



State of Connecticut Criminal Justice Information System Roadmap

Revolutionary Technology Linking Connecticut's Criminal Justice & Law Enforcement Community

November 2012 | Vol.1, No. 7

Criminal Justice Records in CISS: *Same Rules, New Tools*

The mission of CISS, simply stated, is to collect and disseminate information — to act as the exchange — between criminal justice agencies to ensure that all in the Connecticut criminal justice community can efficiently obtain the most up-to-date information.

Criminal justice information in Connecticut originates with an arrest — by either local law enforcement or state police. From that initial arrest, information can flow through many agencies in the judicial, executive, and legislative branches of government. And historically, prior to the mid-1980s, everything was paper-based.

The way the criminal justice agencies move their data has undergone huge changes, and although progress has been made, the movement has been spasmodic and uneven. Some agencies have gone electronic, while others remain paper-based. Against this uneven and shifting landscape, the State of Connecticut passed legislation mandating the CJIS Governing Board to create CISS.

With CISS development underway, and with its initial launch coming up fast, stakeholders have expressed

concerns about the rules governing retention and deletion of records.

“We want to reassure our stakeholders that we understand that each of their agencies has their own policies, and we are working with them as we build CISS,” says CJIS Executive Director Sean Thakkar.

“We also want to emphasize that we don’t have answers to all questions at this time,” Thakkar says. “What we can say with certainty is that CISS depends on collaboration between all stakeholders. At each step in this building process, we are working to assure that our partners’ policies are integrated into CISS.”

The *general answers* to the overarching questions around CISS records access, retention, and deletion are simple — Connecticut statutes and the policies within each agency will continue to govern what information is shared, retained, expunged, and deleted (erased). The relevant statutes fall primarily within Connecticut General Statute Titles 7, 11, and 54. www.cslib.org/publicrecords/2011PubRecLawsRev.pdf and www.cga.ct.gov/2011/pub/chap961a.htm

There are two authorities that oversee public records and administer the

Continued on page 2

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

IN THIS ISSUE

Criminal Justice Records	1
CJIS Governing Board	2
News Briefs	3
CJIS Program Overview	3
CISS Updates:	
Technology	4
Testing update	5
Business	6
OBTS Update	6
CIDRIS Update	7
FAQs	8

CJIS Governing Board

Revolutionary Technology Linking
Connecticut's Criminal Justice &
Law Enforcement Community
November 2012 — Vol. 1, 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

Leo C. Arnone, *Commissioner,*
Dept. of Correction

Reuben F. Bradford, *Commissioner,*
Dept. of Emerg. Services & Public Protection

Eric Coleman, *Senator*
Co-Chair, Joint Committee on Judiciary

Michelle Cruz,
Office of Victim Advocate
Melody Currey, *Commissioner,*
Dept. of Motor Vehicles

Donald DeFronzo, *Commissioner,*
Dept. of Admin. Services

Gerald M. Fox, *Representative*
Co-Chair, Joint Committee on Judiciary

John Hetherington, *Representative,*
Ranking Member
Kevin Kane, Esq.,
Chief State's Attorney

John A. Kissel,
Senator, Ranking Member
Richard C. Mulhall, *Chief,*
Conn. Chiefs of Police Association

Susan O. Storey, Esq.,
Chief Public Defender
Erika Tindill, *Chair,*
Board of Pardons and Paroles

CJIS SENIOR MANAGEMENT

Sean Thakkar,

CJIS Executive Director

Mark Tezaris, *CJIS Program Manager*

Nance McCauley, *CJIS Business Manager*

Rick Ladendecker,
CJIS Technology Architect

Comments, inquiries, and corrections
about this newsletter should be directed to:
Mark Tezaris, *CJIS Program Manager,*
Mark.Tezaris@ct.gov, or
Margaret M. Painter, *Senior Communications*
Specialist, Margaret.Painter@ct.gov

relevant statutes that pertain to the CJIS community — the Judicial Branch and the State Librarian (whose authority is delegated to the Public Records Administrator). The latter has authority over all executive branch agencies and municipalities, which includes all local police departments. (csg 11-8-8a) www.cga.ct.gov/2011/pub/chap188.htm Records in the Connecticut criminal justice system originate in the system by one route — with arrests made by local and state police. The route that records travel from there varies widely depending on the details of the case.

The legislature created rules and vested authority in the Public Records Administrator to oversee the proper retention and destruction of records.

LeAnn Power, Connecticut's Public Records Administrator, explains that the specific time periods cited in public records' retention schedules are *minimum* requirements. <http://www.cslib.org/publicrecords/retschedules.htm>

Even though vast quantities of electronic data can now be stored in CISS at a fraction of the cost of paper records, that does not mean, says Power, that all records should never be deleted. "There are administrative, legal, fiscal, and historical criteria that factor into decisions of retention or deletion," she says.

From the perspective of some in the criminal justice community, since data can now be indexed and searched in ways previously unimaginable, it is *very useful* to retain this data. Of particular interest to the CJIS community and the team now constructing CISS is that CISS can be a permanent repository for

electronic criminal justice records.

There are a few areas of the law that mandate deletion of criminal justice records — for instance if a case has been nolledd — and there are very specific time parameters within which these actions must take place. www.cga.ct.gov/2011/pub/chap961a.htm

The most important thing to bear in mind about the availability of records in CISS is that it will be built to carry out the *business rules that agencies use now*. The only change is that CISS will be able to permanently store records.

The rules of access to CISS data will be created from within each agency by its own management, which will appoint a System Administrator to work with CISS to map its rules for the data it "owns" flowing into the system.

For instance, regarding security, the means of securing the data is different; the rules for who, what, where, when, and why will be the same. Whereas traditional paper files would be locked in a steel file cabinet accessible only to personnel who passed several layers of physical security and have a key, we now have virtual storage with layers of electronic security built around delegated authority, certificates, and means of authentication.

Each agency will also retain primary responsibility for changes to data after it is shared with its criminal justice partners. This, too, will not change.

If a statute change impacts data shared by an agency, it will remain the responsibility of that agency's System Administrator to communicate that

The rules for access to criminal justice data — the who, what, when, where, and why — will not change because of CISS. But CISS will revolutionize the way we transmit & use data.

CISS Project Management Team

Mark Tezaris, CJIS Program Manager

Top-notch project management skills are essential to handling the constant troubleshooting that is inherent in a large and dynamic project like CISS. Without this constant monitoring of risks, the CISS project could not have progressed this far.

April Panzer and Lucy Landry are the two Senior Project Managers working on the CISS project. When they joined the team, in March and June respectively, the project was just starting up; the Project Management Office had not been set up. Expectations, along with the stress level, were high. Together we drew up the blueprints for the CJIS Project Management Office (PMO) and began building it.

Now 10 months into the project, we are looking at delivering the first part of the OBTS Search (CISS Wave 0, version 1) in December 2012. The planning, people, and communication skills that Lucy and April possess are crucial to managing the day-to-day tasks necessary for successful project management.

These issues or risks are usually escalated to the Program Manager. I normally spend about a third of my day troubleshooting problems that could negatively impact the project. These issues cover a full spectrum — they can be technical, financial, or logistical. I am proud to report that we are on-target despite the recent hurricane. The

goal is to keep the team and project in scope, on schedule, and in budget daily.

This is the “micro management” aspect of our jobs. The recently-updated CJIS Strategic Plan is the “macro” aspect of project management. The Strategic Plan encapsulates the statutory mandate to the CJIS Governing Board; it spells out our mission and outlines how the CJIS operational team plans to carry out this mission.

Our next major step, in January 2013, will be to plan out Wave 0, version 2 and Wave 1 over a 30-day period, and more broadly lay out plans for the following 90 days. ■

Meetings in October

The October 18 Quarterly CJIS Governing Board meeting was an opportunity for the CJIS staff to update the Board on the status of all programs over the past 90 days.

Program managers reviewed the accomplishments and plans for OBTS, CIDRIS, and CISS.

Steven Wallick, System Administrator, gave a demonstration of the Nastel performance monitoring tool. Nastel was acquired a few months ago. After completing testing and training, it was put into operation recently, monitoring all the transactions in OBTS. Wallick emphasized the power, versatility, and usefulness of Nastel. The staff is excited about its potential for monitoring CISS, when it goes online.

Highlights for CISS were the

description of the timeline of the CISS project’s Wave 0, versions 1 and 2 and the accomplishments of the business and technology teams. This information was also reviewed in detail at the October 3 CISS Status meeting, attended by roughly 40 stakeholders. ■

For minutes of these and other meetings, visit www.ct.gov/cjis

Top right, Steven Wallick, System Administrator, demonstrates the Nastel performance monitoring tool at the October Governing Board meeting. Bottom right, Mark Tezaris, CJIS Program Manager, describes the early CISS project timeline during the CISS Monthly Status meeting.



CISS Technology Update

Richard Ladendecker, CJIS Technology Architect

The past month has been productive for the CISS Technology team. We have completed several vital tasks which are necessary to support CISS. These include acquiring storage and network equipment, and ordering the CISS firewalls.

During September, we received the storage sub-systems which will make up the foundation for the CJIS platform. The first of these two systems, the SAN (Storage Area Network) will contain the storage to support CJIS Development, System Unit Testing, User Acceptance Testing and Production. In all, this storage array contains a total of 203 Terabytes(TB) of space of which 136TB will be usable. The difference is the amount of storage required to support redundant RAID storage architectures (mirroring and stripping functions).

The three technologies that affect the throughput of a system are the storage configuration, the type of CPUs and the design of the application. In the case of storage, the SAN was defined and configured to contain four storage Tiers or “types of storage medium.” These tiers each have distinct characteristics which will be leveraged to support the CISS system.

Tier One — the most critical — is Solid State Disk, or SSD. This tier has high-speed electronic memory for its storage and delivers information 75 percent faster than equivalent high-speed rotating disks. Tier one will be used exclusively for the “indexing” environment in the CJIS application and will result in near 1-second response times for search results (at the

application level).

Tier Two contains high-speed (15K RPM), medium density disks (600GB), which hold the Operating Systems, the Primary Databases and files that require fast access. Tier Three will hold the replicated databases from the all agencies, including local law enforcement, and is made up of medium speed (10K RPM); higher density drives

Once CISS is fully mature, the replicated agency data environments will span more than 30 distinct systems and will hold in excess of several trillion records.

(900GB). These databases are updated frequently and are accessible only from the CJIS application precluding the necessity to have high-speed drives. The Fourth Tier contains the slowest drives (7.2K RPM) but these have the highest density; 2 TB. These drives are used for archived files and data which is not vital and not actively being accessed.

As we move into November and December we will develop the mapping plans to assign storage allocations to the various CJIS environments (DEV, SYSTEST, UAT, and PROD) and will culminate with provisioning these in early January 2013.

In September, we also acquired CONNX, the data access tool which will enable CISS to access and control the movement of data between

CISS agencies and CISS. CONNX is capable of integrating with almost all of the common legacy data environments (VSAM, ISAM, Relative, Indexed, RMS) and virtually all databases (Oracle, SQL Server, MySQL, Paradox, SyBase, Lotus Notes, etc.).

We installed CONNX in our development and system testing environments and successfully replicated OBTS data into CISS. The flexibility and functionality of CONNX will reduce the resources required to support Extraction Transformation and Loading (ETL) activities and will also be a vital tool to aid in publishing data to/from our agency partners. Once CISS is fully mature, the replicated agency data environments will span more than 30 distinct systems and hold in excess of several trillion records. Using CONNX enables the CISS application to index data from a common repository, SQL Server.

The initial proposition was to allow CISS to support accessing agency data via federated queries, copying replicated databases or crawling production databases. The limitations of using federated queries (asking agency systems to send data on a case-by-case basis) was the constant impact on the network and the large number of queries the agency systems would be required to respond to. This paradigm, combined with the requirement to maintain a 5-second-or-less average response time, made it unworkable to use federated queries. This left only two alternatives to collect

Continued next page


data from our CISS agency partners: crawling replicated or production data environments.

This situation also creates potential bottlenecks for CJIS. One issue involves replicated data being “stale” or “static.”

If data is replicated by an agency and this data is “old,” then two conditions could arise; (1) if the replicated data is sent as part of an information exchange, it has the potential of being incorrect and (2) if the data is not present in the replicated data environment then it cannot be searched.

Consider a case where “ticketing” a database is replicated for access to CISS every two hours. After the database is crawled by CISS and the Search Index is updated, a ticket record is added to the “live” database. A query for the License Plate of the vehicle or the individual of interest will not return any results until the next two hour interval passes and the replicated data is updated in CISS. While this example is simple, it could have catastrophic results for more time-sensitive data elements.

As we work with our agency partners we will identify issues such as these and resolve them using strategies which are effective and secure for all parties. ■



Technology
workshops
will resume in
January
(dates TBA)

Getting Ready to Test

April Panzer, CISS Senior Project Manager

CJIS will be the first agency to implement the federal security standard used to control information access, the Global Federated Identity and Protection Management framework, known as GFIPM (pronounced gee-fip-um).

This standard is based on the concept of a *federation*, defined as a “group of two or more trusted partners with business and technical agreements that allow a user from one federation partner (participating agency A) to seamlessly access information resources from another federation partner (participating agency B) in a secure and trustworthy manner.” Passports are an example of a credential used in a federation agreement. Each nation certifies their citizens’ identity, travel status, etc. and all other nations trust this certification and abide by the attributes of the identity.

The GFIPM identity claim provides a standardized means for allowing agencies to provide data access to trusted users that they do not directly manage based on:

- Identification/Authentication — *Who is the end user and how was he or she authenticated?*
- Privilege Management — *What certifications, clearances, job functions, local privileges, and organizational affiliations are associated with the end user that can serve as the basis for authorization decisions?*

From the collected attribute and privilege information, one or more claims are established for each user. These claims are also mapped to each data field and record for each database being searched by CISS.

The initial December launch of CISS will be limited to Sworn Law Enforcement Officer (SLEO) attribute claims. “A user is identified as a SLEO if all of the following conditions are true:

- The user is a full time employee of a state-recognized law enforcement agency.
- The user has the authority to make an arrest.
- The user is certified by a State Certifying Authority, such as Peace Officer Standards and Training (POST) or an equivalent.

Alternatively, a user is a SLEO if he or she is a full-time employee of a state-recognized law enforcement agency, acting on behalf of a SLEO, in performance of the user’s assigned duties.” *Global Standards Council* (www.it.ojp.gov/gsc)

By limiting this initial CISS release to *this one claim*, the intensive testing can ensure that security is 100 percent correct. ■

CISS Business Update

Nance McCauley, CJIS Business Manager

Global Federated Identity and Privilege Management (GFIPM) Claims Data Mapping Workshops

The CISS business team completed the series of workshops with CJIS partner agencies to map agency source systems' data to CISS. These workshops provided the CISS development team with the requirements for developing the business rules and associated GFIPM security claims for Wave 0, CISS Search, and Wave 1 UAR Information Exchange capability.

The collaboration of CJIS and the agencies' business and technical resources made this critical data mapping exercise a success.

The implementation of the GFIPM claims standard will position the State of Connecticut, CJIS for future secure and trusted information sharing among state, regional, local, tribal, and federal organizations.

Testing Activities for Wave 0, Version 1

In preparation for the implementation of the CISS Wave 0, Version 1 – CISS Search, the CJIS test group has drafted a detailed test plan to ensure the application meets the requirements for this release. As part of this plan, during the period from November 26th through December 7th, CJIS project testers will view and validate security, search, and data retrieval functionality to validate system functionality.

During the second week of testing, a small group of users selected from local law enforcement agencies and the Judicial Branch will join CJIS project testers to complete User Acceptance Testing (UAT) validation.

These initial users will review existing functionality, provide crucial input on the look and feel of the system, and give their impressions on performance and usability.

The testing process will give us valuable information that will be used to confirm that system requirements are met and that changes can be implemented in future iterations of the system to ensure that the completed system meets the needs of the end users. Successful completion of UAT is a valuable activity that will make CISS a more effective, efficient, secure and user-friendly application for sharing critical information throughout the CJIS community. ■

OBTS Update

Shirley Medeiros, CJIS Operations Director

The OBTS Quarterly Release 7.4 quarterly construction is complete and is currently in testing. The release deployment is scheduled for November 2012. The key changes for this release are in the areas of data purity and general database maintenance.

Data Purity Related Activity

The data purity review uncovered 40,533 arrest records where the UAR number was set to 99999999 from the Day 1 Data Population (D1DP). The business rule is that either a UAR number or a Ticket Number will be sourced, not both. The corrective action will set the UAR to a null value if there is a ticket number present.

The D1DP used "AR" for the Alien Registration code. The correct code is "Alien Registration," and that correction was made in this release.

General Database Maintenance Activity

The admin page priority sort order was corrected to display error filtering rules with respect to high and low priority.

The MRM event log was corrected to record the 'who' and the 'why' when starting and stopping any of the application's components.

Next Month

- Test and deploy Release 7.4 deliverables.
- Finalize Release 7.5 deliverables and begin construction.

The Next 90 Days

- Complete data comparison and evaluation effort of the Judicial Branch's source systems and document findings for OBTS/Judicial Branch systems.
- Kick off the data purity initiative for the OBIS system with the Department of Correction. ■

CIDRIS in Brief

John Cook, CIDRIS Project Manager

Criminal Records

Continued from page 2

Just Finished

- The CIDRIS program is making good progress. All 11 troop barracks are now submitting OUI cases. Based on a review of OUI submissions during the months of July, August and September, the combined troop activities show a success rate of approximately 69 percent for initial OUI submissions. This is a substantially higher level than the previously reported figure of 51 percent for the 2nd quarter and an increase of approximately 35 percent.
- Judicial and CJIS have completed testing of the new CJIS Forms Viewer application. The CJIS Forms Viewer allows CIDRIS users to search OUI document attachments by UAR and Misdemeanor Ticket Numbers and print agency documents on demand.
- DESPP completed development of a new CAD/RMS software program to help stakeholders reconcile electronic document attachments in support of the new CJIS Forms Viewer application.

Next Month

- The CIDRIS team will continue work to implement the CJIS Forms Viewer application. CJIS expects to complete system and user acceptance testing to prepare for transitioning the Forms Viewer into a production environment.
- DESPP and CJIS plan to update the CIDRIS information systems to support new statute numbers. As background, Judicial updates state statute tables several times each year to support changes to criminal offense codes. The statute table updates also require DESPP staff to assign and link National Incident Based Reporting System (NIBRS) codes to the new statute table before use in CAD/RMS. NIBRS is part of the Uniform Crime Reporting Program.
- CJIS is also working to expand the CIDRIS program to add support for the Division of Criminal Justice. Initial work efforts include coordination of new team members, planning exercises and analysis of agency technology architecture and systems.

Next Three Months

- Achieving near 100 percent data accuracy with CIDRIS OUI submissions is a high and necessary priority to support CJIS agencies transition to use paperless records. As a result, the CJIS team will continue to review submission errors from DESPP and promote good practices for process improvements with DESPP, the Judicial Branch, and DMV. ■

change and interpret its impact. Again, the business rules will be the same, but CISS will be the mechanism for transmitting information to the respective agencies.

“The processes by which these events take place are being developed as we construct CISS,” says Rick Ladendecker, CJIS Technology Architect. “Because records retention statutes specify minimum timeframes, is it possible that one agency — the Board of Pardons and Paroles — might deem it necessary to obtain information from an agency that may choose to delete its records after that minimum has expired? Yes, it is possible. Therefore we believe that unless there is a legal imperative to destroy a record, CISS should retain records indefinitely.”

John DeFeo, Executive Director of the Board of Pardons and Paroles says, “Regardless of what the other agencies’ retention policies are, BOPP is entitled to all information [on an offender] and may retain any relevant information. So that is not an issue for us.” DeFeo also notes that the broad rules established by the State Public Records Administrator don’t restrict BOPP.

“The bottom line is securing the information BOPP needs to make good decisions,” and, he says, “CISS will be an invaluable tool to do just that.”

The CJIS Governing Board’s administrative committee met and discussed retention periods. The committee will survey all agencies and report at the January 2013 Governing Board meeting. ■ ~ Margaret M. Painter

For more information on Connecticut’s Public Records Administration, go to www.cslib.org

FAQs

What is Electronic Document Management and how does it support CISS?

Enterprise Content Management (ECM) is the strategies, methods and tools used to capture, manage, store, preserve, and deliver content and documents related to organizational processes. ECM tools and strategies allow the management of an organization's unstructured information, wherever that information exists.

There are multiple forms of information but in effect they all break down into two distinct categories, Structured and Unstructured. We are all familiar with computer systems and their ability to manipulate information, commonly using database and/or data files to process as information. This is the "structured" category of information. This type of data can be sorted, searched, added, changed, deleted, have calculations made against numerical elements and a slew of other functions. Structured data is on almost all business environments the common underlying foundation to data processing. It appears in the form of reports, as information in our personal bills, across the television as a stock ticker on CNN or as statistics presented in a meeting.

Unstructured data is entirely different whereas this data can be in the form of images, binary data files, audio or video recordings, electronic documents and almost any other element of electronic media that cannot be classified as structured. Imagine trying to sort an image from a fingerprint or sorting an audio recording by words contained in the recording. Computers are not commonly designed to process unstructured data as easily as structured data. This is where the value of Electronic Content Management (ECM) comes in.

ECM are technologies that help us streamline and automate business

processes, connect with information systems, and access and manage content across an enterprise. The best of breed for ECM systems tend to be reliable, scalable, and highly available enterprise platforms which integrate content and business processes across individual organizations and interconnected communities.

The CISS project design uses IBM's FileNet as its Content Management platform. Some of the key benefits of IBM's FileNet ECM are listed below.

Manage Risk and Ensure Compliance:

Controlling the use and access to information, FileNet enables use of claims-based security and supports advanced security, comprehensive auditing, events, lifecycle management, and workflow capabilities.

Increased Agility and Responsiveness:

FileNet also allows organizations to manage a full range of structured and unstructured data, and processes information securely and reliably. It uses object-oriented metadata repositories that provide maximum flexibility for setting up document and folder classes, as well as content storage options. This will provide CISS with the agility it needs to support its 24x7 environment in real time.

Maximize IT Investments:

FileNet is based on industry standards, such as J2EE and XML Web Services, to enable agencies to maximize the investments they have already made in their IT environments. Extensive testing with industry-leading infrastructure products is done to ensure FileNet applications can be deployed rapidly in any environment.

Real-time Monitoring:

The FileNet platform provides a set of systems and performance monitoring features including integration with leading Enterprise System Management (ESM) tools. This enables system administrators to view system performance in real-time – identifying potential problems before

they occur and ensuring optimal uptime for CISS. In addition, FileNet supports the leading clustering, high-availability, and disaster recovery products.

Broad Range of Integration Options:

The FileNet platform provides a powerful set of capabilities for integrating with desktop and packaged applications, content repositories, and legacy systems – enabling agencies and individual facilities to communicate with one another, regardless of installed platforms.

Support for Many Storage/Media Types:

FileNet supports the leading storage vendors in the industry and a comprehensive range of both hardware and software offerings over all popular media types including SAN, NAS, and iSCSI.

For the CISS world, FileNet will be used for two distinct environments: the first accommodates the ability for CISS to store Electronic Content (EC) from documents attached to Information Exchanges (IEs); the second for agencies and LEAs to store criminal justice data – a repository for EC that they can easily access. CISS will scan this EC repository to support searching and retrieval of documents.

Agencies and LEAs will be able to search their own EC repositories. No agencies or LEAs will be allowed to directly search the CISS EC repository (1) where Electronic Content from Information Exchanges is stored. The security implications and restrictions being implemented as part of CISS prevents this EC repository from being searched directly since CISS is supporting a Claims based architecture for security and FileNet uses a Domain based architecture, both of which are not interoperable with each other. ■

For more information on any of these subjects or to submit a question or subject for discussion, please email margaret.painter@ct.gov.