department
- * Communication equipment high and low band radios MDT's with GIS/GPS
- * Computer hardware and software to submit reports and document training
- * A new building to house additional equipment and make response times more efficient
- * Proper staffing of all shifts and equipment or the technology is useless

Emergency Operations Center and E-911

Background

At the time of this report, Emergency Operations Center (EOC) and E-911 are located in two separate locations. Both of these emergency services are located in facilities that do not support the theme of the Continuity of Government under emergency / disaster situations. The EOC building was built with good intentions at the time. However, it is questionable if it meets the today's standards for preparedness. The E-911 is located within a facility that could be engaged in hostile activities and is directly open to the public and has too many distractions for the operators to function in their proper role. The configuration of the hardware and the location of the server will leave the county and the city without a functioning E-911 center. The current power source has failed numerous times leaving the E-911 center offline to incoming and outgoing calls. This means that

the City/County can be taken to its own court with a civil suit as well as possible having to repay federal and state monies for not living up to federal mandates of operational readiness.

Findings

- A. The EOC must request a status overview of the current operations center. In lieu of the terrorists situation around the world, EOC needs to know if the current facility meets the current state and federal guide lines if the can survive an attack or if it needs modifications or to be replaced.
- B. Upgrade the EOC with state-of-art GIS/GPS computer technology
- C. Upgrade of the EOC and E-911 through new radio, call center management software and Computer aided dispatch system that log city and county responses and integrates the Avaya phone system, also capable of Automatic Vehicle Location
- D. Upgrade alert hardware for key personal and school district bus drivers
- E. Upgrade to the Avaya Phone system to include Voice over IP
- F. Acquire a transportable Radio Interconnect system for Voice over IP
- G. Upgrade from the civilian travel trailers to a Emergency Management Command Post on a commercial chassis and the ability to send real time streaming video within four hours of an event to state and federal authorities and sustain E-911 communications in the field
- H. Review inter-local agreement to cover gaps in fair funding of call center
- I. Deploy a Virtual Emergency Operations Center that use wireless networks and handheld devices to overcome inherent EOC participation problems from the site and protects communication and data with the redundancy, security and flexibility

Department of Information Technology and Public Safety

Agency Mission

The mission of the Department of Information Technology (DIT) is to provide citizens, the business community, and County workers with timely, convenient access to appropriate County information and services through the use of technology. DIT supports, manages, and coordinates all aspects of information technology to provide quality services to County customers and assists in the improvement of service delivery to County citizens through the deployment and use of technology in Departments. Services are provided through proven, best practices management techniques and application of County policies and procedures. The work of DIT is performed by County staff/consultants/contractors, in both direct execution and project management

roles. Staff is augmented by contractors to accomplish projects or for peak support activities. Funding for DIT activities is included in the General Fund, and charge back for department services, Technology Infrastructure Services, which includes data center operations, the enterprise data communications network, radio center services, and E-911 communications. DIT also manages and supports major projects including those with countywide strategic importance, such as infrastructure and application system modernization.

Trends/Issues

Implementing DIT, would enable the County to make tremendous strides in updating the County's overall IT assets, including development of an enterprise technology architecture; developing a County Government Website and Geographic Information System (GIS); developing standards; implementing an enterprise-wide office productivity system of e-mail, calendar, workflow, and office suite products; modernizing the County's network communications infrastructure providing improved connectivity and through-put to County agencies at various sites; delivering an integrated land development and records imaging system; implementing customer relationship management technology in key areas constituent and consumer complaints; making all systems Y2K compliant; migrating to more efficient and cost effective data center equipment; and tripling the number of County users connected to technology. DIT will distinguish itself as a leader in e-government practices as follows:

- Implement major enhancements in the e-government initiatives using public access technologies, the Internet, Kiosk, and Interactive Voice Response (IVR). This includes a design of a County website to facilitate day to day practices after normal business hours; software changes to accommodate the provisions of payment of various bills and services; an Internet customer service application where by taxpayers can report address changes or the move-out; the addition of 4 automated information Kiosks; and the implementation of a Web-based system which enable citizens to pay tax bills electronically and submit inquiries for permits, plan reviews, and inspections scheduling.
- Implement modifications to the County's payroll system to accommodate Payroll Direct Deposit and Pay for Performance based on new Personnel Policies and Procedures.
- Develop an IT architecture model for Claiborne County, including updating enterprise-wide IT standards, enhancing IT project request guidelines, and establishing a comprehensive software application inventory.
- Implement an enterprise wide GIS data repository online over the Internet with GUI for County staff and the Web for public use.

- Implement a Countywide software-training program.
- Complete the migration of private e-mail accounts of County employees to an official County Electronic Mail, and PC and LAN based office productivity systems to all county desktop computers.
- Install a positive identification system for Public Safety, which include a mug shot subsystem and links to regional, state and national public safety agencies.
- Install tracking system for Board of Supervisors' constituent correspondence.

Future Initiatives

Claiborne County continues to operate in a detached automated information-processing environment, which includes the IBM AS400 as well as client server and PC/Networked-based platforms. The major initiatives include upgrading the current IBM AS400 hardware and maximizing the use of this versatile environment, both by Citizens through public access technologies, and by County staff using improved Automated business processes. In addition, use of public access technologies and the Internet is expanding; therefore, information protection concerns need to address the Potential vulnerability associated with corporate and agency servers, local and area Networks, and Internet applications. To deal effectively with these issues, DIT Initiatives for the next several fiscal years will be as follows:

- Implement e-government design and Web enable prioritized business transactions via the Web, IV, and Kiosk public access platforms.
- Start the e-permitting initiative and design integrated voice, data, and wireless communication systems for all departments.
- Finalize the planning for thee constituent call center.
- Enhance overall IT infrastructure capacity in line with IT initiatives and technology usages.
- Enhance the County's information protection and security. A vigorous focus will be applied to the development and implementations of countywide computer security measures and identify required infrastructure changes essential to the use of Web and e-government business strategies. This includes additional security expertise for both the Local Area Network (LAN) and Wide Area Network (WAN), and proactive monitoring network activities to identify potential security lapses.
- Administer a level of LAN server and application support services to meet customer requests for server, application, and desktop support.
- Bridge the County government's "digital divide" between those who have access to the Internet and those who do not by providing various tools for County staff to access information.

- Upgrade countywide Microsoft Windows and Office products to enable departments to take advantage of available features and properties, and provide user support for those applications.
- Increase the use of enterprise-level technologies by County departments and agencies including GIS, the Internet, Workflow applications, Imaging, and Data Mining.

Trends/Challenges

DIT must be in position to be highly responsive to the evolving needs of County agencies, and the demands of a tech savvy population and business community who want fast and convenient service. In addition, the County has a diverse cultural community that needs the same level of interface into County information systems and automated services as the English proficient population. This translates into needing a level of language options available in public access technologies, which would contribute to the effectiveness and efficiency of agency programs that serve the public.

Now, more than ever before, technology is a target of legislation on the Federal and State levels. New legislation and mandates have requirements and standards for deployment of technology, particularly around privacy and security of data, client records, and information. The Health Information Protection and Accountability Act of 1996 (HIPAA) is one of those that place specific requirements on automated databases and transmission. Initially intended to target the health care and insurance industries, the legislation affect all entities that maintain such records. This is expected to have significant impact on the County in several agencies that maintain medical information including the Health Department, Claiborne County Hospital, Juvenile Court, Fire and Rescue, and the Sheriff's Office. The legislation is specific On information formats, security, and communications and electronic data exchange Standards that must be implemented if electronic means are used in these programs.

Other challenges that DIT will face are from legislation that impacts the technology Industry, which in turn impacts the market and products. There are trends in the way The market sells its products. There are trends in the way the market sells its products And services that will make budgeting for IT even more of a challenge. For example, The office products and database software markets (Microsoft and Oracle as example) Are moving to annual license payment structures, similar to the way the mainframe Software pricing was done in the past. Also, organizations have to account for the Number of systems, servers, PC's and/or simultaneous users in the IT environment, And license accordingly. Some jurisdictions have been surprised recently by audits Being conducted by the software giants, and some have been fined by the United States government for having unlicensed software installed on machines. One organization in Virginia had to pay \$600,000 in such fines.

DIT must be able to quickly provide infrastructure capacity to address other trends and County business opportunities. Geographical Information Systems (GIS) Repository Will need to be implemented to assist in the creation and identification of data that Shall validate information in the proposed \$25 million dollar transportation corridor For Highway 61 South for Claiborne County, Warren County and Natchez. The following are example of GIS databases based around driving/transportation Issues:

Reasons for GIS Repository Implementation

Drive Issue	Business Need	Description	Partners	Comments
Reporting Requirements	Road Inventory	County Road Authorities maintain roads with inventory information that is used to determine gas tax allocation	County and City, School District	
Reporting Requirements	GASB Reporting	Fixed Asset Inventory must be developed and maintained to comply with GASB 34.	County and City	
Reporting Requirements & Efficiency and Coordination	Flood Zoning, Work with FEMA and MEMA	Aligning these systems would prevent unnecessary duplication of data and effort.	County and City	
Reporting Requirements & Planning	Map Production	Organizations must produce cartographic products for decision makers, public education, and other routine purposes.	All	
Emergency Management	Access Restrictions	Emergency responders need accurate, current information on road closures, weight limits, and related matters.	County and City, E911, Bureau of Census	
Emergency Management	Emergency Coordination	Agencies need to share information concerning evacuation routes and determine alternate routes.	County and City, E911, School District	
Emergency Management	Transportation Infrastructure Vulnerability Assessment	Vulnerability assessments must be performed for transportation infrastructure statewide and assign a risk level.	County and City, E911	
Emergency Management	Street Address Assignments	County and other agencies must be able to assign unique addresses to new construction promptly and reliably. Conveying that information to other agencies.	County	
Public Safety & Land Management	Railroad Inventory	A variety of information about rail lines is needed to support an assortment of planning, management and safety needs, such as location, ownership, and road crossings.	County and City, E911, Bureau of Census	
E-Government	Street Names	Basic attribute information to be included with any centerline file.	County and City, E911	
E-Government	Project Tracking	Recent completed project data that can be queried on demand.	County and City, E911	
E-Government	Public Notification	Rules and regulations often call for public involvement prior to implementing a variety of activities. Automated methods can dramatically facilitate public participation	County and City	

		and education.		
E-Government	Service Rights Determination	Knowledge of address locations is necessary to determine service rights. Online applications can greatly facilitate this need.	State and Local Government	
Drive Issue	Business Need	Description	Partners	Comments
E-Government	Mapping using Address Matching	A fundamental use of the transportation network will be location determined by address.	Transit, County and City, E911, Census, Private Business	
Economic Development	Routing	Cooperatively sharing data regarding existing and proposed transportation infrastructure.	County and City, E911, Bureau of Census	
Transportation Safety	Collision Analysis	Agencies collect collision data to analyze problem transportation corridors.	County and City Governments, Transit Organizations	
Transportation Safety	Intermodel Analysis	Location and risk information must be available to assist decision makers in reducing intermodel safety issues such as when railroad tracks cross roads	Local Governments, Railroads, Transit Authorities	
Transportation Planning & Efficiency and Coordination	Infrastructure Planning	Organizations need to share plans for construction or modifying transportation infrastructure including sidewalks. This will identify opportunities for coordinated efforts. This data will be stored in the GIS database.	County and City, E911, Bureau of Census	
Transportation Planning	Detailed Collision Analysis	Analysis of roadway collisions is sometimes based upon the entire system surrounding an occurrence, including off and on ramps, roads, signals, and structures connecting to the roadway.	Public Works, Emergency Management	
Transportation Planning	Alternate Route Analysis	Decision makers need to evaluate and map alternate routes and communicate with the public.	County and City, E911, School District	
Transportation Planning	Traffic Flow Analysis	Planning units of agencies need to map and analyze traffic flows.	County and City, Community Transit	
Transportation Planning	20-Year Transportation Plan	Developing a 20-year plan involving statewide transportation planning data, as well as a variety of other data.	Highway District, City	
Transportation Planning	Tracking Activities along Transportation Network by	The specific need identified was stated as, "Knowing when and where utilities plan to work so we can combine paving efforts."	Public Works	

	Organizations without Jurisdictional Responsibility			
Transportation Planning	Right of Way Widths	Current and future right-of-way widths for transportation planning and property acquisition.	Highway District, City	
Drive Issue	Business Need	Description	Partners	Comments
Transportation Planning	Volumes Traffic	Current and projected volumes for transportation planning	State and Local Government, Private Business	
E-Government Planning & Efficiency and Coordination	Modeling Freight Flows	Information on truck trips, commodities, truck configurations, origins, destinations, and specific routes for all highways must be incorporated into a GIS database and made available to highway planners, modelers, and policy analyst	Freight Policy and Planning	
Efficiency and Coordination	Survey Data Sharing	Engineers scoping and designing an infrastructure project would greatly benefit from knowing what areas have been surveyed by other agencies to avoid resurveying the same area.	Highway District, City Governments Transit Organization	
Efficiency and Coordination	Roadway Improvement Sharing	Sharing road improvements among jurisdictions would facilitate coordination and help realize efficiencies.	Public Works	
Efficiency and Coordination	Accurate centerlines and right-of-way	It is very important that the feature location is accurate for purposes of metes and bounds legal descriptions.	State and Local Government	

Tele-work is one other example of one of these opportunities. Commercial sector studies show that this is a very attractive and highly effective option for the workplace. An appropriate IT plan for telecommuting will provide secured communications into County systems, an 'extra-net', provide a device (PC, laptop, PDA, or other), and support.

Digital 'signature/authentication' is a growing technical trend. The County should try to participate on a pilot program with the Mississippi Department of Safety and the Mississippi Highway Patrol (MHP). The programs will allow the MHP officers to scan newer driver license bar coded information on the back of license during traffic stops. This will allow the officer to print a thermal receipt/ticket for the violation and the court and fine type information will be automatically up dated on Justice Court system. This will elevate the possible error of information during the re-keying of inaccurate information, however the technology is young and evolving. It is the future for transmitting formal documents and transactions between business entities and jurisdictions. DIT should work on appropriate application of digital authentication with

several County agencies. Wireless communications is another technology that the County should acquire in its working inventory to increase productivity, especially for field type services/workers. Today, inspectors/investigators are using wireless devices to access systems and enter data on the spot.

DIT must be especially vigilant of the explosion of change in technology and establishing technology refresh cycles that are cost effective and smart, i.e. choosing the right approaches and products that will deliver good value, are supportable, and can be seamlessly enhanced over time. The technology industry is currently in a high state of rapid change - making decisions about what to implement and how to manage the vast variety has become more of an art, less a science. Selecting vendors has also become more of a challenge, especially as businesses buy out other businesses and change their product portfolio's accordingly.

DIT will be challenged in attracting and retaining skilled IT workers, particularly in this high region. Even through recent market instability has provided a larger pool of job applicants this is likely to be a short-lived trend. Skills needed in IT are changing also. In addition to technical skills, more analytical, business and managerial skills are needed too. We must look at employment standards and non-traditional strategies for compensation so that we can compete in the job market for the best-qualified applicants.

As more County services are made accessible through 24/7 e-government strategies, DIT will have to determine a resource structure to provide 24/7 system support and maintenance. A number of strategies should include a variety of out sourcing and equipment configuration options. As well, agencies that rely on these systems will need additional training capacity if they are to leverage all the benefits from the systems they use.

Administration and Planning Office

Background

For purposes of this report, the administrative office refers to the office housing the county secretary, administrative assistant,. This office has many Responsibilities and duties, such as general county administration, communications, general accounting and maintaining municipal records and minutes of various meetings, facilities and buildings and grounds Port Commission and Economic Development. Future Initiatives include Flood Plan and Zoning, utility (garbage) billing, County Planning, Permits, Ordinance and Zoning.

Findings

At the time of review, the office uses two Dell Dimension personal computer (PC) workstations, both running Windows XP operating systems and MS office 97. The administrative assistant runs the RVS utility software and the MIP accounting software. The office has two HP LaserJet printers and one Okidata dot matrix printer for water billing printouts. The county secretary has a CD Read/write drive on her workstation and McAfee, a free anti-virus software package.

Since the on site review, the administrative assistant received a cable Internet connection. The cable modem used has a Linxus 640 router and firewall combination appliance. The office should be commended for conducting daily backups of the MIP accounting software packages. The office also has two telephones lines and a line for a fax machine.

Recommendations

- * All remaining PC's should be upgraded to Pentium
- * Software and a workstation to perform GIS functions for Flood Planning
- * Replace fax machine with internal modem fax cards
- * Replace copier with digital network printer
- * Integrated and update enterprise software between Chancery Clerks and Purchasing Administrator
- * Acquire constituent tracking system
- * Acquire new billing software for garbage collection and devise a plan to collect over \$250,000 dollars in delinquent payments and the collection of security deposit prior to service and hire a third party to recover loss revenues
- * Collaborate with Port Commission on strengthen its position as an container Port by an investment program to upgrade its port authority infrastructure and embrace new technologies and systems to maintain a competitive edge.

Streamline workflow In Chancery, Circuit Clerk and Tax Assessor Offices

Background

The three elected offices above have the awesome task of maintaining, authenticating and collecting resources for the County. The Chancery Clerk has the task of recording and maintaining paper records for over hundreds of years of land transactions and other official records. The Circuit Clerk must record legal documents and instruments filed within the Counties to include liens and seal court order documents and maintain the court docket and jury selection and voter roles. The Tax Assessor/Collector has the responsibility of finding the just valuation of every parcel in Claiborne County and granting entitlement tax exemptions to qualified homeowners while all these offices provide the taxpayers of Claiborne County with the highest quality customer service.

Findings

The front office task requires the utmost attention of all the clerks and Deputies to ensure that the information that is entered into the records are accurate and complete. Although the paper-based system is logical and was appropriate when it was designed at that time, it imposes many burdens. The current software lacks the features and the ability to turn the paper resources into a data repository where by these three offices as well as all other county agencies can query accurate information. Duplicate records must be posted in the tract books, an often many different pages. The growing number of paper records poses an ongoing storage and security challenge. To say, we have not covered backroom operations where audit trails have been loss due to missing links in software and reporting features. **The previous Tax Assessor/Collectors office has had a *lapse of integrity (thief or misappropriation of funds)*.** Maintaining the physical integrity of the records and restricting access to authorized personnel are concerns because, although most of the records are public information, some are not. Currently, documents have over run storage space within the Courthouse. The Circuit Clerk has document overflow in the Attorneys room, meeting room and available storage. The Chancery Clerk has broached her current capacity and has documents in areas that are at risk to water or fire damage. Building a space to accommodate proper storage could absorb resources that could improve this antiquated system. To build out the Courthouse or some other facility at a mere 10,000 square feet at \$300.00 per foot would cost the County \$3,000,000 million dollars and this is not with the added cost of insurance and utilities. It is imperative that GIS and document imaging software and hardware are integrated within these offices. In light of this, current reporting measures, such as GASB34 intends to better reflect the way the current infrastructure is accounted for, thereby making financial reporting easier and more comprehensive for today's county government.

Recommendations

- * These offices acquire GIS and Document Imaging software/hardware to streamline workflow to reduce overtime and research time
- * Complete a GIS parcel-base map conversion and achieve Ortho-accuracy this year
- * Reduce the number of copiers and replace with self help desks
- * Remove all fax machines and replace with fax modem cards
- * Plan a back scan of all pertinent documents
- * Remove all redundant hardware from inventory and maintenance contracts
- * Develop separate web pages for all three offices
- * Purchase ergonomic furniture for staff and have customer space that is ADA customized

Improve the management of the county's electronic records and data.

Background

Collecting, sorting and storing data have become easier with the proliferation of powerful, low-cost computers. Once considered a luxury item used only by large corporations, today even the most modest organization can afford the basic information technology (IT) necessary for management electronic files.

Electronic documents or files either "born electric" or are converted from a hard-copy to an electronic format. Word processing, spreadsheets, correspondence (email), forms, Web site content, workflows and customer management files are just a few examples of the electronic documents and data created and maintained in today's organizations.

One way to manage electronic files is to store them in a database; or an electronic filing system where electronic files are placed in a specific format for quick and easy retrieval. By placing information in a database; a user can perform queries, which is a request for a single record or for specific information within a record. Users can search thousands, possibly millions of records of data to find a specific request. For this reason, databases have become invaluable to many organizations.

Many organizations would prefer to have all their records and documents in an electronic database; however, they may have to contend with years of legacy documents in storage. Legacy documents are historically printed (hard copy) documents (i.e., reports, receipts, ledgers, photographs). Depending on the time

Requirements for legacy documents, an organization could fill an entire warehouse. Electronic documents or records storage requires considerably less space. For example, one compact disc can hold a four-drawer file cabinet of about 10,000 pages. In addition, many organizations often file legacy documents by a single category, such as a name or date. This makes retrieving information from legacy documents an arduous task. Maintaining legacy documents on paper is not an ideal situation for any organization.

One solution is to use an electronic document or records management system (RMS). RMS can be categorized in two ways; the first refers to the use of records management software to catalogue printed records. Even if an organization's records are primarily paper documents, they can still benefit from the use of a records management software application. For example, a public library may contain thousands of paper documents, but a software-based system is the most efficient way to maintain an index of these documents or identify their physical location. In the case of public organizations, such as small counties, records management software applications are beneficial because they automatically alert records custodians when to purge or destroy legacy records.

The second type of RMS uses electronic records management software with a document imaging system, in which the documents/record are no longer maintained in printed form. The best-known, decades old standard for legacy documents is the use of microfiche. Microfiche is storing photographed paper documents on small filmstrips. Microfiche is a relatively inexpensive way to store and manage entire warehouses of paper documents. Microfiche is a static medium, however, and does not allow searches or queries. For that reason, microfiche is not the recommended solution for an organization's RMS.

Within the last decade, the cost of digital records, management tools such as optical scanners and high-speed copiers has dropped significantly, making them affordable for even small organizations. One of the fastest growing forms of document storage and retrieval technology is digital imaging. Digital imaging refers to storing documents as an electronic file or record. The newest digital imaging systems use special software programs that recognize and index document content, which enables users to search the content of thousands of documents.

One of the most common digital record formats is a portable document format file (PDF). A PDF captures information from scanned copies of documents or directly from a desktop publishing application, making it possible to send formatted documents and have them appear electronically exactly as they appear on the original hard-copy document. PDFs can be static or automatically imbedded with digital search information, which provides both real imaging and database functionality. The largest benefit to storing data in a PDF format is that it requires minimal space on computer hard drives. For example, a 100-page

document that has been prepared using a standard word processing application may require as much as 1 megabyte (about 1000 kilobytes) of storage capacity. When this same document is scanned into PDE format, it requires less than one-tenth the space (about 100 kilobytes). Organizations may process a million separate documents or records during a year, and the ability to compress such a large amount of data may eliminate the need for additional storage hardware. Costs for industrial-grade PDF record systems less than \$10,000 PDF is just one of many searchable image formats in which information can be stored.

Another technology that has become commercially available within the past few years is the Web-enabled e-form (electronic form). Now that most modern organizations are connected through a local area network (LAN), standardized forms for nearly any purpose within organization can be made accessible to all employees connected to the LAN. E-forms are completed and submitted using a workstation, and are generally paperless. Once posted, employees to submit vacation requests, time cards, maintenance requests or anything that suits the needs of the organization can use e-forms. Using e-forms eliminates the need to create an electronic image of printed documents because the record or document will retain an electronic form, from its creation until it is purged.

It is incumbent on an organization to have a process for comparing the value of various types of information management tools and the cost of maintenance. The primary factor to consider within this process is whether the costs of maintaining information are reasonable and appropriate. Planners should research initiatives at the federal level and in other states and communities to see if any other entity has developed technology that may be adapted for local use. Moreover, in researching records, management applications, the organization should consider:

- connectivity needs (compatibility of different information systems)
- duplication of information (similar collected multiple times);
- validity of the information (information which is accurate and useful)
- timeliness of the information (ready access)
- accessibility (difficulty of access); and
- ownership (confidentiality/security and proprietary considerations).

An organization should learn about the types and availability of information to properly assess the type of management system it requires. This process requires the adoption of standards for the organization and categorization of government information and records. The organization should evaluate any management process by evaluating;

- time constraints and information turn-around;
- the appropriate level of detail;
- ease of use and understanding; and

- the reliability and completeness of the system.

Finally, an organization should include all ongoing projects, in the records/data management strategy. It is also should review and assess current problems and opportunities. An entity should be as precise as possible in quantifying the benefits and resources, both current and long term.

Findings

- * **The county maintains departmental record/files in a decentralized and hard-copy format.**

County departments store their own individual hard-copy records, which does not facilitate file sharing or database development. Moreover, each county department's storage space is limited.

For example, the county has a hard-copy file for each physical address in the County. The assistant county secretary maintains these records in county hall and files building permits by address. The county secretary maintains a Binder with a handwritten log of the files. The information stored in the files and binder is not electronically tracked, so information requests require a manual search. Therefore, any type of summary report requires pulling each file and checking for the needed information.

Official minutes of various councils, committees, boards and work group meetings are taped and documented. The documented minutes are entered into the computer, and the electronic versions are saved as word processing files. The official signed copies are stored in a binder in the county secretary's office. The electronic documents are saved by date. Each electronic document file allows word or term searches, but only within that document. Without access in an electronic format, searches or queries are not available and information must be manually researched.

Another example is the maintenance requests completed by the county public staff. The administrative office pages the county maintenance worker, who responds to calls as they come in. The county does not have a formal process for processing and documenting service calls. Therefore, the maintenance history on equipment, fixtures and improvements are not recorded or useful for long-term planning. In addition, maintenance staff effort and effectiveness is not quantifiable. As the county grows, it will be easier to justify staff salary and performance evaluations when the work products are detailed.

- * **The county does not have a formal, documented policy for records storage, retention and destruction.**

Although each county does an adequate job of hard-copy records management, the county does not have countywide documented policies and procedures that outline when records should be transferred from the county's workstations to a storage facility, or when they should be purged from the storage facility.

- **The county has used outside assistance with its record management.**
In 1994, the county received a Certification and Acceptance Report indicating the county was effectively following a records retention schedule. Currently, the county records management is performed by the retired former county secretary on a part-time basis.

Recommendations

Improve the management of the county's electronic records/data.

A. Acquire a central file server that can be used by all county departments.

The county should centralize its departments' electronic records/data files department level databases onto a single file server .

The server may contain multiple databases, possibly one for each department or major functions within each department. Centralized electronic records and information are easier to maintain and protect and allow a uniform manner for implementing security measures, correct and consistent backup procedures and effective file sharing.

B. Establish policies and procedures for the county's electronic records and data management.

Policies and procedures should be developed that detail the management of the county's electronic records and data. A countywide, official effective date should be established on which employees should begin using electronic records and following the new records management procedures. Since some records and information are more critical than others, each department should classify its types of records and manage them according to its classification. Other topic that should be a part of records management policies and procedures include (at a minimum):

- responsibilities for data entry;
- specify report/records recipients (internal and external);
- access, security and privacy issues;
- record and data backups;
- long-term storage; and
- retention and destruction of records

C. Consider options for training and assigning responsibility for records

management.

The county should assign responsibility for records management to the county secretary or administrative assistant. Although the former county secretary will perform records management services for the county on a part-time basis, a current staff member should be responsible for ensuring records management requirements are completed as required by law and county policy.

The Mississippi State Library and Archives Commission has adopted administrative rules establishing standards (including classifications) and procedures for state records management. It also has analysts and resources, specific to electronic records storage, available for local governments

Parks and Recreation

Background

This department provides social, community and sporting conferences and events for the County residence.

Findings

- A. All of the computer equipment is obsolete**
- B. Replace all PC's**
- C. Surveillance equipment is need at remote sporting areas**
- D. The Department needs online registration for sports activity**
- E. Develop income and family events by sponsoring Inter-National Volks Marching (Walking, Bike riding) Events on historical places and events**

Road Management Department

Background

The sole basis of this department is to keep the traffic arteries open for the traveling public. But there is a greater purpose in that these staffers keep the high investment of dollars on track as their daily work schedules ensure that the infrastructure stays intact and preserves the investment into the County's physical plant and financial viability. The Department head wants to be proactive versus reactive.

Findings

The road department does not have the tools nor the software or hardware necessary to support GIS or the new requirements for GASB 34. He has an admin staff that spends 95% of the day unengaged of departmental duties. The billing for refuse pickup is completed once a month and not by district or cycle. At this moment, there is over \$250,000 dollars in uncollected fees.

Recommendations

- A. Replace obsolete PC's**
- B. Provide department with GIS Interface along with AVL and GPS**
- C. Obtain software and hardware that will allow him to forecast resource requirements**
- D. Forge a partnership between financial officer and road manager that allows for increased efficiencies and improved bond ratings due to proactive fiscal management thru Roads and Pavement management, Work order, service call, equipment and material management. Material purchased in bulk and only delivered on schedule due to proper planning and just in time delivery of material to prevent waste and misappropriations.**
- E. Use of PDA's in the field to record reports on Locations, Sign management, routes, Projects, Daily time sheets**

Improve the municipal court's database software.

Background

One way to manage electronic files is to store them in a database. A database is best described as an electronic filing system in which files are placed in a format, which facilitates the quick and easy retrieval of specific records. Databases require specific software programs that allow users to perform functions within the database, such as viewing, adding and, if authorized, altering or deleting a particular file or record. Software programs dedicated to managing databases are referred to as database management system (DBMS). There are many different types of DBMS, ranging from small systems that run on personal computers to massive systems that run on mainframes. A DBMS and generally all software programs can be divided into two broad categories; DOS_driven and Windows-driven.

Seasoned computer users may be familiar with the term DOS (disk operating system), which refers to the first type of commercially available computer operating system, and any software programs that use DOS are referred to as a Dos-driven program. When using a DOS-driven program, all commands are entered using only a keyboard at a command prompt (cursor). DOS provides only minimal screen features because it was designed when computers had substantially more performance limitations, and therefore the computer dictated how a user interfaced with it. Using DOS-driven programs for database management is especially difficult due to the number of complex keyboard commands required to manipulate the database.

Among other shortcomings, DOS is still 16 bit operating system, which is a technical reference to its limited ability to perform multiple functions. DOS does not support multiple users or multitasking, a necessity for today's office environment. For some time it has been widely acknowledged that DOS is insufficient for many modern computer programs. Many programs that were written for DOS are still in use, but the original software manufacturer may no longer support many of them. For this reason, most programs that were written in DOS have been discontinued.

A contemporary to the DOS environment is the graphic interface (GUI), more commonly referred to as a windows-driven environment. For purposes of this report, the term windows-driven is a de facto industry reference to a mouse-driven, spatially designed graphic-user interface, and is not intended to be associated with,

or an endorsement of the MS-Windows products. In a windows-environment, a user enjoys the computer's graphics capabilities to make software programs easier to use. In a windows-driven environment, an end-user can perform many commands by using a computer mouse to simply click on an icon or menu item. A well-designed GUI can free a user from having to learn complex typing commands and also provides a spatial or visual element to the screen development. The introduction of the windows-driven environment was the pivotal development that made desktop computing possible for the average office worker.

A database can only be effective if the information is accessible to all users. One of the easiest ways to make information accessible is to it in one location. Most organizations do this by placing their databases on file servers. File servers are computers used a central storage point for much of an organization's data. Individuals with workstations that are connected (networked) to the server can access the database information stored on the server. When two or more workstations are able to extract information from a file server, it is referred to as A local area network.

Findings

- **The county's DOS-driven municipal court records software provides limited functionality.**

The municipal court's DOS-driven database software, referred to as the Municipal Court Reporting System (MCRS), has limited functionality. Performing a general name search using the current MCRS database is difficult and rigid because it requires search criteria, such as a surname, to be typed as it is recorded in the MCRS database. This is contrary to the more intuitive windows-driven records programs, which are designed so that data that is entered inconsistently can still be retrieved. For example, a records search for the surname "Mendez" using widows-driven database software could yield close alternatives such as the surnames: Mendez or Mendez-Rincon. The ability of windows-driven database software to recognize and locate partial or similar information makes it more functional than its DOS-driven counterpart.

- **The municipal court manually enters the sheriff's department's UCRS data into its MCRS database.**

Records and data from traffic citations are manually entered into the MCRS database. The Uniform Criminal Records System (UCRS) database software used by the county's sheriff's department does not electronically transfer citation information into the MCRS database.

Although the sheriff's department uses database software developed by the same company, ticket information is not electronically passed between the

two systems. The UCRS database software could be windows-driven, which makes it more difficult for users to share information with the DOS driven MCRS software. However, problems encountered when bridging DOS-driven with windows-driven programs are just a few of many factors that can impede information flow. Other factors such as training and lack of connectivity are contributing factors. For example, the sheriff's department and municipal court are not networked, which makes it impossible to transfer any electronic files by disk.

- **The transfer of data between the UCRS and MCRS is difficult because the municipal court and the sheriff's department are not networked.**

In any systems environment it is far more difficult to share data without established and accessible parts, such as properly networked workstations. Even if the MCRS and UCRS database software were compatible, the county would have difficulty sharing data because the workstations do not share a common database on a central file server. The county staff can copy the data onto a disk and transfer (export) the data from one software program to the other; it would not be as efficient as if the data could be automatically exported to the other database.

- **Some Municipal court records are stored on a workstation hard-drive in the municipal court.**

The county does not have a central file server; therefore, municipal court records and data are contained on AS400 at the courthouse. Although municipal court personnel are diligent about performing regular data backups, a workstation hard drive is more vulnerable than a file server because it does not have as many data integrity tools as a standard file server. Moreover, each workstation may be loaded with varying degrees of security software. This situation can be a vulnerability if less adequately protected workstation contains the court's database. The network that contains court records was affected by virus attacks within the past two years, and although a large majority onto a better protected file server. Finally, controlling physical access to a central file server is easier than controlling access to multiple workstations.

Recommendations

Improve the municipal court's database software.

- A. Migrate to a windows-driven version of MCRS database software.**

The county's first options include upgrading its current DOS-driven software to a windows-driven program. Delta Computers the county's municipal court records software vendor, has indicated that a windows-driven version of the MCRS database

software has been in development for more than two years; however, the company did not provide a specific release date for the newer version of the MCRS database software.

The county should anticipate potential costs with the migration, such as training and licensing fees. Generally speaking, migrations from DOS-driven systems to windows-driven systems are worth the additional training and licensing fees.

This recommendation is contingent on many factors such as; whether the county's current vendor will develop and release a windows-driven version of the MCRS database software within a reasonable time; the cost of licenses for the newer MCRS database software, associated costs such as training, or the state of the relationship with the current vendor when the county decides to move forward. Considering these factors, the additional recommendations are offered as possible options.

If the county decides to purchase the windows-driven version of the MCRS database software, it is important the county negotiate with the vendor to obtain The best price for licensing, training and support. The funds necessary for implementing most of these recommendations may be available through the county's court technology fund.

In the meantime, the county is encouraged to share its concerns about the MCRS database software with Delta Computers, the county's MCRS vendor. Prior to contacting the vendor, the municipal court should make a detailed list of concerns about the MCRS database software. This list could include perceived functional shortcomings of the software, with specific examples cited. For example, the judge noted that the query tool within the MCRS database software was cumbersome and not intuitive.

The sheriff's department officials said they also have concerns about the general functionality of the UCRS database software. Since the MCRS database software is supposed to be compatible with the Uniform Criminal Reporting (UCRS) database software, the municipal court should make a detailed list of concerns about the MCRS database software. This list could include perceived functional shortcomings of the software, with specific examples cited. For example, the judge noted that the query tool within the MCRS database software was cumbersome and not intuitive.

The sheriff's department officials said they also have concerns about the general functionality of the UCRS database software. Since the MCRS database software is supposed to be compatible with the Uniform Criminal Reporting System (UCRS) database software, the municipal court and sheriff's department and the District Attorney should meet to share concerns and determine what functions they desire, before contacting the software vendor. Preparing a detailed list of concerns can be adequately addressed. The software vendor will either be able to help the county reconfigure the database software applications over the telephone, or the county staff may have to attend a training function at the vendor's offices or have a vendor representative provide on-site training.

Court staff had concerns about the functionality of the MCRS software; however, some of the issues may be related more to proper end-user training. The current MCRS annual software maintenance agreement does not cover refresher training. For this reason, the county is encouraged to carefully review training options with the vendor before contracting for another year of MCRS software maintenance. The renewal of the MCRS contract will provide an opportunity to negotiate for much needed training, without paying the full amount of about \$400 per four hour session, per person.

In the meantime, the court is encouraged to maximize the use of the telephone support that is included as part of the annual software maintenance agreement. To the end, the court should discuss its concerns about the limitations of the MCRS software with the vendor.

Finally, the county should not invest in additional MCRS software training if the county decides to purchase a new court reporting software system from another vendor, or purchases the windows-driven MCRS software package, if and when it comes commercially available.

As with any business relationship, there are costs associated with terminating the relationship with a current vendor to obtain the services of another.

B. Consider all software vendors who provide municipal court database software.

If the current software vendor is unable to satisfy the county's needs, the county should consider the vendors. Numerous companies offer windows-driven software that is dedicated to processing municipal court records and transactions. As part of the process of reviewing other software vendors, the county should first review its relationship with the current vendor and assess issues such as the costs of the software, service and support agreements and overall customer satisfaction. If the county decides to actively pursue other vendor options, the county must consider factors, such as the prospective vendor's general support policies, the new software's ease of use, training of personnel to use the newer software and the ability of the vendor's software to perform required tasks.

The cost of municipal court records software differs greatly depending on available options. The county, however, should participate spending around \$6,000 or more for a fully integrated municipal court database software program. In most cases, this price includes software licenses, software installation, training for users, technical manuals and telephone support as negotiated.

Municipal court records software should be compatible with the UCRS data-

base software, or whatever sheriff records management software the police department is using at the time. Much of the information contained in a county's municipal court records database, such as citations or arrests, is originally documented by the county officers as a officer report or general traffic citation. For this reason, software developers will create both law enforcement records management software to work in conjunction with each other especially since both software programs will probably draw information from a common municipal database. As a matter of functionality, these two types of database software programs are often purchased from the same software developer, at the same time.

Although not imperative, it is advisable that the county purchase municipal court reporting software and police reporting software from the same vendor. From a fiscal perspective, the purchase of the two database software programs at the same time may offer additional opportunity to negotiate a better price for the county. Finally, it is simply easier to deal with one vendor as opposed to two, in the event a problem may arise.

When considering other software vendors, county officials should clearly understand that prospective vendors may need to recode the county's existing data. Recoding, also referred to as rewriting source code, is the process used by a prospective vendor's software. Recoding is a critical issue when considering vendor options, and unless negotiated otherwise, it may not be incorporated as part of the software price. For the reason, it is important that expectations of the county and the potential vendor are mutually understood when discussing data recoding.

The purchase of software is a large capitol outlay and the county is encouraged to actively negotiate prices for licensing, installation and support.

C. Transfer all databases and software programs that contain the courts records and data to the county's proposed file server.

Unlike the current process in which the court records and data are maintained on a single workstation hard drive, the proposed file server will be equipped with data mirroring, fault tolerance systems and automated backup procedures. Maintaining this information on the proposed file server is a more stable option, and is preferable to maintaining the municipal courts records on a workstation hard drive.

The municipal court may have concerns about the accessibility and vulnerability of court records, if they are stored on the proposed file server. Sharing space on a file server, however, does not mean shared access or a reduced level of confidentiality. A file server will increase the security and integrity of the municipal court's records. Newer file servers are equipped with built-in data integrity

systems and methods that can be used to monitor and restrict access to court records, such as passwords and user IDs. In addition, a server is generally fitted with software and hardware tools to protect it from external and internal threats such as hackers or computer viruses. This recommendation is predicated on the the assumption that the county will purchase a file server and install a LAN, regardless of where county hall is located.

- D. Hire a collection agency to collect over \$750,000 dollars in uncollected fines**
- E. Booting or confiscating vehicles towed and impounded or collect state income tax returns suspend drivers license**

Internal Controls

A. What are internal controls?

Internal controls are the plan of organization and procedures in an office that help to :

- * safeguard assets;
- * ensure the reliability of bookkeeping and accounting data;
- * promote operational efficiency;
- * encourage adherence to prescribed policies and procedures; and
- * encourage adherence to prescribed laws and regulations.

Internal controls are what you do to ensure responsibilities are performed correctly the first time.

Regarding money, a sound system of internal control should:

- * minimize the possibilities for errors and misuse of funds;
- * provide a clear audit trail (show who did what and when); and
- * detect errors and irregularities on a timely basis.

Regarding people, a sound system of internal controls should:

- * help employees perform their jobs properly the first time; and
- * protect and support the innocence of those who do their job correctly.

B. The Principles of Internal Control

The four principles of internal control are:

1. appropriate division of duties;
2. qualified personnel;
3. sound procedures for authorizing, recording and reporting transactions;
and
4. actual performance.

1. Appropriate division of duties

If possible, three basic functions should be performed by three different people within an office and within an organization:

- a. authorization (approval) of transactions;
- b. recording of transactions; and
- c. custody of assets (cash and other property).

For example, a person making collections and issuing receipts (custody of assets) should not be the person to prepare and approve the bank deposit (approval), and neither of these persons should record the day's receipts in the cash receipts journal (recording).

If one person does perform two, or all three of these functions, there is no independent check for mistakes, and errors and irregularities may go undiscovered for a long time.

In many offices, it is often impractical to maintain a strict separation of duties because the size of the staff is small. When that is the case, add other compensating controls, such as:

- * rotating duties among personnel;
- * more strict supervision;
- * double-checking work;
- * enforced vacations;
- * additional training to improve the quality of personnel; and
- * more frequent internal audits.

The basic point to remember is that no single person should handle a transaction from beginning to end.

2. Qualified personnel

People performing the work should have the proper background, qualifications and skills to do the work before they are hired. They also should receive the appropriate training when they start to work and refresher training when necessary.

What can help to ensure these standards are met?

- *Adopt good hiring practices:
 - screen applicants
 - verify applications and resumes
 - verify references and skills
- *Provide regular training:
 - in-house training
 - regular staff meetings
 - outside classroom instruction

All personnel should understand how their duties fit in with the duties of others in the office, and with other offices in the government.

3. Sound procedures for authorizing, recording and reporting transactions.

All offices should have sound, clearly-written, documented procedures that assign responsibilities to specific people to ensure the job is performed properly the first time.

If personnel understand what is expected of them, they will tend to perform their jobs with fewer errors, and the chances of fraud will be less.

At a minimum, procedures should provide for:

- *proper division of tasks (which jobs are performed in which office or department);
- *segregation of duties for authorizing, recording and reporting transactions;
- *identification and operation of the accounting records such as;
 - general and specialized journals(revenues, cash receipts, cash disbursements);
 - general and subsidiary ledgers;
 - fund types; and
 - account groups.
- *appropriate flow of documents;
- *cross-referencing of documents;
- *periodic reconciliation of subsidiary records to control totals;
- *reasonable amount of checking and verification;
- *effective, timely transaction reporting;
- *safeguarding assets;
- *bonded employees who have access to cash and other valuables;
- *communication of procedures to those who need them; and
- *information on where to obtain answers not covered in the procedures and the exceptions to the procedures.

Basic internal controls for receipts:

- *use pre-numbered receipts for all intakes of money;
- *maintain strict control over all receipts, both issued and unissued;
- *issue triplicate receipts;

- *have a separate cash box/drawer/register for each person taking in money;
- *maintain strict control over the access to cash;
- *work mail independently of over-the-counter receipts;
- *place a restrictive endorsement on checks as soon as they've received;
- *use change funds for making change only;
- *provide a space for indicating mode of payment on receipt forms;
- *ensure receipts are signed or initialed by the person issuing; and
- *remit deposits daily.

Basic internal controls for disbursement:

- *disburse all funds with a check;
- *obtain a receipt for all remittances;
- *never pre-sign checks;
- *never make checks payable to "cash" or "bearer,"
- *require proper authorization of checks;
- *write "VOID" on checks when necessary and keep them with the checkbook;
- *safeguard a check-signing machine or stamp; and
- *cancel supporting documents upon payment.

These are the components of a good audit trail. They show who did what and when.

The county of Claiborne should be commended for its documentation of procedures for expenditures, disbursements and receipts for the Chancery Clerk, cash receipts, general fixed assets, payroll and other administrative functions.

4. Actual performance

A division of duties, qualified personnel and sound, documented procedures will not guarantee good internal controls. The system must be followed. Operations and results must be periodically monitored to see if the system is working as it should.

One way to ensure periodic monitoring is internal auditing, a close companion of internal controls. Here's why:

- * Without internal auditing, it's impossible to tell if the internal control system is operating as it should be. If it's not operating as it should be, it's not doing any good.
- * Without an internal control system, an internal audit may not be possible because there may not be anything to audit or the audit may not reveal who did what and when. There must be an audit trail.

The less frequently internal audits are performed, the higher the likelihood

that errors and irregularities will occur and go undetected for long periods of time. Internal auditing is the single most important way to improve the internal control system.

C. Reviewing your internal controls and draw your conclusions

Every department or office that handles public funds should address the following questions:

- * Are internal control principles in place?
- * Are they operating as planned?
- * Are sound, documented procedures in place?
- * Are the basic internal controls for receipts in place?
- * Are the basic internal controls for disbursements in place?
- * Is there an appropriate division of duties?
- * Are the personnel qualified?

Talk with your managers and staff. Do they understand what's going on? Or, do they tell you they will have to check on it and get back to you?

Observe the office as it works. Is there an efficient flow of work when things get busy, or are people just standing around? Does it look professional?

Design a flowchart of some of the procedures and transactions. Do they make sense? Are they efficient?

Re do some transactions according to the procedures in place. Are the transactions properly filled out, cross-referenced, correctly added, etc.? Did you come to the same conclusions? Would you change the procedures?

A review of internal controls should conclude with the decision that either:

- * internal controls are reliable; or
- * internal controls are unreliable.

If you can rely on internal control, then you can be confident that work is being performed correctly and any errors or irregularities will be brought to your attention in a timely manner. If you cannot rely on internal controls, then you need to take corrective action immediately.

F. The significance of mail

Each department/office should develop procedures to ensure all money received in

the mail is properly processed, deposited and accounted for, while at the same time establishing a clear-cut audit trail. Proper management of mail collections is particularly important because:

- * the person making the payment is not present; and
- * no receipt is issued at the time of collection.

In general:

- * mail should be picked up by the designated mail cashier or delivered to the cashier unopened;
- * mail should be opened by one person and all checks and currency removed before further distribution of mail; and
- if possible, the person opening the mail should not be the same person who handles other receipts of cash.

The mail cashier:

- open all mail addressed to the office or department;
- sorts out mail intended for others, retaining all that contain currency or checks and forwards other mail to appropriate offices;
- restrictively endorses all checks (i.e. "For Deposit Only, Account# _____");
- lists all currency and cash received on a Daily Mail Collection Report in sufficient detail to identify the person from whom the money was received, its purpose, including appropriate coding, and the amount received;
- after all mail has been received, totals all currency and checks and compares that amount to the total on the Daily Mail Report. Finds and corrects any errors. Initials or signs the corrected report; and
- forwards the mail collections and the collection report to the cash receipts cashier.

The cash receipts cashier:

- receives the mail collections and documentation from the mail cashier;
- verifies that the amount received equals the amount shown on the mail collection report.
If it does not equal the amount, investigate any discrepancies;
- if requested, prepares and mails receipt(s). Enter receipt number on collection report;
- prepares bank report or remittance to city/county treasurer or finance officer
- makes deposit or remittance; and
- forwards copy of collection report and deposit slip or remittance receipt to accounting department or finance officer for bookkeeping entries.

The accounting department or finance officer:

- verifies the amount shown on the collection reports equals the deposit slip or remittance receipt; and
- makes appropriate bookkeeping entries.

G. Some things to remember

No 100 percent guarantee:

No combined system of internal controls and internal auditing can guarantee that an operation is totally free of errors and irregularities. In fact, a system that attempts to do so would be cost prohibitive. A good system can, however, be a means minimizing errors and irregularities and provide for earlier detection than otherwise would have been the case.

Cost of internal control and internal auditing systems:

The costs of internal controls/internal auditing should not exceed the benefits you expect to derive from them. Internal control costs should bear some relationship to the amount at risk. For example, you wouldn't want to spend \$10,000 setting up a system to protect only \$500.

There's no substitute for an audit trail:

Without an audit trail, there's no way to check how the system is operating. You must know who did what and when. Obviously, pre-numbering documents and cross-referencing documents and entries is essential.

In a manual system, pinpointing responsibility can normally be accomplished by checking handwriting, initials and the like.

In an automated system, the who, what and when still is necessary. You should be able to trace all entries, changes and output to a specific individual (see Issue 3.1 for discussion on administrative and access rights of certain database software).

There are likely to be additional costs associated with going from business day system

In summary, management practices have to be nimble, decision processes fast, technologies deployed to be flexible and user-friendly, system kept 'healthy' and vital, and support levels must be adequate. All these must be optimized for the County to continue to be considered a best-practice organization and maximize the returns on investment (ROI) on Information Technology.

Claiborne County Hospital

Background

Claiborne County Hospital and the Claiborne County Chemical Dependency Unit form the nucleus of the facility. The portions of the hospital appears to be over forty-five years. The staff are well trained and are specialist in there assigned areas.

Findings

The computer systems are mostly Pentium III and IV and operating systems range from Windows 98 to XP. The billing and medical records software are in DOS format. The medical recorded system has a passive update feature. The medical notes are transcribed by a staffer and left for review by the provider. The system is backup off site by the software vendor. Local records are saved and backed up on magnetic tape. The Administrator is to be commended for having UPS attached to the primary power supply of PC workstation. But, the backup generator is only tested once a week by manually tripping the machine, our concern is that it may not start automatically due to some type of maintenance issue. There is not a log to state otherwise and we never take for granted that the key personal will be there when it fails to operate. This leaves the X series IBM server for potential data loss up to a total crash. However, tapes are stored in an unlocked drawer and some tapes manage to leave the facility via personal vehicle. There is not at this time a business continuity plan.

Recommendations

- A. The facility should find a seamless menu drive software to operate its facility. This software is obsolete and is static and flat on the monitor and will cause eye strain after prolong use.**
- B. The hospital should acquire software that allow them to interface with GIS component software.**
- C. The accessories should be install correctly and not left on top of the server cabinet**
- D. An investment in Voice Recognition software can speed the transcription of doctors notes within hours than days and save resources of overtime pay.**
- E. The IBM X series server will need to be replaced in two to three more years. If the hospital would consider residing and storing files on the County file server it could save the administering of a expensive maintenance contract on out of date equipment.**
- F. The hospital could have access to on hand technical support by sharing some of the cost with the county**

- G. The generator should be tested and certified by credentialed service provider.
- H. The hospital should have total communications (radio, cell phone, Voice over IP) with emergency services public and private.

Clabome County School District

Background

The school district has a rich history of achievement by the product it has produced in Leadership in the community and the number of college graduates in its past. Unlike all organizations, the school district has been faced with the evolution of our nations economy and the rapid pace of change due to great strides in science and technology that has infused all aspects of the American Life style.

Findings

Delta Communications has assessed the current technology plan and has determined that its direction and potential execution will lead the District to an antiquated platform to support our children's 21st century education. Also, current computer hardware/configurations, operating procedures and support measures are behind in delivering reasonable levels of support to the administration, faculty and staff. The present plan has been based solely on installing infrastructure (wiring, routers, switches) and computers in buildings and classrooms developed and built for Americas Industrial Age. Educators have a daunting task of preparing our youth for an unpredictable future. Yesterday's classrooms of straight rows of desks and performing repetitive task are obsolete models for teaching and learning. The Information Age requires the constant need for the increase of information and mental and tactile stimulation to improve and evolve the minds of our future leaders and workforce. The developer of the plan did not structure the document to allow for changes in technology and best practice or for contingences. At best, the plan has a shotgun blast effect across the school district that only places a bandage on current problems and needs. However, we realize that this plan does not meet your " **Vision** "of superior Administrative Services and Resource Accountability and Management, realization of technology integration in the classroom curriculum and modernization of educational facilities. The Plan should be revised to meet and exceed your "**Leadership Vision**" and surgically repair and mend areas that are not compliant of National and State mandates.

The current technology staffing structure will paralyze the information and communications capabilities of the district. The theory of knowledge is power has been allowed to run rampant within a one-person (with a god complex) department. The lack of documentation of work orders, logs of software/hardware configurations and equipment location could require tremendous number of man-hours to organize the

operation. The key person can mask inappropriate activities and or leave with sensitive data/documents and or equipment without prior knowledge of the administration or key management.

It is not the intent of Delta Communications to perform an audit or find fault. Instead, we are concerned for the success of our clients and those whom they serve.

The following is a list of concerns relating to accountability security of high dollar items:

- Improper processing of invoiced items after receipt
- Lack of proper tagging of School District property
- Lack of by room list of hardware/software and accessory equipment
- Improper installation of wiring and racking equipment (past and current)
- Pirated software (could lead to high cost fines)
- Lack of documentation of current in work progress and budgeted purchases
- Lack of work schedules for technology staff and assigned projects
- Trip hazards/electrical shock hazards throughout School District
- Lack of equipment replacement schedules
- Lack of uniform platforms software and hardware for computers and their usage
- Unacceptable down time for request for service
- There should be a two week detailed work schedule for the tech staff to the administration of what and where they will be and what is being done and the level of expense of the work requested
- Lapses in Integrity (misappropriation of supplies and equipment) in shipping and receiving and within district facilities

Recommendations

- A. Integrate GIS software to allow the school district to improve bus routes and save fuel resources**
- B. Develop school locations**
- C. Population forecast**
- D. Ensure vital information is gleaned for additional federal funding**
- E. Draft a plan to the Board of Trustees that outline your philosophy, vision statement and the guiding principles for technology use in the school district**
- F. Draft an implementation plan that uses common sense approach to using technology in the classroom**
 - **the curriculum is driving the technology program**
 - **students will have equal access to modern computers**
 - **students will have equal access, appropriate to their grade level**
 - **staff is trained to teach and use technology and**

- **management decisions will deliver technology resources equitably and efficiently to the learner**
- G. Design new school buildings with Ergonomics and the Environment for learning**
- H. Conserve resources by share computing space with county file server**
- I. Develop paperless offices and administration by tracking and Enterprise- wide software**
- J. Acquire professional staffing to support and implement technology plan**
- K. Develop Budget to support plan (see examples)**

U.S. Department of
Homeland Security
Washington, DC 20528



Homeland
Security

June 20, 2006

Mr. James Miller
Claiborne County
P.O. Box 474
Port Gibson, MS 39150

Dear Mr. Miller:

I want to extend a heartfelt thank you for your cooperation and assistance during the recently concluded Comprehensive Review (CR) of the Grand Gulf Nuclear Power Station. Your cooperation with team members from the Department of Homeland Security, Federal Emergency Management Agency, Federal Bureau of Investigation, and the Nuclear Regulatory Commission, as well as our partners in the private sector, is commendable.

Such willingness and active cooperation with the CR team is essential to the success of the CR process. Your effort will not go unrewarded, as not only will the results of this Comprehensive Review contribute to enhancing our nation's security and preparedness against terrorism, they will also play a pivotal role in helping the Department of Homeland Security effectively allocate Federal resources for years to come.

Again, thank you for a job well and for contributing to the defense of our nation.

Sincerely,

A handwritten signature in black ink that reads "Michael J. Garcia".

Michael J. Garcia
Federal Team Leader
Risk Management Division, DHS
703-235-5755
Mike.Garcia@dhs.gov