BCCS Pulse Newsletter

A newsletter of the Bureau of Communication and Computer Services

Summer 2012

This issue

IBOP-EC Project Impact

- Federal funding of $62 million dollars
- Public and private funding of $34 million dollars
- 1000 miles of new fiber
- 1000 miles of upgraded fiber
- Fiber will be installed throughout a 55 county region in central and eastern Illinois
- Directly connect more than 400 community anchor institutions
- New fiber backbone will support speeds up to 1.6 terabits per second
- 169 direct jobs created or maintained
- 507 indirect jobs created or maintained
- Project completion date August 2013

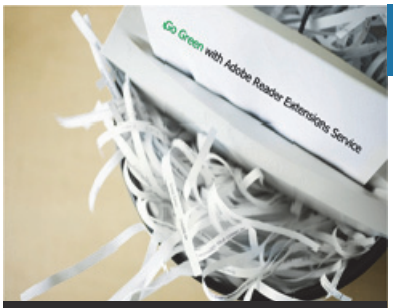
Beginning in August 2010 with $62 million in federal funding and $34 million from public and private partners, the Illinois Broadband Opportunity Partnership-East Central (IBOP-EC), when completed will bring 1000 miles of new fiber and 1000 miles of upgraded fiber to a fifty-five county region in central and eastern Illinois. In collaboration between the Department of Central Management Services (CMS), Illinois State University (ISU) and more than 40 public and private sector partners, the IBOP-EC will join together more than 400 community anchor institutions, directly connecting them via fiber to the upgraded Illinois Century Network (ICN) supporting high speed connection of up to 1.6 terabits per second.

As we travel the state "Lighting Up" Illinois, and talking to many Illinois citizens they tell us that they are anxiously awaiting broadband service and the business and educational opportunities that it will bring. Litchfield High School was the first to experience these benefits and the teachers, parents, students and administrators couldn't be more pleased with the results. The rest of the states fifty-five county region is not far behind with a completion date of August 31, 2013 for the entire project.

Brad Greenspan, Science Teacher for Niles North High School, couldn't have said it any better when he explained, "Technology allows us to bring students to the science world and bring the science world to the students…merging the kid world with what's happening in the outside world. It's that next level of that circle getting bigger and bigger."

Charlie Niehaus, Technology Director for Altamont Unit 10 Schools understands how important the ICN will be to realizing his goal of delivering better learning tools in the classroom as ICN fiber will deliver 50 times the bandwidth that they could have access to just a couple of years ago. Charlie sees the opportunities and is positioning his students to be competitive in the 21st century.

Mark Latham, City Manager for the City of Highland recognizes the importance of having a broadband infrastructure for sustaining future economic growth and the quality of life in his community. Lacking sufficient Internet service in the area, the city decided to build their own fiber optic network. The new infrastructure will offer speeds of up to 100Mbps and allow residents, municipal offices, and local businesses connection to high speed broadband along with access to two major Internet hubs, one in Chicago and the other in St. Louis. With the focus on economic development the city plans to attract new businesses and retain current ones. "We have had a lot of entrepreneurs and innovators and we want to keep that tradition going."



Go Green with ARES

- ARES is a shared service, hosted within BCCS enterprise data center.
- ARES allows users to create pages from templates, alter form fields, enable digital signatures, incorporate 2D barcodes, and allow file embedding.

State Agencies Realize Cost Savings

- Eliminates the hassle and expense of paper and printing supplies associated with processing pay stubs.
- Eliminates the costs associated with mailing paper stubs
- Reduces time and costs required to produce pay stubs and lost pay stubs.
- Streamlines workflow and increases productivity by payroll and administrative personnel who manage pay stub activities.

Adobe Reader Extensions Service (ARES)

The Bureau of Computer and Communication Services (BCCS) will continue to offer Adobe LiveCycle Reader Extensions (ALCRE) through the Adobe Reader Extensions Service (ARES). ARES is offered as a shared service, hosted within our enterprise data center, distributed via our state-wide network infrastructure, and supported by our technical resources.

ARES provides electronic form owners with the capability to apply usage rights within a Portable Document Format (PDF) allowing the user to activate functions within Adobe Reader to enhance end user interaction. This functionality includes the ability to create pages from templates, alter form fields, enable digital signatures, incorporate 2D barcodes, and allow file embedding.

ARES continues to be available to all state agencies, boards, commissions, universities, colleges, offices of the General Assembly, and Constitutional Officers, as well as, county and municipal governments within the State of Illinois. If you would like to add or continue using the ARES service, please click on the following link for more information: http://www2.illinois.gov/bccs/Pages/ARES.aspx

Note: To utilize all the features available with this service, you must create the source document with the latest Adobe Acrobat Professional development tools. Please see the Adobe website at www.adobe.com for more information.

For further information concerning this service offering please submit your questions and contact information via email to Bill Tumulty, ARES Service Administrator at Bill.Tumulty@illinois.gov or call: 217-524-0577.

Green Government Awards Electronic Pay Stub System (EPASS)

Green Government Awards are presented by the Illinois Green Government Coordinating Council (GGCC) in recognition of outstanding environmental leadership and innovative sustainability accomplishments by Illinois state agencies and public institutions.

This year the Awards ceremony was held in the Executive Mansion in Springfield, IL, where Governor Quinn presented eleven awards that honored agencies for their extraordinary green efforts on behalf of the State of Illinois. The ceremony also featured a panel on CMS Green Initiatives and launched the official unveiling of the 2011 GGCC Annual Sustainability Report. The GGCC was particularly proud of the FY 2011 Sustainability Report with a record number of agencies, boards, and public institutions reporting this year.

BCCS was recognized in the category of “Green Information Technology” for the Electronic Pay Stub System (EPASS) application, which delivers pay stubs electronically. BCCS implemented EPASS in order to eliminate the costs associated with mailing paper stubs to employees every two weeks. EPASS is a secure, easy to-use web-based tool that utilizes encryption and password management to ensure the protection of sensitive pay stub information, maintaining that information for seven years.

EPASS is currently being used by 30+ state agencies, which includes more than 34,000 employees, approximately two-thirds of our state employee workforce. BCCS will continue to roll out EPASS to other agencies. Agencies using EPASS have eliminated the hassle and expense of paper and printing supplies, reduced or eliminated the costs of postage and materials and the time required to reproduce lost pay stubs. They have also streamlined workflow, increased productivity by administrative personnel and reduced storage costs by eliminating paper copies.

To learn how EPASS can reduce your payroll processing costs while providing a valuable service to your employees, please contact Valerie Bolinger at 217-558-0629.

Illinois Department of Corrections
IT Consolidation

In our continuing effort to consolidate IT support for the State of Illinois, BCCS recently partnered with the Illinois Department of Corrections (IDOC) to bring their IT infrastructure beneath the protection and back-up of the State's Data Center.

In the transition BCCS welcomed twenty-two employees from IDOC who have quickly become valuable members of the team, providing years of technical expertise and business knowledge about their legacy agency. Since the consolidation last November, BCCS has been able to provide shared enterprise services and solutions, support and deployment power to many projects. Together, we have implemented the relocation of sixty-three servers to the state's data center, deployed approximately 3000 personal computers with the Microsoft Enterprise Agreement (MSEA) 2010 suite of products to 40 locations statewide, and migrated more than 6200 e-mail accounts to enterprise e-mail services. We also continue to upgrade and modernize IDOC's office technology.

To date, the following agencies, have been consolidated for efficiency and enterprise cost saving purposes:

Department of Agriculture, Department of Central Management Services, Department of Commerce and Economic Opportunity, Department of Corrections, Department of Employment Security, Department of Transportation, Department of Environmental Protection Agency, Department of Financial and Professional Regulation, Department of Insurance Department of Healthcare and Family Services, Department of Human Services Department of Natural Resources, Department of Public Health, Department of Revenue

About the Department of Corrections

The mission of the Department of Corrections is to protect the public from criminal offenders through a system of incarceration and supervision which securely segregates offenders from society, assures offenders of their constitutional rights and maintains programs to enhance the success of offenders' reentry into society.

E-Benefit Statements

Members of the State of Illinois Group Insurance Program may now view their group insurance benefits information online. The link below will direct members to the Public Authentication Portal screen. Users should click on the "Sign Up" button to create a public ID. Upon registration, you will be prompted to enter a valid email address for ID validation.

cmspublic.illinois.gov/eben

Follow the steps as outlined on the screens, paying special attention to the Public ID and Password requirements. Once you've created an ID, you will receive an email with a link to validate your new Public ID. When you click on the link to validate, you will see a new screen with a "Continue" button. Click on "Continue" to return to the Public Authentication Portal (Sign in screen). You should then enter the Public ID and password you just validated and click the "Sign In" button.

The next screen is a one-time registration that asks for your last name, social security number and birth date. By registering, you will be able to access your online benefit statement, while making sure your **information stays protected**.

Members who have trouble logging into the site should contact their agency group insurance representative (GIR).

Your online benefit statement will be updated the first Friday of each month. Members who do not feel their information is correct should contact their GIR immediately to resolve any potential issues. Agency GIR's will be able to access and print the statement for members.

Stop.Think.Connect.
Cyber Tips

Stop.

Stop hackers from accessing your accounts - set secure passwords.

Stop sharing too much information - keep your personal information private.

Stop and trust your instincts, if something doesn't feel right, stop what you are doing.

Stop and think about who can see the information you post online. Are you giving total strangers access to your personal information?

Stop any questionable online behavior. Only do and say things in the virtual world that you would do and say in the real one.

Think.

Think about the information you want to share before you share it.

Think how your online actions can affect your offline life.

Think before you act - don't automatically click on links.

Think about why you are sharing information online. Is it going to be safe?

Think about why you're going to the site. Did you get it from someone you trust?

Think about who you're talking to online. Do you *really* know who they are?

Connect.

Connect over secure networks.

Connect with people you know.

Connect with care and be on the lookout for potential threats.

Connect safely and show your friends and family how to behave online.

Connect with people and sites you trust when you're online.

Source: www.staysafeonline.org

Cyber Security Tips For Your Personal Computer
Social Networking

Cyber attacks on social networking sites continue to grow in popularity thanks to the volume of users and the amount of personal information that is posted...

State policy requires state computers and the internet to be used for business purposes only.

The popularity of social networking sites like Facebook, Twitter, LinkedIn and others has expanded tremendously in recent years. Nearly two-thirds of Americans use these sites regularly and because they are more ubiquitous for both personal and professional activities they are also the prime targets for malware distribution and scams. To protect you we are offering some information and tips on how to keep your system secure when utilizing these sites:

What are the security concerns of social networking sites?

Cyber attacks on social networking sites continue to grow in popularity thanks to the volume of users and the amount of personal information that is posted. The nature of social networking sites encourages users to post personal information giving the perception of anonymity and a false sense of security, which can cause users in many cases to provide more information about themselves and their lives online than they would tell to a stranger in person. The information you post online could be used by those with malicious intent to conduct social engineering scams and attempt to steal your identity for access to your financial data.

What can you do to be safe?

- **Keep your system updated:** Ensure that any computer you use to connect to a social networking site has proper security measures in place, including anti-virus, anti-spyware, and a firewall. Make sure you keep your operating system updated and patched. Set the configuration to "auto update" so patches can be applied automatically without intervention.
- **Use strong passwords:** Protect your social networking account with a strong password. Do not share this password with anyone or use it for other sites. In addition, some social networking sites support features for stronger authentication, such as using one-time passwords when logging in from public computers or using your phone as part of the login process. Enable these features where ever possible. It is critical that passwords used on social networking sites not be used on other sites.
- **Links:** Be cautious when clicking on links. If a link seems odd, suspicious, or too good to be true, do not click on it...even if the link is on your most trusted friend's page. Your friend's account may have been hijacked or infected and may now be spreading malware. For example, many individuals are tempted to click on a video they see on a friends page, but these videos may lead to a malicious website and when you access that site it has malicious code which can infect your machine.
- **Scams:** Criminals take advantage of the open nature of social networking sites to defraud individuals. Such scams sometimes use the pretext of an offer for a job or money. Be cautious when contacted on a social networking site with a request for money or with an offer that's surprisingly good.
- **Privacy:** Do not assume privacy on social networking sites. For both business and personal use, confidential information should not be shared. If a site's privacy policy is vague or does not properly protect your information, do not use the site.
- **Personal Information:** Do not respond to an email request asking for your personal information or asking you to "verify or confirm" your information, your user-id and/or your password.

Be cautious about installing applications: Some social networking sites provide the ability to add or install third party applications, such as games. Keep in mind there is little or no quality control or review of these applications and they may have full access to your account and the data you share. Malicious applications can use this access to interact with your friends on your behalf and to steal and misuse personal data. Only install applications that come from trusted, well-known sites. If you are no longer using the app, remove it. Also, please note that installing some applications may modify your security and privacy settings. Source: www.us-cert.gov