



FOR YOUR INFORMATION

April/June 2011

Mississippi's Research Network

By Jimmy Webster

Department of Information Technology Services

DESCRIPTION

For several years the research universities within the State of Mississippi have sought support for the build out of a research network within Mississippi, much like their peers in other states. The primary partners in this endeavor included the four research universities (University of Mississippi in Oxford, the University of Southern Mississippi in Hattiesburg, Mississippi State University in Starkville, and Jackson State University in Jackson) who would serve as the original tenants of this network. Other possible research tenants included the Stennis Space Center, the University of Mississippi Medical Center, the Memphis Coalition for Advanced Networking, and the Engineer Research and Development Center.

During the 2010 Regular Legislative Session support was garnered by Governor Haley Barbour to build out a research network. Language in Senate Bill 3184 provided the opportunity for the state's research entities to participate in a research network.

As a result of this legislative action and support from Governor Barbour, AT&T designed a research network based on the criteria established by the universities, the Governor's Office, and ITS. The primary purpose of this network is to provide the research entities with a high-performance, high

INSIDE THIS ISSUE

Mississippi's Research Network	1
State Data Center Move Completed	2
What is Computer Forensics?	3
Exchange 2010 Platform	5
Health Information Technology (HIT)	5
ITS Institute Offers Training in New Facility	6

capacity optical network with access to national research networks such as Internet II and National LambdaRail (NLR) as well as to encourage collaboration within Mississippi. The network design consisted of two diversely routed 10 Gig Ethernet connections (providing a total of 20 Gigs of capacity) into each research location all collapsing back to the Louisiana Optical Network Initiative (LONI) point-of-presence in Jackson where access to Internet II, NLR, and Commodity Internet are provided. A contract addendum was drafted to the existing statewide contract with AT&T for the requisite telecommunications products and services.

This research network will be called the Mississippi Optical Network (MissiON), and will provide the research infrastructure to allow the State of Mississippi to foster new educational opportunities and to keep Mississippi's research universities nationally competitive among peer institutions and agencies. The Mississippi research universities will serve as the primary nodes on this high-performance, high capacity, and resilient fiber optic network utilizing their advanced networking expertise and resources to make the most of this

Mississippi's Research Network

Continued from page one

opportunity. With the appropriate contractual amendments in place, it is anticipated that the MissiON network will be built and implemented during Fiscal Year 2012.

State Data Center Move Completed

By Mike Hatch

Department of Information Technology Services



RELOCATING THE STATE'S PRIMARY DATA CENTER

The State of Mississippi's Data Center has been providing centralized IT resources to state agencies in the downtown Jackson Capitol Complex area for almost 40 years. However, over the weekend of May 14, 2011, a much anticipated move took place. A great deal of effort went into planning and coordinating this project over the last 8 to 10 months, leading to the relocation of the state's primary data center. Given the complexity of the systems, the amount of data that had to be moved, and the challenge of physically moving, re-cabling and re-activating the many components that constitute the state data center, it is nothing short of remarkable that it would all be completed in approximately 36 hours. All production systems were shut down on Friday evening, and without exception, all production systems were restored and fully available to our customers the following Monday at 8:00 am. Many of the systems were

restored and available for access long before Monday morning.

A SECURE & HARDENED FACILITY

The new facility is a structurally hardened, physically secure data center, designed with significant redundancies in primary power, generator power, UPS power, cooling systems, and on-premise fuel and water storage. The new center provides approximately 12,000 feet of raised floor area for hosting the state's critical information systems. The new center is a core network node on the state's fiber optic network, which provides high-speed, redundant access from any state agency connected to the fiber network as well as access from the statewide MPLS network and the Internet. The new State Data Center will improve the efficiency, security, availability, and resiliency of the government systems that we host. The new facility will serve as the state's primary data center, a hub for statewide telecommunications, and a potential business recovery location for state agencies and other state entities.

PICTURES CAPTURE MOVE



A line of shrink wrapped equipment moves through the Robert E. Lee lobby in preparation for transfer to new Data Center.

State Data Center Moved Completed*Continued from page two**Equipment as it arrives on the floor of new Data Center.**Team members work to restore connections after the move.**Team members watch as the State of Mississippi ITS Data Center goes live in the new Eastwood Data Center.***What is Computer Forensics?***By Greg Nohra and Jay White**Department of Information Technology Services*

When I think of computer forensics, an image of David Caruso slowly taking off his sunglasses quickly pops into my mind. David Caruso plays the role of Horatio Caine, the leader of a team of forensic investigators/police officers who use both cutting-edge scientific methods and old-fashioned police work to solve crimes on the TV series *CSI: Miami*. In reality, the link between computer forensics and the general plot of the *CSI: Miami* TV series is not that implausible. In fact, there are many separate forensic disciplines ranging from forensic arts to forensic polymer engineering. Computer forensics is a branch of digital forensic science pertaining to the legal evidence found in computers and digital storage media. As computer technology becomes more prevalent in our society, the need for computer forensic knowledge and experience will be viewed more as a requirement than a luxury.

So, what is computer forensics? The goal of computer forensics is to examine computer evidence stored on a computer in a forensically sound manner with the aim of preserving, collecting, validating, identifying, analyzing, interpreting, documenting and presenting facts and opinions about the evidence/information. Computer forensics is instrumental during a computer incident, whether it is the identification of an intruder on an organization's network or gaining insight into events such as theft of intellectual property or criminal matters. The highest profile incidents usually involve criminal investigation or civil litigation, but computer

What is Computer Forensics?

Continued from page three

forensic techniques can be of value in a wide variety of situations, including attempts to retrieve data that has been inadvertently deleted, recover a forgotten password, or document a list of websites that have been visited. The science of computer forensics seems to be fairly straightforward; however, a computer forensics examination for an organization can be a complicated process that requires a number of skills and tools to obtain credible and reliable evidence that will clearly and factually answer the questions of “who, what, when, where and how” as it relates to a specific incident.

An organization’s ability to practice sound computer forensic technique will help ensure the overall integrity and survivability of their network infrastructure. Understanding the legal and technical aspects of computer forensics will help the organization capture vital information if their network is compromised and will help them legally if the intruder is caught. If an organization ignores the fundamentals of computer forensics they run the risk of destroying important evidence or having the forensic evidence ruled inadmissible in a court of law. Also, if an organization remains uneducated about the proper techniques of computer forensics, the organization could potentially be held liable in civil or criminal court for failing to protect certain types of data.

When an organization is preparing to conduct a computer forensics investigation, the organization must consider any already-known facts about the incident to determine the appropriate strategy. This potential evidence will fall into one of two basic categories of data that can be collected, persistent and volatile. Persistent data is data that is stored on a local hard drive or other medium

that is preserved when the computer is powered off. Volatile data is any data that is stored in memory, or exists in transit, that is lost when the computer is powered off. These two types of data require different types of tools to investigate incidents. An organizations ability to quickly and effectively obtain detailed information regarding an incident will have a direct impact on the success or failure of a computer forensic investigation.

Every organization should be aware of the most stringent aspect of any forensic investigation, the legal implications. Because the investigation may result in legal ramifications, the organization should work methodically and always strive to preserve the original evidence. In most cases it is suggested that any investigative work be performed on a duplicate of the original data, to prevent the original from being altered or destroyed. Working from a duplicate will also help the organization demonstrate that they have maintained the integrity of the evidence throughout the process. Maintaining (and proving) the integrity of the evidence from the initial point of collection is paramount to any computer forensics investigation.

An organization’s ability to gather and analyze evidence in a forensically sound manner and to comprehend the legal concepts of computer forensics will prove to be a benefit to the organization. Organizations that are not prepared to follow the proper protocols of a computer forensic investigation have a significant amount to lose. When CSI: Miami’s David Caruso is faced with a new investigation, he slowly and calmly removes his sunglasses with the confidence that he will be able to solve the crime. When facing a potential computer forensic investigation, does your organization have this same confidence?

Exchange 2010 Platform

By Steve Patterson

Department of Information Technology Services

The Department of ITS is pleased to announce the availability of the State Hosted Exchange Solution and NearPoint Archive for Exchange. The Exchange 2010 platform replaced Scalix, the previous hosted email solution, and has migrated all 37 of its currently hosted state agencies to Exchange as of June 30, 2011.

In addition to deployment of the State Hosted Exchange Solution, ITS recognized that organizations and state agencies of all sizes are increasingly faced with considering email archival systems for eDiscovery, litigation and investigation support, public information requests, storage optimization, as well as meeting regulatory and policy requirements. Since most agencies already have established document retention schedules that include email and other electronic documents, a critical part of the Hosted Exchange Solution is the inclusion of an optional archival system called NearPoint for Exchange. NearPoint is a complete compliance-based solution, archiving Exchange items – messages, attachments, calendar items, tasks, contacts, histories – not just email, into a browsable and searchable online mailbox archive. NearPoint for Exchange delivers archiving, eDiscovery, item recovery, disaster recovery, and storage management in a single integrated solution. It offers a self-service feature, which gives users and auditors access to email that has been protected, archived, and extended via Microsoft Outlook or Outlook Web Access.

Please contact the ITS Service Center at 601-432-8080 if you are interested in learning more about ITS's Hosted Exchange Solution or the NearPoint Archive for Exchange.

Health Information Technology (HIT)

By Kevin Gray

Department of Information Technology Services

Through the American Recovery and Reinvestment Act of 2009 (ARRA), Mississippi received funding for planning and implementation projects to advance secure exchange of health information through a statewide Health Information Exchange (HIE). At the request of Governor Haley Barbour and working in close collaboration with the Office of the Governor's Health Information Technology (HIT) Coordinator, ITS is the State Designated Entity responsible for the overall project management and monitoring of the statewide HIE's ongoing progress.

House Bill 941 was passed in the 2010 legislative session providing the initial structure and leadership rules for the statewide HIE called the Mississippi Health Information Network (MS-HIN). This legislation also created the MS-HIN Board which is responsible for the oversight of the MS-HIN. Board members include representatives from the Division of Medicaid, Department of Mental Health, Department of Health, State Medical Association, Delta Health Alliance, Information Quality Healthcare, Blue Cross Blue Shield, MS Primary Healthcare Association, a hospital representative, Department of Information Technology Services, and the University of Mississippi Medical Center. The Board has met on the third Wednesday of each month since October, 2010.

In addition, to the MS-HIN Board meetings, a small working group was convened to oversee contract re-negotiations with Medicity. Medicity is the vendor that was secured through a state procurement process to provide services for the

Health Information Technology (HIT)

Continued from page five

coastal HIE pilot project. It was decided during the strategic planning process that Medicity would become the statewide HIE platform. The contract negotiation work group met numerous times to discuss expanding the contract statewide, with emphasis on providers meeting the Meaningful Use requirements to be eligible to receive Medicaid incentive payments.

The state was able to finalize contract negotiations at the end of April, 2011 and secured a Health Information Service Provider (HISP) and the supporting infrastructure needed to expand the MS-HIN across the state. The HISP will allow providers, even those without electronic health records (EHRs), to enroll for a federal "DIRECT" address that will allow them to send and receive secure messaging from all other "DIRECT" providers not only within the state, but throughout the country. While this is not a venue of robust exchange, it is an important function that will allow providers the opportunity to meet at least on requirement of Medicaid Stage 1 Meaningful Use. The MS-HIN will also be able to accommodate a robust exchange of health information among providers with EHRs looking to fully leverage all the advantages from an HIE.

Currently the MS-HIN is determining prices for the HIE services and is in the final stage of development of the sustainability model. Medicity

and the MS-HIN are also working to finalize the work plan for the initial implementation phase to begin in July 2011. Once pricing and the work plan have been completed, working closely with the Department of Medicaid and the state's Regional Extension Center, an aggressive education and marketing campaign will be executed.

ITS Institute Offers Training in New Facility

By Susan McLain

Department of Information Technology Services

The ITS Institute, administered for the State of Mississippi by the Department of Information Technology Services, offers an educational program designed to enhance and improve the skills of information processing personnel within state government. The ITS Institute is now offering classes at their new location, 3771 Eastwood Drive, in Jackson, MS. The new facility provides state of the art, hands-on training labs. These labs are configured with a variety of PC applications and have communications capabilities with the mainframe at the State Data Center. As in the past, we continue to provide instruction in almost any information systems area needed by state government employees. We look forward to having you take advantage of training opportunities at the wonderful new facility.

FOR YOUR INFORMATION

Published by:

Mississippi Department of Information Technology Services

www.its.ms.gov

Contact: Caren Brister

601-432-8198

caren.brister@its.ms.gov
