CJIS
State of Connecticut
Criminal Justice Information System
Roadmap
Revolutionary Technology Linking Connecticut's Criminal Justice & Law Enforcement Community
September 2012 | Vol.1, No. 5

CISS: Public Safety Depends on IT

Chief Richard C. Mulhall on Information Technology

When Chief Richard C. Mulhall began his law enforcement career, a cutting-edge mobile communications device was the size of a small suitcase.

The Chief saved it, along with others he's used over the years. The devices are displayed on a shelf in his office at the Newington Police Department; the oldest and largest is about 2-feet high, with a bulky handset and cords dangling from the side. The other devices form a steep slope down to the smallest device, about the size of a pack of cards — a three-dimensional representation of a 40-year career in law enforcement.

A self-described "geek," Chief Mulhall has maintained a keen interest in harnessing the power of technology for law enforcement and is a strong advocate of the Connecticut Justice Information System (CJIS) and the development of the Connecticut Information Sharing System (CISS).

The power of these communications devices has increased in inverse proportion to their physical size and cost. And the laptop computer — unimaginable in the '70s — in every police vehicle has infinitely more computing power than the "super computers" of the day that filled entire rooms, and when 3-foot diameter disks were touted to hold 80 MB of data. The Chief's career has followed a similar trajectory. Chief Mulhall began his career in law enforcement at the age of 19 when he took a job as a dispatcher in the Farmington Police Department. That's where he says he got "hooked" on law enforcement. He went on to get an associate's degree in criminal justice, followed by a bachelor's in sociology at the University of Connecticut. Eventually, he earned a Master's in Public Administration at the University of Hartford.

In his first police job, he was a patrol officer in Avon. He rose to the rank of Sergeant, and because of his technical inclination, ended up helping out with technology in the department.

In 1984, he went through high-tech training at the FBI academy with "the nerds," adding that he was disappointed he couldn't do some of the "fun stuff" like SWAT training. "Computerization was still a new thing. We were taken to a lot of federal labs and saw a lot of things that no one had seen" at that point.

In 1986, Chief Mulhall was named Operations Captain in Bloomfield, where he began putting laptops in squad cars and using computers to maintain photographs of perpetrators. It was one of the first mobile data terminal systems in Connecticut. It was a regional effort using radio frequency to carry the data stream. "We ended up putting up transmitters on Avon Mountain, which was pretty slick at the time," he says with a wry smile.

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

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

He became chief in Bloomfield in 1995, and in 2002, he was named Chief of the Newington Police Department.

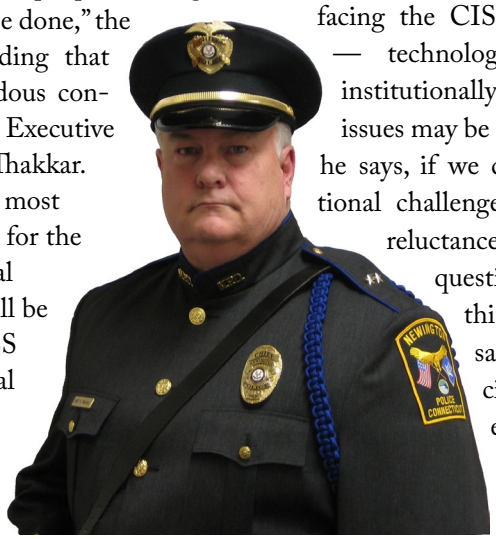
Chief Mulhall's work to improve law enforcement through the use of technology has paralleled his rise through the ranks. In the mid-'90s, he began working with the technology chairman of the Connecticut Police Chiefs Association (CPCA). He became acquainted with CJIS early on through his involvement with the CPCA's technology committee. In 2013, he will assume the position of President of the CPCA.

As far as harnessing information technology for police work, Chief Mulhall doesn't disguise his frustration with some of CJIS' early efforts. The two earliest statewide systems — OBTS and CIDRIS — have had their respective issues and limitations.

But with the Connecticut Information Sharing System (CISS) now under construction, the Chief is enthusiastic. "The good news is that since 2008, we are moving forward."

The Chief appreciates the fact that the CJIS operations and business teams began their fact finding to build CISS with those who originate most of the information in the system — the local cops. Municipal police make 85 percent of the arrests; state police account for the other 15 percent of arrests in Connecticut. "The people in charge know what needs to be done," the Chief says, adding that he has tremendous confidence in CJIS Executive Director Sean Thakkar.

One of the most difficult aspects for the CPCA and local departments will be interfacing CISS with the 91 local police departments' CAD-RMS systems.



There are roughly 20 different systems operating in Connecticut and each one will require specific work both by a local vendor and CJIS. As the interfaces come online, it is anticipated that the new fiber optic Public Safety Data Network (PSDN) will carry public safety data between the local RMS and CISS systems. Once completed, every line cop will benefit from this information sharing project by receiving life-saving information prior to arriving at incident scenes.

The CJIS team is moving along in the process of working with these vendors to define solutions. One of the first steps — a joint effort between the CPCA and CJIS — is to get all RMS vendors CISS-Certified. "They don't have a choice," the Chief says. "If they want to do business with us, they have to be certified. CISS is going to be a reality, and they will have to work with it." Chief Mulhall says he is optimistic. "Personally, I'm excited. I see a much different attitude from the people that are sitting at the table now. Everyone seems to be on board and truly wanting to see this succeed," he says, referring to the 11 agencies that make up Connecticut's criminal justice community. "They've shown up at the meetings and are asking the right questions. There's enough horsepower, and we have a strong project team, and a good leader."

The complexity of the difficulties facing the CISS project are enormous — technologically, logistically, and institutionally. The tech and logistical issues may be the least of our problems, he says, if we don't master the institutional challenges — among them, the reluctance to change. "There is no question that we have to do this," the Chief says. "Public safety depends on it. Our citizens and police officers expect us to accomplish this mission."

~Margaret Painter

CISS Tech Workshop 1: Agency Data Replication

Rick Ladendecker, CJIS Technology Architect, at the August 23 Workshop.

The first CISS Technology workshop for stakeholders on August 23 was attended by more than 30 representatives from all criminal justice agencies, town IT specialists, and police departments.

Rick Ladendecker, CJIS Technology Architect, gave an overview of the CISS architecture, and the three options for agency data replication.

The three options are Federated, Agencies copy their data and present it to CISS, and direct replication (crawling) of production environments. More details are explained on page 4 and in the meeting PowerPoint presentation.

For a copy of the PowerPoint presentation with the three options, as well as other resources and white papers pertaining to the CISS project and technology, go to www.ct.gov/cjis. ■

CJIS Program Overview

Mark Tezaris, CJIS Program Manager

The first monthly status meeting for CISS on August 1 was attended by over 30 stakeholders. We presented an update of the project — July's accomplishments and plans for August. The main focus of the project management team is to complete the project schedule for Wave 0, (see page 6), synchronize those touch points with the Xerox schedule, and implement the solution on schedule, scope, and budget.

As we make progress, good communication with our stakeholders is essential. Therefore, we will be holding our monthly project status meetings and technical workshops, in addition to meeting with agency and law enforcement partners, vendors, etc. to work on specific tasks (e.g., mapping).

The technical workshops, mainly for technical managers of agencies that will be connecting to CISS, are intended to demonstrate the technology we are developing. The primary purpose of these workshops is to educate our constituencies as we build. We want to get our stakeholders' feedback during the build, not after, to make sure CISS meets or exceeds their current needs and is designed to handle our future needs as well.

The CISS team presented a demonstration of the FAST Search of OBTS at the August 1 meeting, similar to the CJIS Governing Board demonstration.
We had a larger than expected turnout with many subject matter experts both on the business and technical side, many members from law enforcement, and CJIS agency managers. This made it difficult to answer all the questions that came up. Several constructive changes came out of that meeting, among them, an open forum in which to discuss questions or issues of interest submitted by stakeholders.

Some of those questions and issues are included in the minutes of the August meeting and in the status update for September sent out the last week of August, which we will review at the September 5 meeting.■

CISS Technology

Richard L. Ladendecker II, CJIS Technology Architect

During August, the Technical group focused on acquiring two key technical architecture elements necessary to the CISS project — data storage and data replication.

Storage

The entire CISS environment will be comprised of more than 125 virtual servers that will support Development, System Testing, User Acceptance Testing, and Production. The magnitude of servers will contain more than 200 databases made up of Agency and Law Enforcement data, multiple Web Sites for the SharePoint Portal, Indexing applications, the Enterprise Service Bus (the CISS work flow), and numerous application support servers.

After a lengthy process to define requirements and through collaboration with several vendors, we have selected two storage sub-systems that meet our technology requirements. These sub-systems will handle the numerous databases and the diverse files sent by the agencies as part of their information exchanges. Both sub-systems have elements that handle device failures, have redundant controllers, and are manageable by the CISS and BEST technical support groups.

Data Replication

A focal point of the CISS environment is its ability to search numerous databases and complex files (PDF, Word, Excel, etc.) and to generate indexes that are used by the "Search Portal." The indexes contain searchable fields and "words" and are continually updated from data replicated from agency data environments and from data and attachments sent as part of "Information Exchanges." Sensitivity and relevancy are the two most important criteria for determining the frequency of "crawling" Agency data structures. Information that is dynamic (changes rapidly and continuously) and is highly relevant to stakeholders would be "crawled" with greater frequency than data that tends to be stagnant or of lower relevance to a CISS User.

The CISS technical requirements for Data Replication include 1) single product that can access virtually any data environment; 2) is simple to install and configure; 3) has a low impact on an agency and CISS; 4) is auditable and logs and timestamps all transactions; 5) is scalable; 6) supports governance; and 7) can move information from any data environment to any other data environment using simple or complex algorithms.

Gathering Security Profiles

During August, the CISS Technical group began soliciting Security Integration Options from CJIS community agencies. The agencies have the ability to select from three different security models: Federated, Trusted Domains, and Internal CISS. Each model has properties that will handle any Security Authentication integration between CISS and the agency. In several cases, more than one model will be adopted as several agencies have multiple authentication environments within their organization.

Mapping

The CISS environment implements claims-based architecture, as opposed to the current roles-based environment. The Claims-Based methodology provides a fine granular definition to security compared to the Roles-Based model. It has been widely adopted in Federal and state agencies for handling security and authentication processes. Claims-based architecture is used to provide a definitive structure for mapping agency data elements, defines the Claim attributes of a CISS User, and allows CISS to clearly delineate "who" can see sensitive information.

Creating Technical Architecture Design Documents

Technical Design Document Reviews by the Technical Group continued in August and will be an ongoing effort as part of progressive elaboration with Rolling Waves (the project methodology CISS is using; see page 6.)

The initiation of each wave will include detailed design reviews to incorporate the development and implementation of new processes, technologies, and architectures.

Providing documentation for the CISS environment requires identifying all aspects of the CISS project where it interfaces at all levels with any organization. This includes support, training, code testing, quality testing, performance standards, communications, security, and a series of other attributes. The CISS Technical team, in conjunction with the CISS Business and Project Management groups and the Xerox/AIC teams, have been developing support and technical documents to support Wave 0 — CISS search of OBTS. This effort also includes documenting SLAs with BEST and Xerox, and identifying and developing Standard Operating Procedures (SOPs). This includes creating documentation for integration with our agency partners for Information Exchanges and Security/Authentication integration. ■

CISS Project Overview

Lucy Landry and April Panzer, Senior Project Managers

The first production implementation of CISS is just around the corner. Following the rolling wave method of development, this first release is Wave 0. It will give users the ability to search the OBTS database from the CISS Search Portal. As was demonstrated in July and August, the increase in performance is significant.

The CISS business team has been and will continue reaching out to the CJIS Community for input in several important areas. (See right column, this page.)

Coming up, the technical team will be discussing user access security with the stakeholders' technical representatives. The CJIS business team will finalize requirements and design for System Administrator functionality. Each agency will also need to nominate an agency CISS System Administrator.

Training for Agency System Administrator and those "Super Users" that will be participating in User Acceptance Test, will take place in the fall. The training will be accessible online and should take no more than 30 minutes to complete. Agency System Administrators and super users will be contacted with training dates.

The first group of users to access OBTS via CISS in December will be from DOC, DMV, DPDS, SCO, CSSD, OVA, DESPP, as well as the following local law enforcement agencies: Berlin, Branford, East Haven, Fairfield, New Haven, Plainville, Watertown and Windsor Locks. Other users will be brought on during the first quarter of 2013.

In the coming months, we will also be developing Help Desk processes and SLAs. ■

See what's developing at www.ct.gov/cjis

CISS Business Update

Nance McCauley, CJIS Business Manager

The CJIS Business Team has been busy over the past month gearing up for Wave 0 of CISS — OBTS Search. We have attended a series of knowledge transfer sessions led by the Xerox Team regarding GFIPM and claims-based Security topics.

The CJIS Business Team and Collin Evans from the Xerox Team conducted GFIPM data source mapping sessions for the Judicial systems that currently send data to OBTS to determine field-level security rules that apply to the data elements. The sessions were interactive and productive. Documentation will be sent out for review and to verify information that was gathered.

In August, the CJIS team attended the TriTech Software Systems annual meeting to provide information, discuss next steps, expectations, and answer questions for the LEAs that TriTech supports. (TriTech is one of 16 vendors that provide State LEAs with CAD-RMS software.)

In September, the business and technical teams will send out RMS vendor certification packages to all of the CAD-RMS vendors.

The CJIS Business Team visited the New Britain, Derby, and Hartford area courts to observe the Division of Public Defender Services business processes. The observations were very enlightening and highlighted gaps in sentencing business processes as well as areas that will benefit from electronic processing in the future through the CISS Project. We have determined that the sentencing requirements will be included in Wave 1 of the CISS project.

Screen mock-ups of the CISS application were distributed to business stakeholders for review, with a feedback deadline of August 31.

The CJIS Business Team is working with the Division of Criminal Justice to schedule observations of CISS business processes in the courts for the month of September. ■

CISS: There *is* a Method to this Madness

As the CISS project gets into full swing, it is evident that some of our stakeholders are concerned about our methodology. There have been questions like: "Why are you building the infrastructure and code without the fully completed specifications?" "Why are the specifications for auditing, security, infrastructure and other areas of the project still not complete?" So there is some concern that the CISS operations team is "making it up as we go along." Of course this is not the case, but it might seem that way to those used to traditional waterfall project methods.

In contrast to the traditional "waterfall" methodology that many managers are accustomed to, the CISS Project is using a "Rolling Wave" iterative methodology.

The traditional waterfall methodology is often considered the classic approach to the systems development life cycle. This development method is linear, sequential, and has distinct goals for each phase of development. When one phase is completed, the development proceeds to the next phase, and turning back can be costly.

The major advantage of waterfall method is that it allows for departmentalization and management control. Development moves from concept, through design, development, testing, installation, troubleshooting, and ends up at operation and maintenance. Each phase of development proceeds in strict order, without any overlapping or iterative steps. The disadvantage of waterfall development is that it does not allow for much reflection or revision. Once an application is in the testing stage, it is very costly to go back and change something that was not considered in the concept stage.

Rolling Wave planning is a project management technique that involves progressive elaboration to add detail to the Work Breakdown Structure (WBS) on an ongoing basis. At the beginning of the project, near-term deliverables are broken down into work packages and defined at the greatest level of detail. Approved requirements are elaborated in sufficient detail required for the next iteration. Deliverables and schedule activities that will take place several reporting periods in the future are more broadly defined. Currently, in the CISS project, Wave 0 is broken down fully in the WBS. Waves 1 through 3 are outlined only to the level of subprojects.

While scheduled activities for Wave 0 are underway, the detailed planning for Wave 1 will begin. As Wave 1 is put in motion, planning for Wave 2 will start and so on.

This would be counterintuitive to those who are used to the waterfall method and expect all of the details to be worked out before the build starts.

There are several advantages to the wave approach. First, results are delivered faster so there is faster Return On Investment (ROI). Stakeholders get a close look at the wave deliverables and are able to provide feedback. This, in turn, increases the likelihood of customer satisfaction. Waterfall delivery can take years from start to finish, risking its own obsolescence by completion (particularly in the technology arena).

CISS is unique in the nation because it will connect and share data throughout the whole CJIS community, not just parts of it as other states have done. The wave approach allows for discovery of the best way to build the next wave as we get closer to it. ■ ~ *Mark Tezaris*

Wave 0

CISS Wave 0 — OBTS Search — will be available for users starting in early December. For those of you who saw the early product demonstrations in July, Wave 0 will look familiar. The main difference will be more fields for structured search and a more finely-detailed search results page.

Wave 0 will also include full claims-based security, so each user will see records and data elements that they are allowed to see based on their GFIPM (Global Federated Identity and Privilege Management) claims. Full logging of every user interaction (from login, through searches and logout) and audit capabilities will also be implemented for Wave 0.

While Wave 0 is being developed and tested over the next couple of weeks, detailed design work will begin on Wave 1 (Uniform Arrest Report or UAR); the first set of "information exchanges" that will involve multiple agencies and move information (notifications, messages and documents) around as required, safely and securely, to their destinations based on a triggering event, which in Wave 1 is a felony arrest.

As the CISS project continues, successive waves will deliver functional components for Search (more agency sources), the user Portal (including agency "team sites") and additional information exchanges logically grouped by workflows. ■ ~ *Phil Conen*

CISS Technology Workshops

The CJIS Technical Team will be conducting Technology Workshops into the forseeable future for our stakeholders and their technical staff to familiarize them with CISS technology. Several of these technology topics will be divided into varying levels of proficiency to allow stakeholders with differing technical knowledge to absorb the content.

- **CISS Security, Part 1 — Wednesday, September 5**
- **CISS Security, Part 2 — Thursday, September 20**
- **Service Oriented Architectures** (SOA) — including NIEM, LEXS, JIEM (October, TBA)
- **SharePoint** — for new, intermediate and power users, including advanced & customization examples for administrators (date TBA)
- **SQL Server** — for new, intermediate & advanced users, covering object broker, SQL Server Integration Services (SSIS), SQL Server Reporting Services (SSRS), SQL Server Analysis Services (SSAS), security, performance
- **Enterprise Service Bus** — WebMethods — Integration for intermediate and advanced technical staff who are interested in using Software AG's WebMethods products.

We will post workshop dates in advance. ■

OBTS IN BRIEF

Shirley Medeiros, CJIS Operations Director

Just Finished

- Completed implementing Release 7.3 deliverables to the production environment
- Finalized Release 7.4 deliverables

Next Month

- Begin constructing deliverables for Release 7.4
- Finalize Release 7.5 deliverables
- Continue data mappings of the Judicial Branch's source systems
- Use the Nastel performance tool to identify problem areas
- Conduct OBTS Certification Class at Judicial's Learning Center 9/12

CIDRIS IN BRIEF

John Cook, CIDRIS Project Manager

Just Finished

- Six remaining troops were deployed on CIDRIS.
- In preparation for deployment, training sessions for Troop Barracks and General Area courts for Troop Districts E, K, D, H, C, and F were completed.
- Training also completed for Troops H, C, G, and F during August.
- The implementation cutover to begin submitting Operating Under the Influence (OUI) related charges through CIDRIS began August 10 for Troops E, K and D and August 17 for Troops H, C and G.
- CJIS staff worked with Judicial and DESPP to enhance electronic access to Bondsman file updates.
- Implementation workgroup began review of CIDRIS and Source Agency system use of the FBI National Incident-Based Reporting System (NIBRS) codes, in preparation of 2012 State Statute number updates, expected to be released in October.
- DESPP began work to streamline and enhance OUI submissions to Judicial. This includes an initiative to prioritize and standardize each of the possible combinations of document submissions across all barracks.

Next Month

- Reviewing Agency requests to update CIDRIS message exchanges. One request is for tracking an additional disposition type used to track suspended driver's licenses and disqualified commercial driver licenses.
- The team is also working to reduce duplicative document attachments during message rejects.
- The Implementation workgroup is also developing an automated reporting system to help track and reconcile electronic document submissions between agencies. This effort lays the ground work for reducing delivery of paper-based OUI documents.

FAQs

Q What is GFIPM?

The use of GFIPM is a requirement of the CISS RFP. GFIPM stands for "Global Federated Identity and Privilege Management" and is a federal standard published and used within the US Department of Justice and by its federal and state partner agencies. GFIPM is centered on the exchange of security tokens between trusted identity providers. A service provider (in this case CISS) trusts an Identity Provider to provide security information about a user. This security information is included in a security token with every request made by the user of the service. The security token contains security *claims* about the user. A claim is a *statement of truth* or a *fact*, about the user that the Identity Provider *claims* to be true. For example, an Identity Provider might claim that a person's last name is "Smith" and that their first name is "Joe." Since the service being accessed by the user trusts the Identity Provider that is providing the security token, it can make access control decisions based on these facts (claims) provided about the user.

GFIPM provides a dictionary of claims, referred to as the "GFIPM Metadata." Similar to the NIEM standardization of a criminal justice terminology dictionary, GFIPM provides a dictionary of security related terms (claims) that can pertain to a user. By having a standard dictionary/vocabulary, partnering organizations (a Federation) have a common language for describing information about users, also known as the users' *Federated Identity*.

The *Privilege Management* portion of GFIPM is the ability of a service provider to make access control decisions based on the security claims that were provided for that user. A security token might contain a claim asserting that the user is a sworn law enforcement officer, and CISS can restrict access to specific functionality or data by checking to see if the security token contains the *SwornLawEnforcementOfficerIndicator* with a value of true. Similarly, if CISS is requested to return criminal history data to a user, it will check to see if the user has a claim that states they have *View Criminal History Data privileges* before providing that data to the user.

What's the benefit? A key advantage of using GFIPM's standard for security within CISS, is that Connecticut will be able to link to and share information with other local, state, and federal CJI jurisdictions without changing anything in CISS or in any local business processes. Through memoranda of understanding (MOUs), the CISS Identity Provider could be trusted by Federations such as the CJIS Federation, and CISS users would have access to CJIS tools such as the N-DEx portal. This is because both N-DEx and CISS are making access decisions based on a standard language that defines security claims (GFIPM).

Q What is the difference between *Claim-Based* and *Role-Based* Authorization?

Role-based security has been the norm for securing information from unauthorized users for a long time and works well when controls are based on job (and therefore system process) specifications; someone needs access only to the record types and data elements needed to perform their job.

Role-based security maps jobs to system processes based on business processes and a user's related responsibilities. Roles are created to mirror the business process and are not easily transferred to another system. An issue with role-based security is apparent when multiple organizations try to share information. Since there isn't a standard vocabulary definition for roles, we can't securely make access decisions based on a person's role. For example, an *analyst* role in one organization may have different privileges than an analyst in another organization.

Between multiple agencies with separate systems, roles are often broadly defined and lack common definition (e.g., analyst); making a security solution problematic, if such a solution is to be applied to users from multiple agencies, multiple states, and federal agencies.

This is where *claims-based* security comes in because *claims* are more fine-grained than *roles*, allowing multiple organizations to agree on the meaning of a claim. GFIPM defines a common vocabulary of claims for the criminal justice and law enforcement communities. A claim is a stated fact about a user. Instead of defining a person as an *analyst*, you would claim that the person has the *privilege* to search criminal history and/or criminal intelligence data. A claim provides a person with a specific clearance level, a specific certification, or a specific privilege.

What's the benefit? Claims are fine-grained enough that different organizations know exactly what a claim means. If we can understand each other's security information, then we can trust each other's users through claims-based security. CISS is required to provide federated security, since users from all of the agencies from across the State will be using the system. Given that it is impractical, and insecure, to manage all users centrally, a federated security model is recommended. Agencies will maintain their own user accounts, as well as maintain the access privileges (security claims) for their own users. Using GFIPM allows the CISS to have a common vocabulary of security claims for all users across all agencies. ■

For more info: http://www.gfipm.net
http://msdn.microsoft.com/en-us/library/ee536164
http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1179

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