



**Quarterly Program Status Report  
to the  
Criminal Justice Information System (CJIS)  
Governing Board**

**April 17, 2014**

---

**Connecticut Information Sharing System (CISS)  
Connecticut Impaired Driver Records Information System (CIDRIS)  
Offender Based Tracking System (OBTS)  
Connecticut Racial Profiling Prohibition (CTRP3)**



## Table of Contents

Criminal Justice Information System (CJIS) Governing Board .....	5
Report to the Governing Board .....	7
Executive Summary.....	8
Budget.....	11
Recommendations from the Office of the Attorney General and the Auditors of Public Accountants	12
Connecticut Information Sharing System (CISS) Detailed Status Report .....	15
Offender Based Tracking System (OBTS) Status Report .....	21
Connecticut Impaired Driver Records Information System (CIDRIS) Status Report .....	22
CJIS Programs – Recommendations for Consideration.....	23
Connecticut Racial Profiling Prohibition Status Report .....	25
Appendix A –Commonly Used Acronyms .....	26



## Criminal Justice Information System (CJIS) Governing Board

---

### Agencies and Members

#### Office of Policy and Management

**Mike Lawlor, Under Secretary**

*Governor's Appointee and Co-Chair*

Benjamin Barnes, Secretary

#### Department of Administrative Services

**Donald DeFronzo, Commissioner**

Mark Raymond, CIO, DAS-BEST (Designee)

#### Office of the Chief State's Attorney

**Kevin Kane, Esq., Chief State's Attorney**

John Russotto, Esq., Deputy Chief State's Attorney (Designee)

#### Department of Correction

**James Dzurenda, Commissioner**

Cheryl Cepelak, Deputy Commissioner, (Designee)

#### Department of Motor Vehicles

**Melody Currey, Commissioner**

George White, Division Chief (Designee)

#### Court Administration and Operations

**Judge Patrick L. Carroll, III**

**Chief Court Administrator, Co-Chair**

#### Board of Pardons and Paroles

**Erika Tindill, Esq., Chairperson**

John DeFeo, Executive Director (Designee)

#### Connecticut Police Chiefs Association

**Richard C. Mulhall, Chief (Designee)**

James Cetran, Chief (Designee)

#### Department of Emergency Services and Public Protection

**Dora Schriro, Commissioner**

Brenda Bergeron, Chief of Staff (Designee)

#### Division of Public Defender Services

**Susan O. Storey, Esq., Chief Public Defender**

Brian Carlow, Esq., Deputy Chief Public Defender (Designee)

#### Office of Victim Advocate

**Garvin G. Ambrose, Esq., State Victim Advocate**

Hakima Bey-Coon, Esq., Staff Attorney (Designee)

---

### Chairpersons and Ranking Members of the Joint Standing Committee of the General Assembly on Judiciary

**Eric D. Coleman, Senator, Co-Chair**  
*(Designee TBD)*

**John A. Kissel, Senator,**  
*Ranking Member*

**Rosa C. Rebimbas Representative,**  
*Ranking Member*

**Joe Verrengia, Representative**  
*(Designee for) Gerald M. Fox,*  
*Representative, Co-Chair*

### CJIS Committee Chairs

#### Administrative Committee

Larry D'Orsi  
*Deputy Director, Criminal Matters*  
*Court Operations Division*

#### Implementation Committee

Chief Richard Mulhall  
*Connecticut Police Chiefs Association*

#### Technology Committee

Evelyn Godbout  
*Information Technology Manager*  
*Division of Criminal Justice*



## Report to the Governing Board

---

### Criminal Justice Information System (CJIS)

This report is pursuant to Connecticut General Statute (CGS), 54-142q. The Criminal Justice Information System (CJIS) Governing Board provides this report and directs the projects within this report in order to meet the CJIS Goals.

### Organization of the CJIS Governing Board

As stated in CGS, Section 54-142q, the CJIS Governing Board shall be composed of the Chief Court Administrator, the Commissioner of Public Safety, the Commissioner of Emergency Management and Homeland Security, the Secretary of the Office of Policy and Management, the Commissioner of Correction, the chairperson of the Board of Pardons and Paroles, the Chief State's Attorney, the Chief Public Defender, the Chief Information Officer of the Department of Information Technology, the Victim Advocate, the Commissioner of Motor Vehicles, the chairpersons and ranking members of the joint standing committee of the General Assembly on judiciary and the president of the Connecticut Police Chiefs Association.

CGS, Section 54-142q, expanded the membership of the CJIS Governing Board. In summary, co- chairs were established and the membership was expanded to include representation from the Legislative Branch through the chairpersons and ranking members of the Joint Standing Committee of the General Assembly on Judiciary. Each member of the CJIS Governing Board may appoint a designee.

The legislation specifies the Chief Court Administrator and a person appointed from the CJIS Governing Board membership by the Governor to be co-chairs. The co-chair appointments were immediately made to facilitate the further organization of the CJIS Governing Board. The Chief Court Administrator, Judge Patrick L. Carroll III, is one of the co-chairs. The Governor named Mike Lawlor, Under Secretary, as the other co-chair (and designee).

The CJIS portfolio of programs — CISS, CIDRIS, OBTS — all meet the business objective requirements set forth in CGS Section 54-142q.

The technical component of the Connecticut Racial Profiling Prohibition project is a recent addition to the CJIS portfolio of programs.

## Executive Summary

---

### Update on CJIS Projects

The CJIS Technical team continued to work diligently over the last three months to prepare for the deployment of Phase I of the [Connecticut Information System \(CISS\)](#). They installed and configured server software to support virtual server clusters and high availability. To monitor the availability and performance of the CISS servers, the team installed Microsoft System Center's Data Protection Manager (DPM), which provides disk-based and tape-based data protection for CISS application servers, and System Center Operations Management (SCOM) software.

The CJIS Business and Technical teams determined search source requirements for Criminal and Motor Vehicle System (CRMVS), completed design of Search Release 1 features, and downloaded the complete collection of inmate photos into CISS.

In the next few months, upon re-engagement with Xerox, CJIS will develop with stakeholders and Xerox a realistic, workable release plan for Search and Wave releases. CJIS will also confirm deployment, testing, training plans, tasks and responsibilities. Working with Xerox, CJIS will complete requirements and demonstrate prototypes for the SR1 user interface.

CJIS will select the automated Learning Management System (LMS) to be used for CISS' computer-based training (CBT) and begin the design of an automated user approval and training authorization system.

In addition to the current data sources, CJIS will replicate the CRMVS and add visiting histories to the Offender Based Information System (OBIS) replication.

In the coming months, the CJIS Business team will complete the Waves 1, 2 and 3 Workflow requirements with Judicial Branch (JUD), Division of Criminal Justice (DCJ), Division of Public Defender Services (DPDS), Department of Correction (DOC), Board of Pardons and Paroles (BOPP) and Department of Motor Vehicles (DMV).

CJIS will also begin the design stage for Uniform Arrest Report (UAR) and Misdemeanor workflow requirements upon completion of contract amendment.

The CJIS Technology and Business teams completed the [Records Management System \(RMS\)](#) vendor review with Hunt Computer Design, KT International, and TriTech Software Systems on technology guidelines and documentation. They also developed use case scenarios to better understand how incident and arresting events occur at the local police departments and how information obtained by these events are captured by law enforcement record management systems.

The CJIS Technology team is also working to develop a software library to validate Information Exchange submissions. This will add a level of security to Information Exchanges.

The BEST technology team built a modern routed Internet Protocol (IP) data communications network to support CISS Information Exchanges with law enforcement agencies (LEAs). So far, the teams have deployed the network to nineteen LEAs.

Progress is being made on the [Connecticut Racial Profiling Prohibition System](#). The CJIS teams completed work on a Web application for LEAs' data submissions. The process included User Acceptance Testing on the software before it was released into

Production. The program is now being used by LEAs. To support the Help Desk with any technical issues on data submissions, the Operations team wrote Standard Operating Procedures (SOP) for both CJIS and DAS-BEST.

In the next few weeks, CJIS will create a proposal to automate the process of census data gathering, racial statistical analysis, and reporting, and if accepted, implement it.

For the legacy applications that will integrate with CISS, work continues on integration and implementation, which is scheduled for completion at the end of June 2014. CJIS is working on further integrating [OBTS](#) with CISS. With the new platform in place, the OBTS operational team will focus future application maintenance releases on improving performance and data quality. To improve the security of OBTS, users have been migrated to Active Directory from the legacy eDirectory.

## CJIS Critical Issues and Risks

There are critical issues and risks that will need to be addressed in order for the CISS project to move forward effectively and in a timely manner. Some of these concerns are reflected in the [Office of the Attorney General and the Auditors of Public Accounts report](#) that was released in November (we have listed their recommendations and our mitigation strategy later in this document). This report cited the need for greater transparency and Governing Board participation. The majority of the recommendations are completed or in progress.

Another issue involves the risk of [using consultants for the critical technical positions](#). As pointed out by MTG Consulting, our Independent Validation and Verification consultant, not having experienced state employees working on the CISS project pose significant risk to the success of the project. For CJIS, the late hiring of state positions with temporary contractors presents risk to the project plan and the long-term support and stability of CISS. The risk is that consultants with skills and project knowledge will leave after a short time, taking that knowledge with them. The CJIS Governing Board will have to consider other alternatives such as; 1) hiring consultants, 2) outsourcing the application maintenance to a vendor, or 3) creating a hybrid environment where we have state employees and consultants filling the required positions.

[Funding for the state staffing for the CISS project](#) might be in jeopardy. While the funding today comes from the inmate phone revenue, this revenue source is under discussion for changes by the FCC. Recent rulings have removed the ability to derive revenue from interstate calls. A change to how interstate calls are handled would have a significant impact to the funding of the program. This source of funding reduction will have a substantial impact on the staffing levels. The legislature needs to consider the above risk and provide for an alternate source of general fund monies if this becomes a reality.

[Service Level Agreements \(SLAs\) must be established between CJIS, DAS-BEST and stakeholder agencies](#). SLAs are created to define services to be provided, response times, resources required, and cost of service. They provide transparency and accountability to the agencies signing the agreement. The legislature should encourage agency use of SLAs as a best practices method of standardizing IT application performance requirements and results-based accountability.

## Project Risks

There are several risks that can significantly affect the progress of the CISS project. Two of these risks, the CJIS Security Policy and the Xerox contract amendment, have caused significant delays to the CISS project. Another concern that involves some

stakeholder resource constraint could result in delays due to scheduling.

The **first risk** concerns the [CJIS Security Policy and the use of FBI data](#). The security risks raised by the Department of Emergency Services & Public Protection (DESPP) include the definition of what constitutes FBI data, and whether CISS will be able to receive, transmit, or store FBI data. The CJIS Governing Board is researching Management Control Agreements (MCAs) that other states are using. The MCA is an FBI document that details the relationship between the National Crime Information Center (NCIC) system and the user (CJIS Governing Board). It sets priorities, enforces the selection, supervision, and termination of personnel, and enforces policy governing network systems used to transmit and store criminal justice information.

To alleviate this risk, members of the Governing Board are working with Darryl Hayes of the Department of Emergency Services & Public Protection (DESPP) to construct an MCA that both the CJIS Governing Board and the FBI can agree on.

The **second risk** is the [Xerox contract](#). The contracted vendor, Xerox, and the state met and began discussions to amend the original contract due to changes to project deliverables and project delays. Since contract change negotiations between the state and Xerox remain incomplete, Xerox's significant reduction in staff has almost halted the progress in the completion of the four technical platforms where CISS will reside. It has also considerably slowed the development of the Search Releases and Information Exchanges. As a result, the project timeline and scope has changed and the agreed upon schedule with Xerox that was reported in the July 2013 Legislative report is no longer valid.

The Office of Policy and Management (OPM), the Governing Board co-chairs and the CJIS Executive Director are working with Xerox to finalize a new contract agreement.

A **third risk**, [scheduling with stakeholders](#), could also promote further delays as the CISS project moves forward. Some stakeholder agencies are concerned about meeting time frames set by CJIS for CISS implementation. These concerns stem from the lack of agency resources to provide Subject Matter Experts (SMEs) for CISS and conflicts with seasonal agency work and the CISS schedule.

To mitigate this risk, CISS has assembled a team that will work with each agency to address their concerns individually. This includes bringing in resources to help with the integration, potentially providing financial assistance on a case-by-case basis, and using a governance process to help resolve issues.

## Bond Fund Overview (as of 3/31/2014)

The [budget for the CISS project](#) is on target. The approved funding for the CISS project is \$24,090,000 (this includes \$700K from the General Fund). Of this, the funding received to date is \$20,420,000, the funding expended is \$15,141,799, and the funding available is \$8,948,201. Funding mentioned above does not include operational funding from 2012 to 2015.

## Budget

### Bond Fund Overview as of 3/31/2014

Expenditures	January	February	March	Planned for Quarter	Total PE Through 3/31/14	Total PPE Through 3/31/14
<b>Staff*</b>	\$112,257	\$207,209	\$127,922	\$946,469	\$5,435,256	\$ 6,759,375
<b>IT Hardware</b>	\$23,744	-	-	\$72,500	\$734,218	\$2,300,000
<b>IT Software</b>	-	-	-	\$214,750	\$5,100,158	\$12,970,250
<b>Development</b>	\$59,257	\$28,963	\$1,807	\$101,625	\$1,812,446	\$3,660,875
<b>IT Hardware/Software Maintenance</b>	\$97,170	\$102,932	-	\$230,500	\$2,059,721	\$5,884,500
<b>Project Totals</b>	<b>\$292,428</b>	<b>\$339,104</b>	<b>\$129,729</b>	<b>\$1,565,844</b>	<b>\$15,141,799**</b>	<b>\$31,575,000***</b>

\* OPM State Employees and Consultant Services (excluding ACS/Xerox)

\*\* Operational funding not yet received:

FY 2012 \$2.15M, FY 2013 \$3.15M, FY 2014 \$3.75M, FY 2015 \$3.85M

\*\*\* This is based on original budget developed by MTG Management Consultants

PPE = Planned Project Expenditures

PE = Project Expenditures

## Recommendations from the Office of the Attorney General and the Auditors of Public Accountants

In response to a complaint filed pursuant to Connecticut General Statutes § 4-61dd, the Office of the Attorney General and the Auditors of Public Accounts have conducted an investigation of certain issues raised regarding the planning, construction, costs, and oversight of the Criminal Justice Information System (CJIS).

The following is a list of nine recommendations outlined in the Office of the Attorney General and the Auditors of Public Accounts Report (pages 4-6) dated November 20, 2013 and the plan of action agreed upon by the Governance Committee.

Open Date	Action Item Description	Mitigation	Target Completion
11/26/2013	<p><b>AG Recommendation #1:</b></p> <p>Assess whether, due to complexity and time demands of the project, Board members should appoint designees with the available time and experience necessary to ensure the Board is fulfilling its statutory responsibilities. (See Connecticut General Statutes 54-142q(f)(2), requiring establishment of an Executive Committee staff with criminal justice agency and/or non-criminal justice agency personnel with the requisite technical and operational experience).</p>	<p>1/24/14: The Governance Committee satisfies this recommendation.</p>	Completed
11/26/2013	<p><b>AG Recommendation #2:</b></p> <p>Direct the CJIS Executive Director to communicate all significant issues, both positive and negative, to the Board in a comprehensive, easily understood and timely manner, including by providing the Board with complete copies of all past and future Quarterly Risk Assessment Detail reports issued by MTG.</p>	<ol style="list-style-type: none"> <li>1. All IV&amp;V reports have been sent to Board members.</li> <li>2. Include CISS plain language description from Working Group on all future reports and presentations.</li> <li>3. Provide update on major changes to the CISS project to the Board.</li> </ol>	Completed

Open Date	Action Item Description	Mitigation	Target Completion
11/26/2013	<p><b>AG Recommendation #3:</b></p> <p>Direct the Executive Director to report the status and timeline for completion of the contract discussions with Xerox, including the status of any revised work plan, the timeline of deliverables and the status of payment issues. Representatives from Xerox should participate in such a presentation.</p>	<p>A Special Board meeting will be scheduled to finalize the agreement. Karen Buffkin will provide insight to the Board.</p>	TBD
11/26/2013	<p><b>AG Recommendation #4:</b></p> <p>Direct the Executive Director to provide a detailed briefing on the current budget and timeline of the project, to include an explanation for any differences between the current work plan, budget and projected timeline with the original work plan, budget and project timeline.</p>	<p>At the regularly scheduled Board meeting, provide projected budget and project timeline (and possible project plan if agreement reached with Xerox.)</p>	Completed
11/26/2013	<p><b>AG Recommendation #5:</b></p> <p>Review information developed through the contract status report and/or budget and timeline briefing in order to determine whether corrections or clarifications should be made to the July 2013 Report to the legislature and, if so, provide any necessary corrections.</p>	<p>Update the Legislative report with a copy of the FBI letter and the project plan section and send to the Board for their approval, then to the AG's office.</p>	Completed
11/26/2013	<p><b>AG Recommendation #6:</b></p> <p>Address and resolve all payment issues with Xerox.</p>	In progress.	In progress
11/26/2013	<p><b>AG Recommendation #7:</b></p> <p>Consider implementing frequent quality assurance reviews.</p>	<p>Holding monthly meetings between Sean Thakkar, CISS project manager(s) and Bob Kaelin (MTG).</p>	Completed

Open Date	Action Item Description	Mitigation	Target Completion
11/26/2013	<p><b>AG Recommendation #8:</b>                      Assess the current status of the durational program manager and, if necessary, engage in a search for a permanent CISS program manager with a strong IT background and the ability to effectively communicate and collaborate with the stakeholders, consultants, and contractors. Such an individual should possess a practical understanding of the criminal justice process, including how a matter develops in the criminal justice system and how documents are developed and used by the various criminal justice agencies.</p>	<ol style="list-style-type: none"> <li>1. Potential candidates are being reviewed. The following is the three step process for hiring the next CISS project manager:</li> <li>2. Interview with Sean Thakkar, Mark Raymond (DAS-BEST)</li> <li>3. Interview with Mike Lawlor, Judge Carroll and Karen Buffkin</li> <li>4. Interview with key Board members - Kevin Kane (DCJ), Chief Mulhall (CPCA) and Dr. Dora Schriro (DESPP)</li> </ol>	In progress
11/26/2013	<p><b>AG Recommendation #9:</b>                      Evaluate whether changes, including the addition of personnel, are necessary in the CJIS Leadership and CSG.</p>	This issue has been addressed due to changes already made and more that are forthcoming.	Completed

## Connecticut Information Sharing System (CISS) Detailed Status Report

---

### CISS — Background

The Connecticut Information Sharing System (CISS) is a comprehensive, state-wide criminal justice information technology system that provides the ability to electronically share offender information within the state's criminal justice community.

CISS will provide two major measurable outcomes:

1. The quick, reliable and secure dissemination of event-based information from system-to-system (source to targets), with CISS collecting and delivering the exchanges from and to the edge – the “on-ramp” and “off-ramp” analogy.
2. An enterprise search process that allows a user to quickly find information about a person, event, location or property without needing to know where the information is stored or how it is organized, linking that entity information in the background so that users can quickly jump from (for example) a person view to a location view based on one of the addresses shown for that person. The key here is that a user does not need to know anything about the source systems;

Underpinning the two major visible outcomes is a full federal-level security solution that will secure information to authorized “eyes” only and allow Connecticut to later share information from CISS with federal, state and regional CJIS consortia that use the same security approach for user authentication and authorization. It will also provide a verbose logging and auditing solution that records *every* user and system transaction from log-in to log-out. CISS users would be able to connect to federal and extra-state information sources that use the same security model.

### CISS Key Accomplishments – Period Ending March 31, 2014

#### CISS Wave 0, Version 1.6

- Organized training requirements with Xerox.
- Installed Microsoft System Center's DPM, which provides disk-based and tape-based data protection for CISS application servers, and SCOM software to monitor the performance and availability of the CISS servers.
- Replicated OBTS into the System Test environment as a data source. CJIS can now test OBTS as a data source in CISS.
- The CJIS Technical team executed the initial performance benchmark for infrastructure and external information sources. Having a benchmark helps to measure the performance against industry standards.
- Drafted Standard Operating Procedures (SOP) for CJIS Operations Management.
- CJIS and DAS-BEST technology teams met with Microsoft and F5 Networks technology subject matter experts to design support of a new application networking technology. Use of F5 networks technology will benefit the CISS application by providing additional redundancy, security and performance enhancing technology. Planning discussions to support off-site data storage options were also conducted with BEST.
- Completed installation of twenty network devices in CJIS and municipalities in preparation for CISS Search software. The newer equipment will facilitate the

integration of CISS with the RMS systems in local LEAs.

- Installed and configured server software to support virtual server clusters and high availability. These servers will support a high volume of traffic on CISS.
- Installed additional disk drives, increasing available storage for the User Acceptance Testing (UAT) and Production environments.

### **CISS Waves 1 - 3**

- Gathered business requirements for Uniform Arrest Report, Misdemeanor Summons and Infractions workflows. The scope of these requirements includes electronic submission of incident arrest information by law enforcement systems, information storage and user access using document management functionality and transmission of this information to state agencies to allow stakeholder consumption. The requirements covered several project objectives including the confirmation of arresting data elements and associated documentation packets, notification and messaging, and agency data transformation using national information exchange standards.
- Conducted CJIS Community discussions to review GFIPM claims process (GFIPM 101) and an Introduction to CISS Architecture (CISS 101). Informational discussions help to educate the stakeholders on how CISS works.

### **CISS Search Release 1 and 2 (SR1, SR2)**

- Completed design of SR1 features, such as System Administration and Alerts and Notifications.
- The Paperless Re-Arrest Warrant Network (PRAWN) design is completed (CISS will display only active warrants). Working with the Department of Correction (DOC) and DAS-BEST, CJIS downloaded nearly two million inmate photographs into CISS (SR1). The photographs will provide another level of identity when searching for incarcerated persons.
- Determined search source requirements for CRMVS (SR2).

## **CISS Anticipated Activities – Next 90 Days**

### **CISS Wave 0, Version 1.6**

- Continue to document technical operating procedures that will aid in support of CISS.
- Continue work on release plans to support the new CISS applications.

### **CISS Wave 1 - 3**

- Complete the Waves 1, 2 and 3 Workflow requirements with Judicial Branch, Division of Criminal Justice (DCJ), Division of Public Defender Services (DPDS), DOC, Board of Pardons and Paroles (BOPP) and Department of Motor Vehicles (DMV).
- Start the design stage for Uniform Arrest Report (UAR) and Misdemeanor workflow requirements upon completion of contract amendment. This includes technical discussions to collect and review (I-Zone) data transformation requirements for CISS Information Exchanges using agency code values.

### **CISS Search Releases 1 and 2 (SR1, SR2)**

- Develop with stakeholders and Xerox a realistic, workable release plan for Search

and Wave releases.

- Upon re-engagement with Xerox, confirm deployment, testing, and training plans, tasks and responsibilities.
- Replicate CRMVS. This will allow CJIS to use the data as a source for Information Exchanges without putting a load on the real time system.
- Working with Xerox, complete requirements (for layout and for incorporating stakeholder requirements into features) for the SR1 user interface. This will provide a user friendly interface for Search Release 1.
- Add visiting histories to the OBIS replica. CISS can provide details on people who have visited those who are incarcerated.
- Select the automated Learning Management System to be used for CISS' computer-based training (CBT). This will provide an online training system for CISS users.
- Upon resolution of the CJIS Security Policy, begin with stakeholders the design of an automated user approval and training authorization system. Users will have the ability to test CISS and provide feedback on the application and help to design an effective training system for authorizing the primary administrator who will authorize users.
- Following re-engagement with Xerox, develop and demonstrate to stakeholders prototypes for law enforcement and state agency portals and the user interface.

## RMS Certification

### RMS Certification — Background

Records Management System (RMS) Certification is a collection of guidelines and processes intended to ensure LEAs can efficiently and effectively exchange criminal justice information between their RMS systems and CISS.

### Key Accomplishments – Period Ending March 2014

- Completed RMS vendor review with Hunt Computer Design, KT International, and TriTech Software Systems on technology guidelines and documentation. CJIS developed use case scenarios to better understand how incident and arresting events occur at the local police departments and how information obtained by these events are captured by law enforcement record management systems. The objective of this exercise is to document how data and paperwork are collected, organized, and reported by the local law enforcement officers.

### Anticipated Activities – Next 180 Days

- The business and technology teams plan to continue to review and implement certification package with pilot participants, including work to document requirements to support the National Information Exchange Model (NIEM) and Information Exchange Package Documentation (IEPDs) standards used to send and receive incident arrest information between RMS and CISS.
- The technology team is also working to develop a software library to validate Information Exchange submissions. The library of software, referred to as an “API” can also be used by vendors to develop software that is compliant with the new state standards. The API is expected to help reduce complexity of writing custom software and vendor software development efforts.
- On April 30<sup>th</sup>, a working group will review the certification business requirements.

## **RMS Network**

### **Key Accomplishments – Period Ending March 2014**

- Over the past three months, CJIS and BEST technology teams built a modern routed Internet Protocol (IP) data communications network to support CISS Information Exchanges with LEAs. As a benefit to the community, this new network supports a high-speed data transmission using selectable committed information rates, FBI compliant data encryption and quality of services. This advanced enterprise level network functionality benefits the CJIS community by providing a reliable and secure data communications and network transport. To date, nineteen towns have been deployed on the new network.
- Submitted a deployment plan to PSDN Applications Review Board and garnered approval. The plan provides details for network connectivity between the CISS application and the LEAs' RMSs.

### **Anticipated Activities – Next 180 Days**

- Confirm installation schedule for the remaining towns participating in the CJIS RMS Network. A project charter and memorandum of understanding are also being developed to affirm participant data sharing and operational obligations.

## CISS Program Issues and Risks with Mitigation Strategy

### Risk 1

The uncertainties of whether CISS will be able to receive, transmit, or store “FBI data” and its relationship to the CJIS Security Policy is causing significant delays to the project.

#### Impact

The CISS project is experiencing and will continue to experience significant schedule delays, increased costs and changes in scope. It will also potentially strain relationships with stakeholders and the vendor. These delays have a negative “domino” effect in many other areas of the project.

#### Mitigation

The CJIS Governing Board is developing a Management Control Agreement (MCA), an FBI document. This agreement details the relationship between the National Crime Information Center (NCIC) system and the application users. The MCA will be used to assist CJIS with creating a joint security policy with DESPP to protect key and sensitive FBI information from unauthorized access.

### Risk 2

Stakeholder agencies are concerned about meeting time frames set by CJIS for CISS implementation. These concerns stem from:

- Lack of agency resources to assist with CISS
- Conflicts with seasonal agency work and the CISS schedule

#### Impact

The CISS project will experience significant schedule delays, increased costs, changes in scope, vendor issues and potentially have gaps of critical data that CISS is required to provide to our information consumers.

#### Mitigation

CISS has assembled a team to collaborate with stakeholders composed of a project manager and business and technical leads who will work with each agency to address their concerns individually and find a win-win solution that brings a significant positive net benefit to that agency. This includes bringing in resources to help with the integration, providing financial assistance on a case-by-case basis, and using a governance process to help resolve issues.

### Risk 3

Because contract change negotiations between the state and Xerox remain incomplete, Xerox has significantly reduced its staff. As a result, Xerox is unable to effectively perform the work needed to build, test, and implement CISS.

#### Impact

Xerox’s significant reduction in staff has almost halted the progress in the completion of the four technical platforms where CISS will reside and has considerably slowed the development of the Search Releases and Information Exchanges. As a result, the project timeline and scope has changed. The delay increases the project costs and stakeholders’ confidence in the project is deteriorating.

#### Mitigation

The Office of Policy and Management (OPM), the Governing Board Co-Chairs and the Executive Director are working with Xerox to finalize the contract as soon as possible.

## CISS — Conclusions

In the first quarter of 2014, CJIS continued preparations to support the CISS application. The Technical team worked with DAS-BEST to install and configure server software to support virtual server clusters and high availability. They also installed Microsoft System Center's DPM and SCOM software. On the hardware side, the team worked on the replacement of outdated equipment in CJIS and municipalities. The newer equipment will facilitate the integration of CISS with the RMS systems in local LEAs.

Work is underway on the designs for the SR1 interface. Designs for System Administration, PRAWN, Offender Based Information System (OBIS) and Active Warrants are now complete.

CJIS continues to work with stakeholders to incorporate additional data sources. In March, OBTS was replicated into the System Test environment as a data source. CJIS also downloaded the complete collection of inmate photos into CISS.

To provide reference guides for the support team, the Project Management team wrote SOP documentation. Working with stakeholders, the CJIS Business and Project Management teams held review sessions on GFIPM and CISS Architecture.

The CJIS Business team will complete the Waves 1, 2 and 3 Workflow requirements with Judicial Branch, Division of Criminal Justice (DCJ), Division of Public Defender Services (DPDS), DOC, Board of Pardons and Paroles (BOPP) and Department of Motor Vehicles (DMV) in the coming months.

The CISS Project Management team will work with stakeholders in the next few months to finalize the RMS Certification Guide. The CJIS teams will continue to review the RMS Certification process with the state and local LEAs and vendors. A technology review workshop is planned to assist participating Law enforcement agencies.

Schedules with the security issues brought forth by DESPP involving FBI data and with Xerox contract revisions are still pending. These delays have been incorporated into the CISS schedule.

## Offender Based Tracking System (OBTS) Status Report

The Offender Based Tracking System (OBTS) is an integrated information-sharing system developed with all the state criminal justice agencies to respond to the growing demand for access to comprehensive information on offenders. Officially launched in 2004, OBTS is used daily by local, state, and federal law enforcement as well as other criminal justice agencies.

### OBTS Anticipated Activities – Next 90 Days

Except for functionality that is required to support CISS, no major new functionality will be introduced until the CISS system is placed into a new server environment. New requirements will only be sought to support issues which require immediate attention.

- Continue to work on the OBTS migration to the new infrastructure, scheduled for completion by the end of June 2014. So far, OBTS database migration to the new environment is completed and tested in the Development and System Test software environments. This new infrastructure will reduce cost of ownership for OBTS and is expected to improve performance.
- Continue to update OBTS security based on recommendations from the CJIS Operations team and Sierra. To improve the security of OBTS, users have been migrated to Active Directory from the legacy eDirectory. This has been completed and tested in the development environment.
- Work with DAS to open a Java Developer and a SQL Database Administrator state position as soon as possible in order to obtain a significant degree of knowledge transfer from Sierra before their contract expires in June 2014. From the nineteen positions requested, the Java Developer and the Help Desk Analyst positions are in the final stage of funding approval.

<b>Issue</b>
The project team is dependent on access to, and cooperation of, subject matter experts residing in source agencies in order to correct data quality issues coming into OBTS. Due to current workload activities and changing priorities, subject matter experts may not be available when needed.
<b>Impact</b>
The effort to significantly improve the data quality in OBTS will be much slower than required.
<b>Mitigation</b>
Closely monitor work efforts needed from the source agencies for data quality issues. CJIS will communicate data issues in a timely manner so that the source agency can arrange their schedule to promptly correct the data.

### OBTS — Conclusions

CJIS is working to further integrate OBTS with CISS. Database migration to the new environment is complete and tested in the Development and System Test phases. The Operations team will continue to work on security. Two positions to support OBTS, Java Developer and Help Desk Analyst, are in the final stage of approval.

## Connecticut Impaired Driver Records Information System (CIDRIS) Status Report

The Connecticut Impaired Driver Records Information System (CIDRIS) is an integrated information-sharing system designed to automate the collection and delivery of Operating Under the Influence (OUI) information among state criminal justice stakeholders. CIDRIS was developed in cooperation with local law enforcement, the Department of Emergency Services and Public Protection (DESPP), the Department of Motor Vehicles (DMV), the Division of Criminal Justice (DCJ), and the Judicial Branch, as well as the Department of Transportation (DOT) and the National Highway Traffic Safety Administration (NHTSA). Development of CIDRIS was completed in 2010. Interfaces to DESPP, DMV, and Judicial agency source systems were created in 2011. Implementation for roll-out to DESPP troops started in mid-December 2011 and was completed in August 2012.

### CIDRIS Anticipated Activities – Next 90 Days

- CIDRIS is in maintenance and support mode only. No new changes are being implemented.

### CIDRIS Program Issues and Risks with Mitigation Strategy

Issue
CIDRIS validates all messages received by DESPP, DMV, and Judicial. Messages that have bad or missing data will not pass validation and will be rejected (to prevent passing bad information along to other stakeholders).
Impact
If the quantity of messages rejected by CIDRIS continues to remain at higher than acceptable levels, CJIS stakeholders won't be able to fully leverage system capabilities, such as automatic data entry into agency source systems and continued delivery of paper documents.
Mitigation
To help reduce the OUI submission errors, the CIDRIS team — including DESPP, DMV and Judicial — will continue to be vigilant in isolating and fixing operational and technical problems. Solutions to the spectrum of problems range from additional technical and training resources to developing additional software programs.

### CIDRIS — Conclusions

CIDRIS is in maintenance mode, with no new changes being planned.

## CJIS Programs – Recommendations for Consideration

1. Compared to 2012, the workload for CISS has increased exponentially in 2013. During this build out of technical, business, and process systems with the CJIS community, a great deal of institutional knowledge is created. Given that most of the CJIS staff is currently consultants, we recommend that the state open nineteen state employee positions which are critical and required for the current needs of the CJIS operational team working on CISS, OBTS, CIDRIS, and other CJIS projects. These positions require the right skills and experience in order to successfully deliver a large, complex, high-visibility project like CISS.

**Impact:** To ensure success, it is essential to have a talented pool of dedicated and skilled CJIS employees that can lead and support the CISS project. The majority of the CJIS team is made up of consultants with short term contracts. Over the course of the project, some of those talented consultants have left CJIS when their contracts came up for renewal, taking invaluable knowledge with them. Currently, only the CJIS Executive Director, CJIS Program Manager, CJIS Business Manager, Durational Project Manager, and the CCT Fiscal Administrator are full-time state employees. If nineteen people are not hired during the second or third quarter of 2014, much more of the accumulated knowledge during the build of CISS will be lost.

These nineteen CJIS project positions are considered critical to the project. Hiring these consultants as state employees would better secure the accumulated knowledge of the CISS project, not only for the technical and business development, but also for the support of Operations of the project. MTG, the consulting company hired to do the Independent Verification & Validation (IV&V), has repeatedly highlighted this as a critical CISS risk.

**Recommendation:** After CJIS met with DAS, DAS-BEST and OPM, there was an agreement to open all remaining nineteen positions. We have ranked the order of hiring needed and we are working to open these positions. Most of the requested start dates are in the first quarter of 2014. Two positions of the nineteen are expected to be posted in the near future.

The CJIS Governing Board will have to consider other alternatives such as; 1) hiring consultants, 2) outsourcing the application maintenance to a vendor, or 3) creating a hybrid environment where we have state employees and consultants filling the required positions.

We need to hire people who have the right skill set and experience with large, complex, multi-million dollar, multi-year projects. We also need to offer salaries close to market rates in order to be successful. The following ranked nineteen positions need to be approved as full-time state employees as soon as possible:

Order of Hiring Needed	Position Name	Needed Start Date
1	Help Desk Manager	1/12/14
2	Lead Senior .NET & Java Developer (1 of 2 positions)	2/17/14
3	Senior Microsoft Certified System Engineer (MCSE) Administrator	2/17/14
4	Senior SQL Database Administrator (DBA) (1 of 2 positions)	2/17/14
5	CISS Application Trainer/Help Desk Support	2/17/14
6	Enterprise Architect	2/17/14
7	Senior SharePoint Developer (1 of 2 positions)	2/17/14
8	Business Analyst (1 of 2 positions)	2/17/14
9	Business Analyst (2 of 2 positions)	2/17/14

10	Senior Project Manager	2/17/14
11	Senior Test Lead	2/17/14
12	Help Desk Analyst (1 of 3 positions)	2/17/14
13	Senior .NET & Java Developer (2 of 2 positions)	2/17/14
14	Communications Specialist	2/17/14
15	Senior SQL Database Administrator (DBA) (2 of 2 positions)	6/16/14
16	Technical Business Analyst	6/16/14
17	Help Desk Analyst (2 of 3 positions)	10/20/14
18	Help Desk Analyst (3 of 3 positions)	10/20/14
19	Senior SharePoint Developer (2 of 2 positions)	11/03/14

**2. The funding for hiring CJIS state staff is at risk. Recent rulings have removed the ability to derive revenue from interstate calls, which currently funds CJIS state staff. This revenue source is under discussion for changes by the FCC.**

**Impact:** A change to how interstate calls are handled would be significant to the program and will have a substantial negative impact on the staffing levels.

**Recommendation:** The legislature needs to consider the above risk and provide for an alternate source of general fund monies if this becomes a reality.

**3. Service Level Agreements (SLAs) must be established between CJIS, DAS-BEST and stakeholder agencies.**

**Impact:** SLAs are an industry best practice. SLAs are created to define services to be provided, response times, resources required, and cost of service. They provide transparency and accountability to the agencies signing the agreement, and help reduce cost by reducing redundancy and waste. An SLA should be established between CJIS and DAS-BEST. CJIS must know what services and resources DAS-BEST will provide as well as the timelines for providing them. The items for SLAs include service availability, disaster recovery, and quarterly resources for planned activities. The provisioning of services using SLAs should be encouraged by the Legislature to allow agencies to evaluate their service levels and reduce costs.

**Recommendation:** The Legislature should encourage agency use of SLAs as a best practices method of standardizing IT application performance requirements and results-based accountability. CJIS delivered a draft SLA to DAS-BEST in December 2012 for review and negotiation in order to implement the first SLA.

**Update -** As the CISS infrastructure build out is completed, CJIS will update the draft SLA and continue the discussion with DAS-BEST, at which time both parties will finalize an agreement.

## Connecticut Racial Profiling Prohibition Status Report

---

Connecticut Racial Profiling Prohibition Project (CTRP3), the Institute for Municipal and Regional Policy at Central CT State University (IMRP), in consultation with the Office of Policy and Management (OPM), has established a Racial Profiling Prohibition Advisory Board to help oversee the design, evaluation, and management of the racial profiling study mandated by P.A. 12-74 “An Act Concerning Traffic Stop Information.” The IMRP will work with the Advisory Board and all appropriate parties to enhance the collection and analysis of traffic stop data in Connecticut.

CJIS is working with Ken Barone, Policy & Research Specialist at the Institute for Municipal and Regional Policy (IMRP), and Jim Fazzalano, Project Manager, at Central Connecticut State University (CCSU) to design, build, test and implement the technical infrastructure, Web application and help desk support required for this project.

### Key Accomplishments – Period Ending March 2014

- Gathered requirements, designed, built and tested Web application for Law enforcement agencies’ data submissions. This will be the Web interface for the LEAs for Racial Profiling.
- Completed User Acceptance Testing. This is testing done by those who will be using the software to ensure that it works as intended. Once they find the software acceptable, it goes into Production.
- Introduced the Racial Profiling Prohibition Web application into Production. The program is now released to all LEAs.
- Finalized the help desk Standard Operating Procedures (SOP) within CJIS and DAS-BEST to support any reported technical issues with submission of data.

### Connecticut Racial Profiling Prohibition Anticipated Activities – Next 90 Days

- Create recurring reports on a monthly basis and send them automatically to CCSU and law enforcement.
- Establish any connectivity needed by CCSU for data access and analysis.
- Complete a proposal to automate the process of census data gathering, racial statistical analysis, and reporting. CCSU needs this information to compare the traffic stop data to the 2011 census benchmarks.
- Plan support and maintenance for the next fiscal year with CCSU.

### Connecticut Racial Profiling — Conclusions

The CJIS technical development and support teams will continue to work with Ken Barrone, Jim Fazzalano, and CCSU to meet the needs and goals of the of the Racial Profiling project.



## Appendix A –Commonly Used Acronyms

---

AFIS = Automated Fingerprint Identification System  
BEST = Bureau of Enterprise Systems and Technology  
BOPP= Board of Pardons and Paroles  
CAD = Computer Aided Dispatch CCH= CT 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 & Planning Div.  
CMIS = Case Management Information System (CSSD)  
COLLECT = CT On-Line Law Enforcement Communications Teleprocessing network  
CPCA = CT 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  
DMV = Dept. of Motor Vehicles  
DOC = Department of Correction  
DPDS = Div. of Public Defender Services  
IST = Infrastructure Support Team  
JMI = Jail Management System JUD = Judicial Branch  
LEA = Law Enforcement Agency  
LIMS = Laboratory Investigative Mgmt. System  
MNI = Master Name Index (DESPP)

OBIS = Offender Based Information System (Corrections)  
OBTS = Offender Based Tracking System  
OCPD = Office of Chief Public Defender  
OVA= Office of the Victim Advocate  
OVS = Office of Victim Services  
RMS = Records Management System  
OSET = Office of Statewide Emergency Telecommunications  
POR = Protection Order Registry (Judicial)  
PRAWN = Paperless Re-Arrest Warrant Network (Judicial)  
PSDN = Public Safety Data Network  
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 Report

### Technology Related

ADFS = Active Directory Federation Services  
COTS = Commercial Off The Shelf (e.g., software)  
ETL = Extraction, Transformation, and Load  
FIM = Forefront Identity Manager (Microsoft)  
GFIPM = Global Federated Identity & Privilege Mgmt.  
IEPD = Information Exchange Package Document  
LAN = Local Area Network  
NAS = Network Attached Storage  
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