CJIS
State of Connecticut
Criminal Justice Information System
Roadmap
Revolutionary Technology Linking Connecticut's Criminal Justice & Law Enforcement Community
July 2013 ~ Vol. 2, No. 7

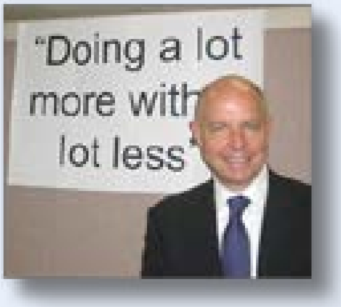
CJIS Rolls Out Two New CISS Team Sites

The CJIS Technology Team is working with the Division of Public Defender Services (DPDS) and one Law Enforcement Agency (LEA) on a project to build internal team sites using Microsoft SharePoint.

SharePoint Team Sites are Web sites, hosted on a corporate network and created from a template. "SharePoint can be used to provide intranet portals, document and file management, collaboration, social networks, extranets, websites, enterprise search, and business intelligence. It also has system integration, process integration, and workflow automation capabilities."*

CJIS Governing Board Co-Chairs

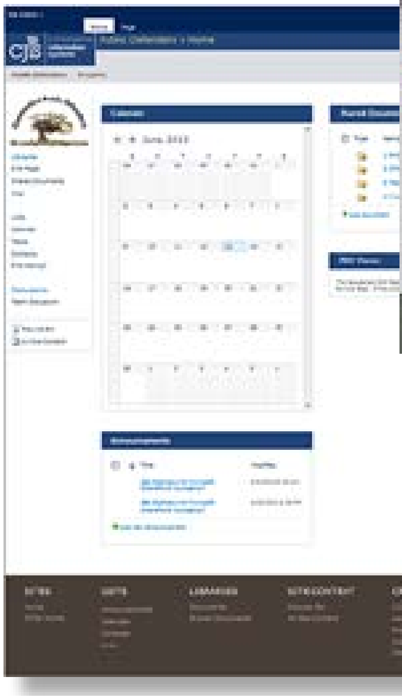
Mike Lawlor,
Under Secretary, State of Connecticut OPM
and
Judge Patrick L. Carroll, III
Deputy Chief Court Administrator



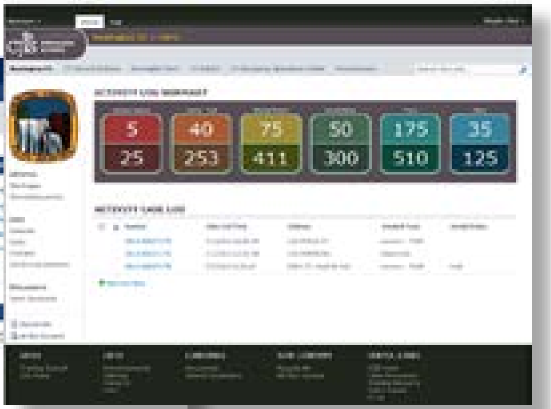
Mike Lawlor, Under Secretary, OPM

Team sites will provide a way to access CISS. From this site, an authorized user can quickly, search, access, and reconcile information they have with data from other agencies.

These team sites will become customized content management structures that encourage consistency and open collaboration between team members. The main benefits of having a team site include:



DPDS Team Site.



LEA Team Site.

- Expand the criminal justice knowledge base with state-wide resources
- Lower business and IT costs with a flexible and scalable collaboration platform.
- Better manage risk by safeguarding information with secure and reliable capabilities.
- Increase in productivity through cost-effective and efficient management.

The template for the Public Defender's team site was built using requirements provided by the business analyst for DPDS. Under those requirements, DPDS will be using a singular site consistent in appearance with other site pages, and only authorized users will be able to

Continued on page 7

CJIS Governing Board
Revolutionary Technology Linking
Connecticut's Criminal Justice &
Law Enforcement Community
July 2013 — Vol. 2, No. 7
www.ct.gov/cjis

Governing Board

Co-Chairs
Mike Lawlor, Under Secretary,
Office of Policy & Management

Judge Patrick L. Carroll, III,
Deputy Chief Court Administrator

Members
Garvin G. Ambrose, Esq., *Victim Advocate,*
Office of Victim Advocate
Reuben F. Bradford, *Commissioner,*
Dept. of Emerg. Services & Public Protection
Eric Coleman, *Senator,*
Co-Chair, Joint Committee on Judiciary
Melody Currey, *Commissioner,*
Dept. of Motor Vehicles
Donald DeFronzo, *Commissioner,*
Dept. of Admin. Services
James Dzurenda, *Interim Commissioner,*
Dept. of Correction
Gerald M. Fox, *Representative,*
Co-Chair, Joint Comm. on Judiciary
Kevin Kane, Esq.,
Chief State's Attorney
John A. Kissel, *Senator,*
Ranking Member, Joint Comm. on Judiciary
Richard C. Mulhall, *Chief,*
Conn. Police Chiefs Association
Rosa C. Rebimbas, *Representative,*
Ranking Member, Joint Comm. on Judiciary
Susan O. Storey, Esq.,
Chief Public Defender
Erika Tindill, Esq., *Chair,*
Board of Pardons and Paroles

CJIS Senior Management
Sean Thakkar, *Executive Director*
Mark Tezaris, *Program Manager*
Nance McCauley, *Business Manager*
Rick Ladendecker, *Technology Architect*

Comments, corrections, and inquiries
about this newsletter should be directed to:
Sean Thakkar, *CJIS Executive Director,*
Sean.Thakkar@ct.gov, or
Patty Meglio, *Technical Writer,*
Patricia.Meglio@ct.gov

PMO Perspective

Mark Tezaris, CJIS Program Manager

One of our key goals on the Connecticut Information Sharing System (CISS) project is to complete requirements for all search sources, information exchanges, and functional requirements by the end of 2013. This will allow both CJIS and Xerox to complete the project by the end of 2014.

There are many risks associated with the CISS project implementation, but the PMO and functional managers are working to assess the resources and the strategy needed to do this.

> *"One key change that we are implementing is a new policy for obtaining requirements from stakeholders that includes an escalation process if an agreement cannot be reached. "*

As part of the CISS "surge," CJIS hired additional staff and implemented new policies and strategy. We are also in the process of vetting out timetables with stakeholders and plan to meet with them to obtain requirements.

Since its introduction, the CISS Project proposed significant changes to the CJIS community. For this reason, the CJIS team has encountered some resistance. Some agencies have expressed legitimate concerns about sharing data, agency resource constraints, and security. Therefore, we are working very closely with the current agencies involved in requirements gathering to mitigate issues and find solutions that would be acceptable to all parties. Based on the agreed upon schedule, we will be working with the rest of the agencies to do the same.

One key change that we are implementing is a new policy for obtaining requirements from stakeholders that includes an escalation process if an agreement cannot be reached. Under this policy, the Business team will communicate with each stakeholder and

Continued on page 6

In This Issue

CISS Project Management Updates

John Cook, Lucy Landry, and Archana Mulay (interim) — Senior Project Managers

The CISS project is moving forward with three separate but interrelated waves — Wave 0, Version 1.5; Search Release 1; and Wave 1.

Wave 0, Version 1.5

In June, the CISS Project team continued with the construction of new environments. The Team completed the construction of the Development environment and the installation of four utility servers (that will provide secure network access, manage resource directories and user identities), and an integrated systems administration center.

Work progressed on a second Software Development Life Cycle (SDLC) environment, named System Test, and began processes to implement the remaining two environments; User Acceptance Testing & Training, and Production.

Approximately 58 virtual servers were created. The vendor conducted knowledge transfer sessions for staff on the new virtual machine environment. As the build out continues, the staff will review the documentation and submit suggestions for modifications to the vendor.

Both the utility servers for Microsoft System Center environment and the FileNet software were purchased. The team finalized the firewall and networking designs, which includes the design of the utility servers.

In the next few weeks, work will resume on the design of High Availability (HA) clusters. The HA clusters will curtail system down time in the event of hardware/software failure and ensure quick and secure data availability and restoration.

The Team is also planning to install the new CISS firewall and FileNet software for document management. Work will also continue on the refinement of the CISS virtual infrastructure with Xerox.

Search Release 1 (SR1)

Work on SR1 in June was focused on completing the final requirements for the Offender Based Information System (OBIS), and for search functionality, pre-defined reports, system administration and alerts, and User Interface (UI). We are currently working on completing the design for PRAWN and User Interface (UI).

MNI/CCH was removed from the current SR1 scope. We are working with DOC to complete data mapping, define the security and business rules, and secure the connectivity infrastructure to allow replication of OBIS information. We are also working with Judicial to complete the technical precursor work for replicating the CIB database.

Progress is being made in establishing the Learning Management System (LMS), which will be used to train new and existing CISS users.

Wave 1

The CISS Project team met with all nine agencies associated with Wave 1. We discussed the scope of Wave 1 and each agency's level of involvement. We also received input from the agencies on resource constraints that would affect the schedule. The team provided a detailed schedule to the agencies for the requirements phase, which is now available.

In addition, the CISS Project team is also currently working on the detailed requirements for the information exchanges that send incident arrest data to CISS (IEs 1.1, 1.2, 1.66, and 1.4). Meetings were held with both the Connecticut Police Chiefs Association (CPCA) and the Department of Emergency Services & Public Protection (DESPP) to determine how to source the data. ■

Staff Changes

Patty Meglio will be replacing Margaret Painter as Technical Writer for CJIS. She will manage all CJIS communications, including CJIS Roadmap and Quarterly Governing Board Report inquiries. Patty comes to CJIS with more than ten years experience in writing techinical documentation and commuication for the business community. Contact Patty at patricia.meglio@ct.gov or 890-622-2250. ■

CISS In Brief

WAVE 0, VERSION 1.5 (W0V1.5)

Current Work

- Kicked off W0V1.5 project plan to follow work activities identified in work breakdown structure (WBS), defined resource assignments, and created schedule.
- Constructed 1st Software Development Life Cycle (SDLC) environment called - Development.
- Constructed 2nd SDLC environment - System Test.
- Completed configuration for 2nd SDLC environment — System Test.

Next Month

- Begin construction of 3rd and 4th SDLC environments - User Acceptance Testing & Training and Production.
- Complete design of clustered and high-availability servers.
- Install new CJIS firewalls.
- Install FileNet software.

SEARCH RELEASE 1 (SR1)

Current Work

- Completed requirements activity for Search Functionality, Pre-Defined Reports, System Administration and Alerts.
- Initiated design of MultiVue Indexing, Saved Searches and System Admin/Alerts screens.
- Completed design activities for User Interface and PRAWN.
- Continued progress on Learning Management System (LMS) upgrades for SR1 training tasks.

Next Month

- Continue SR1 detail design.
- Initiate code development for SR1.
- Conduct UAT for DPDS and LEA SharePoint team sites.
- Establish connectivity with OBIS search sources.

WAVE 1

Current Work

- Reviewed W1 project charter and scope with each agency.
- Reviewed agency resources and availability for the project.
- Communicated schedule of work for requirements phase to all nine agencies.
- Started work on detailed requirements for Information Exchange (IE) for incident arrests.

Next Month

- Work on requirements for IE 1.5 and 1.6, which will send arrest paperwork to Court Operations and Division of Criminal Justice (DCJ).
- Commence gathering requirements for Content Management and FileNet.
- Produce requirements for IE for arrest notifications that will be sent to Bail/Probation, Board of Pardons and Paroles, Department of Corrections, Department of Criminal Justice, and the Department of Motor Vehicles (IEs 1.7, 1.8, 1.9, 1.10, and 1.53).

Technology Focus

Rick Ladendecker, CJIS Technology Architect

The Technology team is putting an infrastructure in place to support CISS. So far, they have assembled 150 virtual machines and 12 servers.

Additionally, the team is designing a model for High Availability (HA) clustering. HA clusters (also known as failover clusters) are groups of computers that support server applications that can be reliably utilized with a minimum of down time. They operate by harnessing redundant groups of computers or clusters that provide continued service when system components fail.

Without clustering, if a server running a particular application crashes, the application will be unavailable until the crashed server is fixed. HA clustering remedies this situation by detecting hardware/software faults, and immediately restarting the application on another system without requiring administrative intervention, a process known as failover.

As part of this process, clustering software may configure the node before starting the application on it. For example, appropriate file systems may need to be imported and mounted, network hardware may have to be configured, and some supporting applications may need to be running as well.

HA clusters are often used for critical databases and file sharing on a network. HA cluster implementations attempt to build redundancy into a cluster to eliminate single points of failure, including multiple network connections and data storage that is redundantly connected using storage area networks.

Leveraging new technology, the benefits for the new HA design for CISS include:

- Reduction of system down time in the event of hardware/software failure
- Secure data synchronization and timely restoration
- Ability to maintain the environment with greater precision
- Reduction in resources needed to maintain the system
- The formation of a secure and efficient disaster recovery plan

Reduction of system down time means that if any system components should have a problem, another group of computers will step up and take over, resulting in prompt operational recovery.

Secure data synchronization insures that data is safe and readily available in the case of a system malfunction.

Greater precision means that team members will be able to pinpoint any issues to specific locations on the system and quickly resolve them.

Because system maintenance will be cost and time efficient, **fewer resources** will be needed to support the system.

Finally, a **disaster recovery solution** will allow a fast replication of data instead of hours of re-programming the system.

The team is also developing a plan and drawing up a framework contract with Law Enforcement Agencies (LEA) to place data into a common data repository to support searching of criminal history. Requested by LEA, CJIS is stepping up to help meet this need. ■

OBTS and CIDRIS Updates

Due to current CISS work activities, the Offender Based Tracking System (OBTS) and the Connecticut Impaired Driver Records Information System (CIDRIS) will be maintained as operational systems. What this means is that no new user functionality, outside what is required to support the CISS application, will be created until such time that the CISS system is placed into a new server environment. Furthermore, no additional software releases are expected to be planned or developed, unless a compelling user case or system-related concern is determined. In the meantime, the OBTS and CIDRIS teams will continue work on data purity evaluations and other data migration activities to support the new CISS architecture. ■

Business Perspective

Nance McCauley, CJIS Business Manager

Several meetings have been conducted over the past year to draft the CJIS Security Policy. In June, CJIS Community stakeholders gathered to discuss how to move the CJIS Security Policy forward. The original goal was to have a draft policy ready to be reviewed by the Administrative and Technology Committees on July 11th for subsequent ratification by the CJIS Governing Board on July 18th. The CJIS Community agreed that the CJIS Security Policy was not ready at this time and recommended the following course of action:

- Assign a dedicated Project Manager to the CJIS Security Policy.
- Work with the DAS-BEST Security Team to determine next steps.
- Work with a CJIS Security Policy expert to facilitate the creation of a draft CJIS Security Policy.
- Review the CJIS Security Policy that is used by OBTS to gain efficiencies and not recreate the wheel. ■

2013 CISS Monthly Status Meetings

Our monthly meetings are held the second Wednesday of every month (with some exceptions) at 101 East River Drive, East Hartford.

- August 14
- September 11
- October 9
- November 13
- December 11

BA Team Customer Survey

Thank you for providing feedback on the BA Team Customer Survey. We appreciate the time you took to provide this information. We are reviewing the results in order to develop action items to improve the service and support we provide to our stakeholders. Look for an update in the August issue of the CJIS Roadmap. Thank you! ■

PMO Perspective, continued from page 2

set up mutually agreed upon dates for the CISS and stakeholder teams to meet for requirements gathering. The Business team will, in advance, send a template with the questions that need answers for the requirements process for Search and Information Exchanges.

The first phase of these meetings will produce a list of tables, fields, business rules, and security restrictions that apply to each shared field. In the second phase of the meetings, a statute or policy will be requested for all of the fields that the source agency has indicated cannot be shared. If there is a statute or policy restricting access to certain data fields, those fields will not be shared.

If there is no statute or policy indicating that the fields cannot be shared, a meeting will be setup by CJIS between the source agency and the consumers of the data agencies to negotiate what is needed by all. Upon consensus, CJIS will use that agreement as the requirements. If there is no agreement, CJIS will escalate to the CJIS Governing Board for a final resolution. This process will provide a definitive roadmap for requirements gathering for CISS with escalation for resolution. As a result, stakeholders can feel confident that their concerns on information security and accessibility will be addressed, and that there are formal methods in place that will determine the type of information that can and cannot be shared. This will ensure that the CISS Project will stay on track for completion in 2014.

We realize that implementing CISS state-wide will not be easy for all involved. But the goal and real opportunity to improve public and law enforcement safety is something that we all agree on.■

Go to www.ct.gov/cjis for FAQs, updates, meeting minutes & other information resources

Team Sites, Continued from page 1

view this site. All team sites will have a top banner that includes the CJIS logo and link to the office site. The bottom navigation banner provides links to commonly used pages and sites. Some sites will also include administrative pages, for example, HR or Financial Functions where applicable. A menu on the left side displays the Public Defender's logo and provides links to pages for shared documents, a calendar, announcements, a contact list, and other useful links.

Agencies can post content on the shared documents page for all team members to view and download. Documents are set up to be checked in and out, with a history of activity on the document, including who edited it and automatic version control. DPDS can use the calendar on its site to assign and track tasks and events for the agencies. They can also use the calendar to view events and tasks.

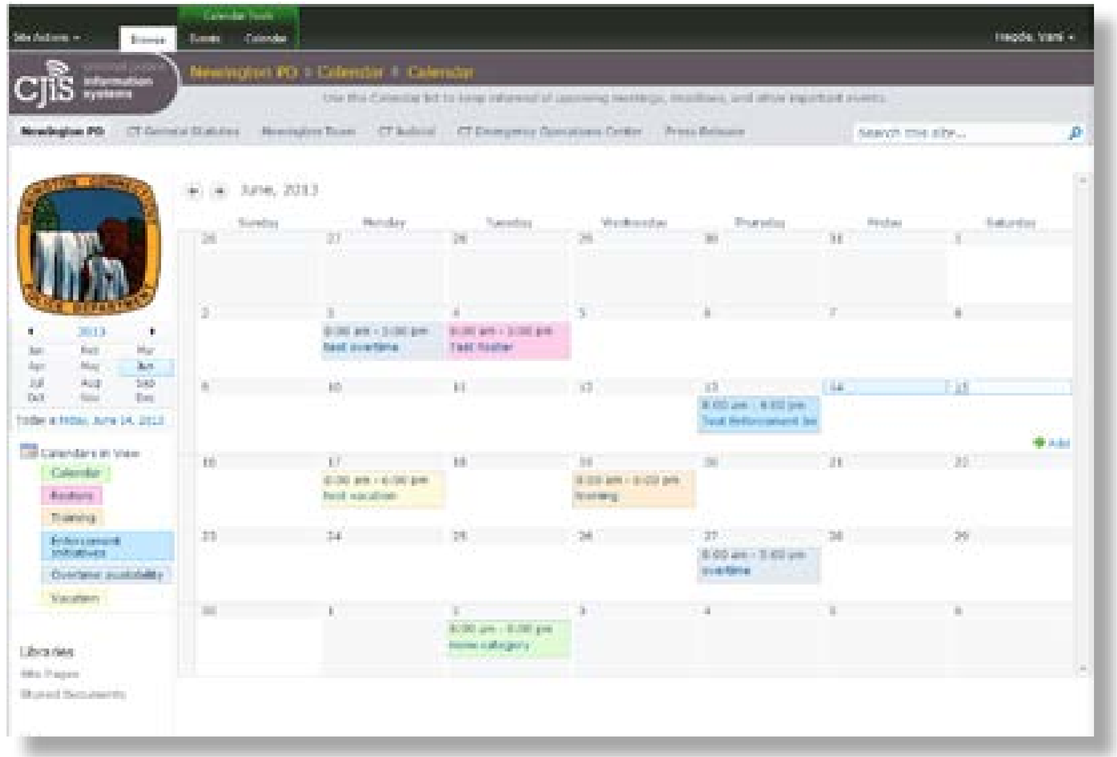
Currently in the test phase, the DPDS team site will support thirty local offices and five special units throughout the state and are expected to be in production by mid-August.

The LEA site prototype is made up of a singular team site that is customized based on their URL address. This will allow each police department to have their own look and feel based on their login ID, even though they are using a single team site. Similar in appearance to the DPDS team site, the LEA site has a top banner with the CJIS logo, and a bottom banner with links to shared pages. The side menu displays the town or city police department logo and lists Site Pages, Shared Documents, Calendar, Tasks, Activity Log Summary, and includes pages for Team Discussions.

The Activity Log Summary page includes a dashboard that displays statistical data. Currently the data is static, but in the future it will be dynamically displayed from a live feed, allowing the viewer to be able to get real-time data on statistics.

Below the Activity Log Summary, an Activity Case Log displays information on reported crime by case number, including addresses, incident type, and arrest status.

The main calendar display for the LEA sites includes four different calendars that are viewed by selecting from a color-coded list on the left navigation panel. LEA has individual calendars for Training, Rosters, Enforcement Initiatives, Overtime Availability, and Vacation.



Calendar view, LEA Team Site.

The CJIS Business Analysts will be working with LEA to obtain requirements for the final design and structure of the LEA sites. A test site is expected to be ready by early August. ■

* Microsoft SharePoint, http://en.wikipedia.org/wiki/Sharepoint, (July 2013)

Acronyms

- AFIS = Automated Fingerprint Identification System
- AST = Application Support System
- BEST = Bureau of Enterprise Systems and Technology
- BICE = Bureau of Immigration & Customs Enforcement
- BOPP= Board of Pardons and Paroles
- CAD = Computer Aided Dispatch
- CCH= Computerized Criminal History (DESPP)
- CIB = Centralized Infraction Bureau (Judicial)
- CIDRIS = CT Impaired Driver Records Information-System
- CISS = CT Information Sharing System
- CIVLS = CT Integrated Vehicle & Licensing System
- CJIS = Criminal Justice Information System
- CJPPD = Criminal Justice Policy Development and-Planning Division
- CMIS = Case Management Information System (CSSD)
- COLLECT = CT On-Line Law Enforcement Communications Teleprocessing network
- CPCA = Conn. Police Chiefs Association
- CRMVS = Criminal and Motor Vehicle System (Judicial)
- CSSD = Court Support Services Division (Judicial)
- DCJ = Division of Criminal Justice
- DAS = Dept. of Administrative Services
- DESPP = Dept. of Emergency Services & Public Protection
- DEMHS = Dept. of Emergency Management & Homeland Security
- DMV = Dept. of Motor Vehicles
- DOC = Department of Correction
- DOIT = Dept. of Information Technology
- DPDS = Div. of Public Defender Services
- FOIA = Freedom of Information Act
- IST = Infrastructure Support Team
- JMI = Jail Management System
- JUD = Judicial Branch
- LEA = Law Enforcement Agency
- LIMS = State Crime Laboratory Database
- MNI = Master Name Index (DESPP)
- OBIS = Offender Based Information System (DOC)
  OBTS = Offender Based Tracking System
- OCPD = Office of Chief Public Defender
- OVA= Office of the Victim Advocate
- OVS = Office of Victim Services
- OSET = Office of Statewide Emergency Telecommunications
- POR = Protection Order Registry (Judicial)
- PRAWN = Paperless Re-Arrest Warrant Network (Judicial)
- PSDN = Public Safety Data Network
- RMS = Records Management System
- SCO = Superior Court Operations Div. (Judicial)
- SLEO = Sworn Law Enforcement Officer
- SOR = Sex Offender Registry (DESPP)
- SPBI = State Police Bureau of Identification (DESPP)
- SLFU= Special Licensing of Firearms Unit (DESPP)
- UAR = Uniform Arrest Record Technology Related
- ADFS = Active Directory Federated Services
- COTS = Computer Off The Shelf (e.g., software)
- ETL = Extraction, Transformation, and Load
- FIM = Forefront Identity Manager (Microsoft)
- GFIPM = Global Federated Identity & Privilege Management (security standard used by FBI)
- IEPD = Information Exchange Package Document
- LAN = Local Area Network
- PCDN = Private Content Delivery Network
- POC = Proof of Concept
- RDB = Relational Database
- SAN = Storage Area Network
- SDLC = Software Development Life Cycle
- SOA = Service Oriented Architecture
- SQL = Structured Query Language