BCCS
Keeping You Connected

bccs.illinois.gov

Pulse Newsletter

A newsletter of the Bureau of Communication and Computer Services

Volume 2, Issue 2 September 2008

It's Good to be Green!

Go Green! Go Green is a global movement to sustain the world's environment. That sentence is quite powerful. Whether you are involved in a grand scale Green project or recycling paper at the office, years from now you will be able to say that you were part of practices that kept a clean environment for the future.

There are many, many ways to Go Green, from using fluorescent light bulbs to using "smart" power strips, from recycling your cell phones to safely recycling IT equipment; the list goes on and on. It is imperative we follow the Green IT movement and join other states by continuing towards a Green IT framework, IT strategies and IT statewide standards.

The State of Illinois has an Architecture Review Board (ARB) which is a multi-agency authority established to facilitate the Information Technology and Telecom Governance process within the executive branch of the State of Illinois. The ARB's responsibility is to ensure State agencies align technology initiatives with the State of Illinois IT and Telecom Strategy, identify and leverage shared technologies across the State's operations, and ensure conformance with established State Information Technology Architecture and Standards. Greg Wass, the State of Illinois Chief Information Officer (SOI-CIO) will factor in ARB recommendations when assessing IT and Telecom project requests and related procurements.

The ARB has created several subcommittees with various focus areas. Green IT is one of these areas. Danis Zinger, CIO of the Illinois Environmental Protection Agency (IEPA) was named as the Chairperson of the Green IT Subcommittee. In May 2008 she asked for volunteers to help with Green IT initiatives.

(continued on page 2)

Enterprise Program Management (EPM)

EPM
Enterprise Program Management Portal
Agency Dashboard
Agency Reports
Executive Dashboard
Management Reports
EPM Processes
EPM Applications
EPM Conceptualization: Planning and Forecasting
EPM Initiation: Portfolio Record
Portfolio Record: Status Reports
Agency View: Portfolio Record
EPM Initiation: (EAF) Executive Governance
EPM Initiation: IT Governance
EPM Home
Enterprise Program Management Portal
EPM Framework
Project Lifecycle
Planning and Forecasting
Executive
IT
BCCS
CMS

The Enterprise Program Management (EPM) Portal will provide Executive Branch agencies, boards, and commissions with unprecedented visibility into the internal processes of the Bureau of Communication and Computer Services (BCCS).

The EPM framework provides end-to-end lifecycle management for acquiring enterprise products and services, beginning with information technology and telecommunications. Visibility into the lifecycle of an initiative or project is intended to facilitate timely and effective processing through the requisite budget, portfolio, governance, qualification/activation, and project management processes.

A new release of the EPM Portal, scheduled to go into production on September 30, 2008, will provide Executive Branch agencies, boards, and commissions with an Internet accessible window into their respective initiatives and projects as they are processed and executed within BCCS. Consolidated and selected agencies will be able to better manage projects by identifying proposed initiatives, forecasting technology requirements and coordinating budget submittals. All Executive Branch agencies, boards, and commissions will be able to create portfolio records, submit project charters and associated documentation, collaborate in qualification and activation, and view project status reports.

The overall goal of EPM is to facilitate successful attainment of State of Illinois business and technology needs by enabling approved initiatives, programs, and projects while effectively allocating and utilizing the State's limited resources. The role of the EPM Portal is to promote effective partnering between BCCS and its client agencies through enhanced communication, coordination, and collaboration on technology-enabled business solutions. ●

IT Rationalization

The IT Rationalization/Consolidation Project has now moved into Phase 3; Remote and Regional Server Consolidation. An extensive amount of planning and discovery will take place during this phase. Data collection efforts both from Springfield and onsite at remote offices have been ongoing and once completed, an analysis of the data will determine which servers should be relocated to the Springfield or Chicago data centers.

These servers may also be considered as candidates for virtualization. Phase 3 will compliment the consolidation efforts in Phase 1 and Phase 2, where servers were brought into a central data center environment, secured and data backup processes monitored.

A quick overview of the entire project shows:

Phase 1: Servers were relocated from the 12 Consolidated Agencies to the BCCS Data Center, 201 W. Adams, Springfield, IL. This phase of the project was complete in December 2007.

Phase 2: Servers are being moved from various locations in the Chicago downtown “loop” area to 401 S. Clinton. This phase of the project is ongoing.

Phase 3: Data collection and analysis to determine which remote servers should be relocated to the Springfield or Chicago data centers. ●

Mark the Date!

On Thursday, October 30th, CMS/BCCS is offering a full day conference and workshops for state-wide agency **Telecommunications Coordinators** at the Capital City Training Center in Springfield.

The conference format has been designed to facilitate the exchange of ideas and information. The morning session will kick off at 9:00 a.m. and includes a panel of guest speakers that will bring you up to date on the latest State of Illinois Telecom initiatives. In the afternoon we are offering workshops providing a hands-on approach for filling out telecom forms and a forum for fielding your questions and issues with the EMS11and Centrex-Mate applications.

Seating is limited, so please complete your registration before October 15th. We look forward to seeing you on October 30th and we hope you enjoy the conference format.

If you have any questions regarding the conference, please contact Agency Relations Valerie Bolinger at 217-558-0629 or by email at: **cms.bccs.agencyrelations@illinois.gov**.

Virtualization Update

Virtualization is a proven software technology that is rapidly transforming the IT landscape and fundamentally changing the way that people compute.

Over the past months, you have heard and read that BCCS is in the process of virtualizing most of the CMS-managed Intel-based servers using blade servers and VMWare. The benefits related to this project include new hardware platform to replace aging equipment, higher uptime due to the built in high-availability/failover capabilities of VMWare environment which translates to a lower overall cost to our customers.

Approximately 300 servers were virtualized in Phase 1 with 200 additional servers relating to the refresh project and agency project initiatives were virtualized. Phase 2 virtualization planning is now underway and when this phase is complete an additional 400 servers will be virtualized. ●

It’s Good to be Green!

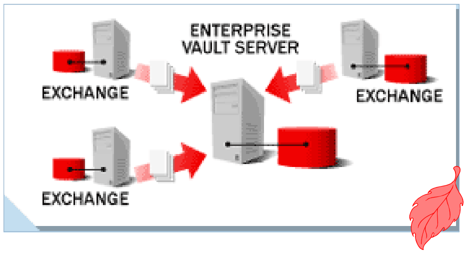
Continued from page 1

She found there were many who wanted to participate, and the Green IT Subcommittee was born. The Subcommittee is comprised of various agency representatives that began with its kick off meeting on June 2, 2008. The brainstorming session produced numerous ideas that were narrowed down to 5 Green IT action teams:

- Green IT Awareness
- Energy Efficiency
- Monitoring Metrics
- Provisioning/Asset Management
- Resource Efficiency

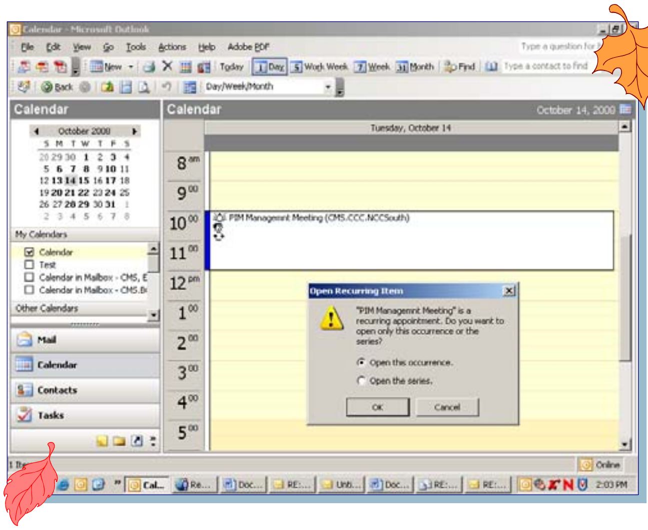
The goal is to shape and promote green IT practices and policies. Think enterprise wide as you watch your agency, board or commission’s hardware go through its lifecycle of acquisition, utilization and disposal. If you would like to participate and join the Green IT Subcommittee please contact Pat Sandidge at 217-785-6878 or send an e-mail message to **pat.sandidge@illinois.gov**. ●

Fall in Love with Email!



CMS is planning the implementation of the Symantec Enterprise Vault email management tool. The Enterprise Vault tool will enhance the capability and usability of Outlook/Exchange archived messages for customers of the enterprise exchange email system. Enterprise Vault provides a method to store archives centrally and allow users to search and access their archived e-mail.

The system also provides a secure web-based interface so that users can search and retrieve archive messages using Outlook Web Access (OWA) while they are out of the office. Message searches will be conducted over the entire archive mailbox without a user needing to know the folder to which a message has been saved. Currently in the Design phase, the pilot roll-out is scheduled for calendar year 2009. ●



Open Recurring Item

"PIM Managemnt Meeting" is a recurring appointment. Do you want to open only this occurrence or the series?

● Open this occurrence.

○ Open the series.

OK Cancel

Using Outlook Calendar 2003 Effectively

Have you ever encountered mysterious disappearances from your calendar or thought that you had accepted an invitation, but missed the meeting? If you have, you are not alone! This second edition of "hints from the PIM team" should help minimize your frustrating calendar occurrences!

- First and foremost, you should **always process meeting requests and updates from your Inbox**. If you or a rule that you have created moves a meeting request from your inbox before the request can be processed by the Outlook code or "sniffer", the meeting will not appear on your calendar and you will likely miss it. If a request ends up in a folder other than your inbox, you need to move it back to the inbox to process it.

- If you want to **cancel a recurring meeting** and are the organizer, you need to open the meeting on your calendar and set a new end date and then send an update. Past meetings will remain on your calendar, but going forward, the meetings will be cancelled.

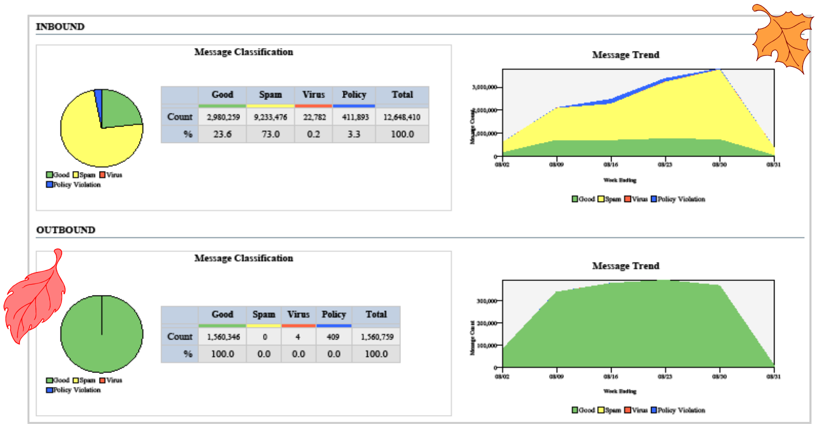
- If you need to **change a recurring meeting to a new organizer**, the original meeting organizer needs to send an update with a new end date. Again, past meetings remain on calendars, but future meetings are removed. The new organizer needs to send a new meeting request going forward.

- If you need to **create a meeting request from an appointment**, you merely need to open the appointment on your calendar and click "invite attendees" and select the people that you want to invite.

For more tips along the lines of effective calendar use, please refer to **http://office.microsoft.com/en-us/outlook/CH062556101033.aspx** and select *Appointments, Meetings and Events and click on "Outlook meeting requests: Essential do's and don'ts."* ●

August 2008 E-Mail Statistics

On average, we block 80% of the email messages sent to Illinois.gov as SPAM. BCCS has migrated 36 agencies, boards and commissions to the Illinois Enterprise Email network. We currently have 51 agencies, boards and commissions using the perimeter solution. ●



INBOUND

	Good	Spam	Virus	Policy	Total
Count	2,980,259	9,233,476	22,782	411,893	12,648,410
%	23.6	73.0	0.2	3.3	100.0

OUTBOUND

	Good	Spam	Virus	Policy	Total
Count	1,560,346	0	4	409	1,560,759
%	100.0	0.0	0.0	0.0	100.0

New Services at BCCS

Systems Security Assessments — based upon the needs and requested services; BCCS can conduct an assessment and provide recommendations focusing on: Network Vulnerability, Penetration Testing, Application Vulnerability and Industry Best Practices. To find out more about the service and how to place a request for a security assessment, please visit the BCCS Services Catalog at link: **http://bccs.illinois.gov/BCCScatalog/services/SystemSecurityAssessments.htm**.

Enabling Services - Cryptography Services
What is included with this service?

- BCCS offers two types of certificates ("organizational" certificates are not available): Personal (e.g. individuals) & Device (e.g. servers) certificates
- An independently certified, highly secured environment ensuring transactions and data are protected.
- Expertise and background gained with implementation of digital signage serving 48 State and local governmental entities.
- Digital identity assignments for individuals or systems.
- Software necessary to enable encryption/digital signature functionality.
- Help desk support.
- To find out more about the service and how to place a service request, please visit the BCCS Services Catalog at link: **http://bccs.illinois.gov/BCCScatalog/services/Cryptography.htm#included**. ●

SOI Directory Update

The State Telephone Directory is available online to provide business listings for state agencies, boards, and commissions and contact information for designated state employees. Users may print Employee Listings and Business Listings for an entire agency or for a selected agency department.

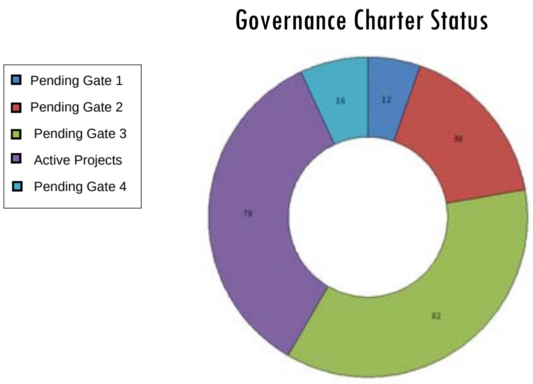
Perform a basic Search by entering either complete first and/or last name or wildcards (*) with partial names and clicking on the "Search" button to access address, telephone, and, when available, email information for state employees. An Advanced Search by Name, with a number of sort options and combinations, is available for more defined searches.

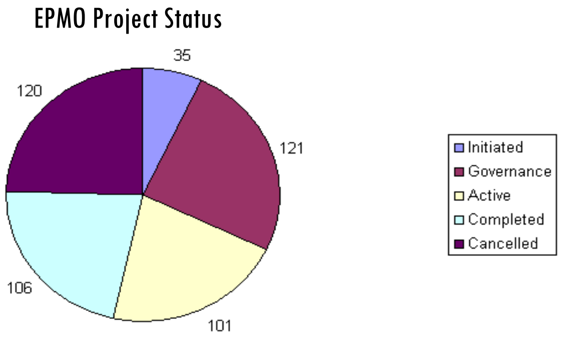
Over one hundred agency Telecommunications Coordinators participated in the specialized training in preparation for the CMS implementation of the new web-based SOI Directory on August 1, 2008.

The project began with a survey which helped ensure that the system was specifically designed to meet the Coordinators' current needs, while providing additional enhancements. After its debut, Telecom Coordinators gave the SOI Directory high marks for its ease-of-use and time-savings: 9.44 on a scale of 1-10. Agency Coordinators are actively taking advantage of the highly improved system. In the first two weeks of use, there had been more than 7,500 updates to the on-line State Directory. The public, state employees and private industry utilize the State Directory to reach specific government entities and agency staff.

Since implementation on August 1st, there have been 37,247 searches conducted on the public site of the State Directory. Following the successful implementation of Phase I, CMS is working on Phase II of the SOI Directory project which will provide even greater functionality. An agency's ability to extract their own data for publication of an internal agency Directory shouldn't be far down the road! ●

BCCS Projects at a Glance





Don’t Let Computer Problems Get You Spooked

October is Cyber Security Awareness Month

In recognition of National Cyber Security Awareness Month, **BCCS/Security and Compliance Solutions** would like to remind employees of the **TOP 8** simple, easy and basic things that everyone can and should do to protect their computer systems and data from harm by various cyber attacks and other types of security incidents that can cause damage, consume computer resources, or expose confidential information.

The goal of National Cyber Security Awareness Month is to educate everyday Internet users on how to *“Protect Yourself Before You Connect Yourself”.* You wouldn’t leave your home unprotected at night, so why make it easy for hackers and thieves to steal your financial information, or take over your computer to hurt others? Protect yourself.

Botnets, phishing, ad-ware, spyware and other attacks make up the more than $100 billion global market for cyber crime surpassing drug trafficking from a monetary perspective. The money obtained through cyber crime can be used to finance terrorism. The threats are real. Hackers are becoming more sophisticated and focused in their efforts. Cyber crime is big business; cyber espionage is on the rise.

Eight Cyber Security Practices to Stay Safe Online:

Protect your personal information…it’s valuable.

- If you're asked for your personal information – your name, email, home address, phone number, account numbers, or Social Security number – learn how it's going to be used and how it will be protected, before you share it.
- Don't open unsolicited or unknown email messages. If you do get an email or pop-up message asking for personal information, don't reply or click on the link in the message.
- If you are shopping online, be careful about providing your personal or financial information through a company's website without taking measures to reduce the risk.
- Read website privacy policies. They should explain what personal information the website collects, how the information is used, and whether it is provided to third parties. If you don't see a privacy policy – or if you can't understand it – consider doing business elsewhere.

Know who you are dealing with online.

- There are dishonest people in the bricks and mortar world and on the Internet. But online, you can't judge an operator's trustworthiness with a gut-affirming look in the eye. It's remarkably simple for online scammers to impersonate a legitimate business, so you need to know whom you're dealing with. If you're shopping online, check out the seller before you buy. A legitimate business or individual seller should give you a physical address and a working telephone number at which they can be contacted in case you have problems.

Use anti-virus software, a firewall and anti-spyware software to help keep your computer safe and secure.

- A firewall works by filtering information coming from and going to your network/computer and/or the Internet. It identifies and rejects information that comes from a location or source known to be dangerous or contains information that seems suspicious. Firewalls help keep hackers from using your computer to send out your personal information without your permission. While anti-virus software scans incoming email and files, a firewall is like a guard, watching for outside attempts to access your system and blocking communications from and to sources you don't permit.
- Anti-virus software protects your computer from viruses that can destroy your data, slow your computer's performance, cause a crash, or even allow spammers to send email through your account. It works by scanning your computer and your incoming email for viruses and then deleting them. To be effective, your anti-virus software should update routinely with antidotes to the latest "bugs" circulating through the Internet. Most commercial anti-virus software includes a feature to download updates automatically when you are on the Internet.

Be sure to set up your operating system and Web browser software properly and update them regularly.

Hackers take advantage of unsecured Web browsers (like Internet Explorer or Netscape) and operating system software (like Windows or Linux). Lessen your risk by changing the settings in your browser or operating system and increasing your online security.

(continued on page 6)

Don't Let Computer Problems Get You Spooked

October is Cyber Security Awareness Month

Use strong passwords or strong authentication technology to help protect your personal information.

- Using passwords that have at least eight characters and include numerals and symbols.
- Avoiding common words: some hackers use programs that can try every word in the dictionary.
- Not using your personal information, your login name, or adjacent keys on the keyboard as passwords. Changing your passwords regularly (at minimum, every 90 days).
- Using a different password for each online account you access or at least a variety of passwords with difficulty based on the value of the information contained in each.

Back up important files.

- No system is completely secure. If you have important files stored on your computer, copy them onto a removable disc, and store them in a secure place in a different building than your computer. If a different location isn't practical, consider encryption software. Encryption software scrambles a message or a file in a way that can be reversed only with a specific password. Also, make sure you keep your original software start-up disks handy and accessible for use in the event of a system crash.

Learn what to do if something goes wrong.

- Be aware of any unusual or unexpected behaviors. If your computer gets hacked or infected by a virus:
- Immediately unplug the phone or cable line from your machine. Then scan your entire computer with fully updated anti-virus software and update your firewall. Take steps to minimize the chances of another incident.
- Alert the appropriate authorities by contacting your Internet Service Provider (ISP) and the hacker's ISP (if you can tell what it is). Often the ISP's email address is abuse@yourispname.com or postmaster@yourispname.com. You can probably confirm it by looking at the ISP's website. Include information on the incident from your firewall's log file. By alerting the ISP to the problem on its system you can help it prevent similar problems in the future.

Protect your children online.

Even though children may have better technical skills, don't be intimidated by their knowledge. Children still need advice, guidance and protection. Keep the lines of communication open and let your child know that you can be approached with any questions they may have about behaviors or problems encountered on the computer.

- Keep your computer in a central and open location in your home and be aware of other computers your child may be using.
- Familiarize yourself with your children's online activities and maintain a dialogue with your child about what applications they are using.
- Implement parental control tools that are provided by some ISPs and available for purchase as separate software packages. Remember – no program is a substitute for parental supervision.
- Know who your children's online friends are and supervise their chat areas.
- Know who to contact if you believe your child is in danger. Visit **www.getnetwise.org** for detailed information.

Reference websites: *www.msisac.org, www.staysafeonline, and http://intra.state.il.us/security.*