

May 2008 Customer Newsletter

Planning for future technology

In an effort to assist with the IT budget planning process, customers will receive information via email, beginning Monday, May 19th, regarding the amount of technology dollars spent with DIS since July 2007, as well as an annualized projection based on new rates.

As you know, technology is always evolving and we would like to use this opportunity to encourage you to think about IT focus areas to consider during the planning process which include:

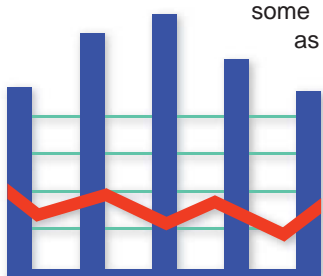
- **Disaster Recovery**
- **Records Management**

- **Encryption**
- **VOIP**
- **Mobile Workforce**
- **Enterprise Collaboration**
- **Business Intelligence**
- **Digital Signature Technologies**
- **Emergency / Mass Notification Systems**

Further information regarding emerging technology services and related budgetary rates is available at www.dis.arkansas.gov for your review. If you have any questions about IT budget planning, please contact your Customer Account Representative.

Rate adjustments

Effective March 1, 2008, DIS adjusted and posted new rates for several service areas. Most adjusted rates decreased from the amount previously charged for the services, providing cost savings to our customers. Rates decreased by an average of approximately 15%, with some rates decreasing as much as 83%,



although rates for the Data Warehouse – Data Mart service area increased.

State and federal laws and guidelines require DIS to operate as a cost recovery agency, billing customers for provided services. DIS monitors over and under recoveries for its services on a periodic basis during the fiscal year. An over or under recovery occurs when the amount of cost to provide a service does not match the amount of revenue received for the service.

To determine the impact of recent rate adjustments to your agency, please review the rate sheet at http://www.dis.arkansas.gov/list_rate.html. For further information or if you have any questions, please contact your Customer Account Representative or send an e-mail to dis.customer.service@arkansas.gov.

Expedited service orders

DIS offers the option of expediting service orders for Windstream Centrex phone lines when a customer has an immediate need. In order to keep the process simple and efficient, updated guidelines were recently implemented. If a service order is submitted with an installation date that is less than the standard five (5) business days, expedited order guidelines apply.

To submit an expedited service order for Windstream Centrex phones, customers should follow the current process and send an email to dis.service.orders@arkansas.gov with “expedite request” in the subject line, alerting the service order team of an outstanding expedited service order request. Expedited requests should involve no more than five (5) phone lines. If the request is received by 10:00 a.m. on any business day, Windstream will complete the order the next business day.

If the request is received after 10:00 a.m. on any business day, the vendor will complete the order on the 2nd business day after the order is submitted. If there is an “extreme emergency”, but a customer is not able submit the request for an expedited order by 10:00 a.m., Windstream will attempt to complete the order the next business day, but installation on that day cannot be guaranteed. DIS teams negotiate every expedited request with Windstream, so the requested installation date cannot be accommodated until an agreement is made with the vendor.

Expedited service orders potentially delay orders in the standard schedule, so please limit your expedited order requests if possible. A \$100.00 fee is assessed on any request for an expedited order, and the fee may apply whether the order is actually worked or not. Please note that custom designed services including ACD (Automatic Call Distribution), IVR (Integrated Voice Response), and Auto-Attendant are not eligible for expedited orders.

For any questions or concerns regarding expedited service orders, please contact your Customer Account Representative or leave your feedback in the Customer Feedback Mailbox on the DIS website at www.dis.arkansas.gov.

Customer Feedback

We want to hear from our customers! If you have any feedback, comments, or problems that you would like to share with us, please go to www.dis.arkansas.gov and click on the Customer Feedback Mailbox. Fill out the feedback form, and the message will be forwarded directly to our Customer Relationship Management Administrator. Feedback from you will allow us to continually improve the service we provide our customers.

DIS Call Center

The DIS Call Center operates 24 hours a day, seven days a week, 365 days a year. Call Center Agents are always available to help you with any problems you are experiencing with DIS provided services. Agents will log information about your trouble and forward a trouble ticket to the appropriate DIS staff.

To contact the Call Center, you may call 501.682.HELP (4357), 1-800-435-7989, or e-mail information to DIS. CallCenter@arkansas.gov.

What's going on at DIS?

DIS Teams were busy with some spring cleaning this past quarter, completing some major maintenance and upgrade projects. Over the last three months, DIS installed a new mainframe, worked with the Arkansas Building Authority (ABA) and Entergy to perform critical electrical maintenance to the MAC building and State Data Center, and installed a new 80 ton chiller for redundant cooling systems.

On Saturday, February 9th, DIS Teams migrated systems to a new mainframe. The transition was a success and customer feedback suggests that it was one of the smoothest migrations thus far. We appreciate all of the customers that worked with the staff to verify applications after the upgrade was complete.

On the weekend of March 16th, Arkansas Building Authority (ABA) teams shut down the power supply to the Multi-Agency Complex (MAC) to allow Entergy crews to perform critical maintenance on electrical systems that support the State Data Center and MAC. The

majority of the electrical work, including the portion that required a shutdown of the data center, was complete within the expected 12 hours. Entergy crews returned to complete the remainder of the critical work on Saturday, April 5th which did not require a shutdown of systems. With the completion of this critical electrical work, a major electrical outage to the building and a subsequent outage of the data center were potentially avoided. We appreciate your patience and consideration, as well as all of the customers and vendors that worked with DIS to make the event as seamless as possible.

Just prior to the scheduled electrical maintenance, one of the redundant cooling chillers supporting the State Data Center failed. DIS Teams worked with ABA to install and test a new 80 ton air cooled chiller on March 20th. The installation and testing was transparent to customers and there was no impact to the state network or hosted systems during the maintenance.

Meet your Customer Account Representative



Curtis Eubanks is a Customer Account Representative in the DIS Customer Relations Management (CRM) Division, where he has worked since the division's creation in 1999. He was the first DIS Customer Account Representative and has enjoyed being a part of the evolution of

the team. Curtis' customer base covers Boards and Commissions, Law Enforcement, the Department of Corrections and Highway and Transportation Department.

Curtis has 35 years experience in state government, working exclusively for DIS since its beginning as the Department of Computer Services (DCS). His career began in Operations

where he served as a shift supervisor. He later moved into the Telecommunications Division providing connectivity to state agencies. Curtis then transferred into Workgroup Systems where he conducted Internet and Exchange Email classes to employees and customers. All of these positions and related experience prepared him for his current challenging position.

Curtis served as a Vice President of the Association for Users of Telecommunications and Information Systems (AUTIS) and is certificated by the Supervisory Management Institute for Leadership. With his years of experience and soft skills, he plays an integral role within the CRM division.

Curtis has a passion for photography, which takes him hiking, climbing, bouldering, and exploring on weekends. Stop by his office and ask about his prints in the "DIS Gallery." He would love to talk to you about them! Curtis also serves as a mentor to Inner City children one night a week. His wife Cindy is a state employee at the Arkansas School for the Deaf. Curtis and Cindy have two daughters; a freshman in college and one in the fifth grade.

Tech Tips

Why does cyber-security extend beyond computers? The issue is not that cyber-security extends beyond computers; it is that computers extend beyond traditional laptops and desktops. Many electronic devices are computers, including cell phones, PDAs, video games, and car navigation systems. While computers provide increased features and functionality, they also introduce new risks. Attackers may be able to take advantage of these technological advancements to target devices previously considered "safe." For example, an attacker may be able to infect your cell phone with a virus, steal your phone or wireless service, or access the records on your PDA. Not only do these activities have implications for your personal information, but they could also have serious consequences if you store business information on the device.

What types of electronics are vulnerable? Any piece of electronic equipment that uses some kind of computerized component is vulnerable to software imperfections and vulnerabilities. The risks increase if the device is connected to the Internet or a network that an attacker may be able to access. Remember that a wireless connection also introduces these risks. The outside connection provides a way for an attacker to send information to or extract information from your device.

How can you protect yourself?

- **Physical security** - Having physical access to a device makes it easier for an attacker to extract or corrupt information. Do not leave your device unattended in public or easily accessible areas.
- **Keep software up to date** - If the vendor releases patches for the software operating your device, install them as soon as possible. These patches may be called firmware updates. Installing them will prevent attackers from being able to take advantage of known problems or vulnerabilities.
- **Use good passwords** - Choose devices that allow you to protect your information with passwords. Select passwords that will be difficult for thieves to guess, and use different passwords for different programs and devices. Do not choose options that allow your computer to remember your passwords.
- **Disable remote connectivity** - Some PDAs and phones are equipped with wireless technologies, such as Bluetooth, that can be used to connect to other devices or computers. Disable these features when they are not in use.
- **Encrypt files** - Although most devices do not offer you an option to encrypt files, you may have encryption software on your PDA. If you are storing personal or corporate information, see if you have the option to encrypt the files. By encrypting files, you ensure that unauthorized people can't view data even if they can physically access it. When you use encryption, remember your passwords and passphrases; if you forget or lose them, you may lose your data.