Report on the Status of the
Criminal Justice Information System (CJIS)

to the

Connecticut Legislature

Submitted by
the CJIS Governing Board

January 1, 2013

Table of Contents

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 Correction,
**   with Parole Functions**
Leo C. Arnone, Commissioner
Cheryl Cepelak, Deputy Commissioner,
(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 Emergency Services
**   and Public Protection**
Reuben F. Bradford, Commissioner
Steven Spellman (Designee)

Office of Chief Public Defender Services
Susan O. Storey, Esq.
Chief Public Defender
Brian Carlow, Esq.
Deputy Chief Public Defender (Designee)

Office of Chief Court Administrator
Judge Patrick L. Carroll, III
Deputy Chief Court Administrator,
Designee and Co-Chair
Barbara M. Quinn, Judge, Chief Court
Administrator

Department of Administrative Services
Donald DeFronzo, Commissioner
Mark Raymond, CIO, DAS-BEST (Designee)

Board of Pardons and Paroles
Erika Tindill, Chair
John De Feo, Executive Director (Designee)

Office of Victim Advocate
Michelle Cruz, Victim Advocate
Merit LaJoie, Complaint Officer (Designee)

Connecticut Police Chiefs Association
Richard C. Mulhall, Chief (Designee)
James Cetran, Chief (Designee)

Department of Motor Vehicles
Melody Currey, Commissioner
George White, Division Chief (Designee)

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

Michael Pollard
(Designee for) Eric D. Coleman,
Senator, Co-Chair

William Tong, Representative
(Designee for) Gerald M. Fox,
Representative, Co-Chair

John A. Kissel, *Senator, Ranking Member*

John Hetherington
Representative, Ranking Member

CJIS Committee Chairs

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

Implementation Committee
Chief Richard Mulhall
Connecticut Police Chiefs Association (CPCA)

Technology Committee
Evelyn Godbout
Information Technology Manager
Division of Criminal Justice

Executive Summary

Sean Thakkar, Executive Director

Governor's Vision for Technology

The Governor's vision for technology provides the foundation upon which CJIS works. This vision is predicated on the following:

- Implementation of <u>efficient, modern business processes</u> that result in cost-effective delivery of services.

- <u>Open and transparent engagement</u> with the citizens of the State.

- <u>Accurate and timely data</u> for policy making, service delivery and results evaluation.

- <u>A secure and cost effective IT infrastructure</u>, including greater use of shared services and applications wherever possible.

- <u>Easily accessible services</u> to all constituents.

CJIS Business Goals and Objectives

- **Efficiency** — Optimize our current investments in technology and leverage existing infrastructure and resources.

- **Flexibility** — "Information any way you want it" — Provide all of our stakeholders with the data they need, on the platform they prefer, and in the most accessible format to suit their needs and business practices.

- **Security** — Develop a secure environment which meets state and federal standards for security.

- **Objectivity** — Provide independent and objective opinions and recommendations to the CJIS Governing Board.

- **Continuity** — Provide services that are "boringly predictable" and totally reliable.

- **Simplicity** — Create a simple way to implement new technologies, so that agencies can implement them smoothly.

Criminal Justice Information System (CJIS)

This report is pursuant to Connecticut General Statutes (CGS), Sections 54-142s. 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

CGS, Sections 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 by the Governor from the CJIS Governing Board membership 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 designated Judge Patrick L. Carroll III, Deputy Chief Court Administrator, to be one of the co-chairs. The Governor named Mike Lawlor as the other co-chair (and designee).

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

- ✓ Efficient modern business processes
- ✓ Open and transparent engagement
- ✓ Accurate and timely data for policy making, service delivery and results evaluation
- ✓ A secure and cost effective IT infrastructure
- ✓ Easily accessible services to all constituents
- ✓ Establish funding processes that will allow the State to measure and maximize its return on technology investments and to target funds to the agency and state priorities
- ✓ Ensure that the appropriate project management, transparency, and accountability systems are in place for successful project implementation and completion
- ✓ Better align agency and state information technology plans and priorities with agency and state priority business and resources available
- ✓ Provide for Agency autonomy so they can accomplish their missions
- ✓ Simplify implementation of new technologies
- ✓ Develop secure environment, meeting State and Federal standards
- ✓ Optimize current investments to leverage infrastructure and resources

Accomplishments

The following is a list of major accomplishments since the July 2012 Legislative Report.

Connecticut Information Sharing System (CISS):

- The Technical Architecture Documents to support development, system testing, User Acceptance Testing (UAT), and production environments are complete.

- All CJIS Partner Agencies have chosen a security option for integration with CISS.

- Xerox high-level design documents have been approved for Wave 0 and the overall system.

- The servers, storage, firewalls, switches, and software for CISS were acquired.

- The CISS Team met with the Records Management System (RMS) vendors and their law enforcement counterparts in July to discuss connecting RMS systems to CISS.

- The CJIS Business Team and Xerox conducted Global Federated Identity and Privilege Management (GFIPM) data source mapping sessions for the Judicial, DESPP, and DOC systems that currently send data to OBTS.

- The Xerox and State teams have completed detailed testing and training plans for Wave 0, Version 1.

- UAT was conducted with stakeholders for the CISS Wave 0, Version 1 — CISS Search.

- CISS Help Desk and operations support plans have been developed; a Help Desk Technician was hired in December to assist CISS users.

- CISS technology workshops have been held for agency stakeholders to help them understand certain aspects of how CISS works.

- The first CISS Monthly Status Meeting with stakeholders was held in August 2012; these meetings are now held at the beginning of every month.

- An integrated project schedule has been created showing both Xerox and State activities in the plan.

- CISS hired a testing lead.

Offender Based Tracking System (OBTS):

- The OBTS 7.3 release was deployed with inquiry performance enhancements.

- The third OBTS/CIDRIS/AFIS User Group Meeting was held on August 15.

- Completed the data purity technical review of the OBTS/Judicial systems.

- OBTS Hands-on Certification Classes were held with 28 students; all received their certification.

- The OBTS team has been working with the CISS Team on tasks needed to build OBTS as the first CISS source database.

Connecticut Impaired Driver Record Information System (CIDRIS):

- The CIDRIS team, DMV, DESPP, and Judicial completed deployment of CIDRIS for all State Troops.

- Judicial and DESPP developed a software program to automatically update surety bondsman and insurance data.

- DESPP made several updates to its Computer Aided Dispatch/Records Management System (CAD/RMS) automation to improve data accuracy and verify document attachments.

- DESPP expanded the CIDRIS training program and installed additional technology for CIDRIS support.

- Judicial developed a new web-based CJIS Forms Viewer Tool to access and print CIDRIS document attachments.

CJIS Programs — Recommendations for Consideration

1. **Open the remaining 13 State employee positions requested for the current needs of the CJIS Operational Team working on CISS, OBTS, CIDRIS, and other CJIS projects. The workload for 2013 will increase exponentially over 2012 for CISS. These positions require the right skills and experience in order to successfully deliver a large, complicated, high visibility project like CISS.**

   Impact: The primary element for success is to have a talented pool of dedicated and skilled personnel reporting directly to the Executive Director. If these 13 people are not hired in the first quarter of 2013, the large amount of work needed to complete CISS will likely push the project schedule completion date further into the future.

   The 13 key CISS project positions are considered critical to initial phases of the project. The Board voted to make these positions full-time State employees. This would allow the State to garner institutional knowledge for CISS application and business requirements of the project. Currently, only the CJIS Program Manager and the CJIS Business Manager have been made full-time state employees. The following 13 positions need to be approved as full-time state employees.

   1. Senior Technology Architect (Manager)
   2. Senior Project Manager
   3. Senior Project Manager
   4. Senior Java Developer
   5. Senior Java Developer
   6. Application Data Base Administrator
   7. SharePoint Developer
   8. SharePoint Developer
   9. Senior Test Lead
   10. Senior Information Security Officer
   11. Senior Systems Administrator
   12. Executive Assistant
   13. Senior Communications Specialist

The consultant company hired to do the Independent Verification & Validation (IV&V) has repeatedly highlighted this as a critical CISS risk.

Recommendations: Because the above positions have not been opened as State employee positions, we hired consultants to fulfill our deliverable obligations as per the contract with the CISS vendor. The State needs to re-classify the thirteen positions listed above to allow for the starting experience needed and have the starting salary closer to the market rates.

2. **Service Level Agreements (SLA) must be established with DAS-BEST and stakeholder agencies.**

   Impact: SLAs are an industry best practice. SLAs are created to define services provided, response times, resources required, and cost of service. SLAs provide transparency and accountability to the agencies signing the agreement, and help reduce cost by reducing redundancy and waste. A SLA should be established between the CJIS Governing Board and DAS-BEST. The Governing Board must know what services and resources DAS-BEST will provide as well as the time lines for providing support and resources. The items for SLA include service availability, disaster recovery, and quarterly resources for planned activities. The provisioning of services using SLA agreements 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 SLA agreements as a best practices method of standardizing IT application performance requirements and results based accountability. Update - A draft SLA was delivered to DAS-BEST in December 2012 for review and negotiation in order to implement the first SLA.

3. **CJIS Governing Board should have full access to Public Safety Data Network (PSDN) and Connecticut On-Line Law Enforcement Communications Teleprocessing (COLLECT) network for its applications. This is a prerequisite for successful deployment of CISS.**

   Impact: The CJIS community agreed five years ago that CJIS use of the COLLECT / PSDN system's network is extremely important to the success of the project. The CJIS Governing Board previously approved CJIS' utilization of the COLLECT / PSDN networks controlled by the Department of Emergency Services and Public Protection (DESPP), which transmits secure data from law enforcement throughout the state. The Board understands the sensitive nature of this data and is prepared to provide appropriate oversight of any use of this system.

   Recommendation: Enact legislation to facilitate use of COLLECT / PSDN by the CJIS Governing Board in compliance with federal guidelines, including designation of the CJIS Governing Board as a Law Enforcement Agency for the purpose of accessing such data. Any such designation should include appropriate restrictions and safeguards. Allocate funding for connection and ongoing operations of agency access to the network.

4. **Change CGS 54-142q to encompass all CJIS Governing Board applications exemption from the Freedom of Information Act (FOIA).**

   Impact: The Legislature should exempt programs under the CJIS Governing Board portfolio from the provisions of FOIA as it has for the OBTS application. Like the OBTS application, CIDRIS and the future CISS application collect data from source agencies (Agencies of Record)

to share with criminal justice agencies that have a need for this data. Like OBTS, CIDRIS and CISS are *not* the source of original entry. FOIA requests should be directed to the agency that collected and entered the data initially. The Privacy subcommittee of the Administrative Committee has been reviewing proposals for FOIA legislation and will present its recommendations to the legislature in the near future.

Recommendation: The Legislature should adopt the proposed legislation submitted by the CJIS Governing Board's Administrative Sub-Committee.

5. **CJIS Governing Board should be designated as a Public Safety Agency by change of legislation to CGS 54-142s.**

    Impact: CISS will not be able to receive any information from federal agencies. An example would be the Automated Fingerprint Information System (AFIS) information from DESPP for CISS Wave 1 – Uniform Arrest Record (UAR) Workflow.

    Recommendation: The Legislature should adopt the proposed legislation change that will be submitted by the CJIS Governing Board's Administrative Sub-Committee.

Connecticut Information Sharing System (CISS) Status Report

CISS — Background

A unified information-sharing and delivery system is the key to preventing tragedies like the 2007 home invasion and triple murder in Cheshire.

While the focus of CGS Sec. 54-142q and CISS is to improve public and officer safety, this project will also reap significant dividends in the efficient use of scarce funding. With the smart, innovative application of new technologies, CISS will reduce overall costs through easier access to information, increased efficiencies in process, and less rework of data entry errors. By managing the investment in the development of the system, CJIS will generate a cumulative benefit of $59M after the system goes into full operation.

CISS will increase public and officer safety by providing more and improved information to criminal justice staff on demand. The system will also enhance business efficiency by increasing the speed of electronic information exchange between agencies — all in a safe and secure manner.

CISS will reduce administrative costs by electronically capturing data and documents at their source, cataloging and storing this data in a central repository, where it will be available to all member agencies. This will create an enormous economies of scale compared to each agency having to copy, file, index, and store all data elements.

These capabilities will create great benefit to society by reducing recidivism, aiding re-entry programs, reducing delays in the judicial process, and improving overall public safety for Connecticut's citizens and public safety officers.

CISS Key Accomplishments – Period Ending December 2012

- All CJIS agencies have selected a security option for integration to CISS.

- CJIS has reviewed and approved Xerox high-level design documents for Wave 0 and the overall system. The CISS team has signed off on the detailed design for the system administrator functionality.

- The Technical Architecture Documents to support development, system testing, User Acceptance Testing (UAT), and production environments are complete.

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

- The CISS Team held a meeting with the RMS vendors and their law enforcement counterparts in July to discuss the CISS project. A high-level overview of the background and purpose of the project, along with a technical briefing of the architecture was presented to set the stage for the meeting. Expectations regarding RMS vendor involvement, technical needs, timing, and next steps were discussed. The RMS vendors were asked to share this information with the law enforcement agencies that they work with. Several RMS vendors and law enforcement agencies have expressed interest in assisting with the pilot for the CISS project. The CISS Team is currently working on the technical specifications for the RMS information exchange.

- The business and technical teams will send out RMS vendor certification packages to all of the CAD-RMS vendors when completed.

- Conducted GFIPM data source mapping sessions for the Judicial, DESPP, and DOC systems that currently send data to OBTS to determine field-level security rules that apply to the data elements.

- Screen mock-ups of the CISS application for Wave 0, Version 1 – CISS Search were reviewed with business stakeholders for their feedback, which was incorporated into the designs.

- Provisioning Xerox for planned technologies to facilitate knowledge transfers (WebMethods, Fast, SharePoint, ADFS, FIM).

- The Xerox and State teams developed detailed testing and training plans for Wave 0, Version 1 – CISS Search.

- The CISS Team has developed and held technology workshops for Agency stakeholders.

- Xerox system test plan strategy and test cases were approved for Wave 0, Version 1 – CISS Search.

- State of Connecticut Business Acceptance Test (BAT) plan strategy and test cases were approved for CISS Search Wave 0, Version 1.

- Xerox training material was approved for Wave 0, Version 1 – CISS Search. Xerox conducted three training classes for local law enforcement officers, CJIS and Judicial Branch users and testers for Wave 0, Version 1 – CISS Search.

- The CISS Team performed Business Acceptance Testing (BAT) and coordinated User Acceptance Testing (UAT) of Wave 0, Version 1.

- The CISS Business Team visited the Willard Cybulski Correctional Institute in Enfield and the Hartford Parole Field Office to observe the DOC business processes in November.

- The CISS Team continued to document CISS business rules for upcoming CISS workflow releases.

- The CISS Team has purchased and is installing with the help of DAS-BEST all of the hardware needed for the CISS project. This effort will be completed in January.

- Nastel monitoring software has been implemented to allow health checks for OBTS and CISS on a real time basis.

- The CJIS Governing Board Strategic Plan has been updated.

CISS Anticipated Activities – Next 180 Days

- In January 2013, plan the various waves needed to complete the CISS project with Xerox using the "rolling wave" methodology.

- Begin implementation of Wave 1.5 (install the new platform for CISS).

- Begin implementation of Wave 0, Version 2 (additional Search databases, functionality and add new users).

- Begin implementation of Wave 1 – Uniform Arrest Record (UAR) Workflow.

- Begin implementation of Team Site development for each Agency.

- Continue working with CPCA to determine the priority order of providing the CISS Search application to additional local law enforcement officers.

- Work with stakeholders to determine the priority of and implement modifications and additional functionality for upcoming releases of CISS Search.

- Review and refine the roles and responsibilities of the Agency System Administrator.

- Work with stakeholders to review and refine the CISS workflow order coupled with search order of agency source systems.

- Continue to refine CISS business rules for upcoming CISS Workflow releases.

- Work with the RMS vendors to document the technical requirements needed for RMS UARs and associated paperwork to be sent to CISS for Wave 1 – UAR Workflow.

- Begin implementation of RMS vendor interfaces.

- Complete the change control between the State and the Vendor for items identified as changes to the scope or the contract.

- The CJIS team is developing new policies for CJIS Security and User Access and work. The team will work with the CJIS Governing Board sub-committees to implement them.

- The CJIS Security Policy will identify pertinent aspects of technology, security, audit, and compliance for CJIS stakeholders. This document is based on the Federal Criminal Justice Information Services (CJIS) Security Policy V5.1 (CJISD-ITS-DOC-08140-5.1) and will be developed in cooperation with the CJIS Technical Committee. It covers security, connectivity, access, encryption, and audit.

- The CISS User Access Policy is being developed for the certification of users of CISS information. This document will evolve into the CJIS User Certification and will encompass user agreements regarding the access, usage, and dissemination of Criminal Justice Information.

CISS Program Issues and Risks with Mitigation Strategy

Risk:

The late hiring of State positions, filling important positions with contractors, and not converting these to State positions, presents risk to the project plan and the long-term support and stability of CISS.

Mitigation:

We are hiring consultants to fill the current positions needed by the CISS team that have not been approved. This will allow us to get the work done that we are contractually required to produce and assure the successful implementation of CISS for the State.

We are working with the Department of Administrative Services (DAS) to open the required positions and change the job classifications for the Technical Architect and two Senior Project Managers. We have had difficulty filling these positions due to relatively low starting salaries offered by the State compared to the private sector. We need to hire people with the right skill set and experience with large, complex, multi-million dollar, multi-year projects. We need to offer salaries close to market rates in order to be successful. Until this is done, the risk exists that the State will lose technical and domain knowledge when the consultants leave.

Issue:

There is an issue concerning the Freedom of Information Act (FOIA) stemming from the fact that official state repositories are subject to FOIA. The CISS data store is a staging repository and not the official repository of record; therefore, it needs legislation to exempt it from FOIA requests and to require those requests be submitted to the agencies that are the repository of record.

Mitigation:

The Administrative Committee has proposed language for the legislation to correct and clarify this, which the Governing Board approved at its July 2012 meeting. This will be brought to the next legislative session.

CISS — Conclusions

The CISS Team, Xerox and DAS-BEST have been working together this past year, from the kickoff meeting in December 2011, to produce the first deliverable of CISS this December 2012. The Google like "Search" of OBTS is that first deliverable.

Over the next quarter the CISS Team will embark on project planning for the entire project in January and begin the implementation of the various deliverables that will ultimately complete

this first phase of the CISS project. This will entail the major part of the work in the project involving all of the stakeholders, RMS vendors and the culture changes needed for CISS to achieve the goals set by the State.

We look forward to working with all of our stakeholders, the CJIS Community, and our vendors in 2013 in order to successfully implement the CISS project on time, in scope and within budget.

Offender Based Tracking System (OBTS) Status Report

OBTS — Background

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 select state agencies.

OBTS Key Accomplishments – Period Ending December 2012

- The CJIS Operational Team completed development of the OBTS 7.4 software release on schedule. Key changes were exact name search results, which improved system performance; adjustments to event logs and maintenance screens to assist administrative use by OBTS team members; and modifications to the OBTS database.

- The database modifications are crucial to ongoing data purity work, which includes tracking of single Offender Based Information System (OBIS) detainer codes, corrections to generic UAR numbers and missing ticket numbers, and updates to correct generic alien registration codes. Each of these changes helps improve the accuracy of information submitted to and retained in OBTS.

- Migration to the new software will take place in February.

- The OBTS Team also worked with CISS project team members to create and test a new data exchange interface. This is significant because OBTS is CISS's first data source. The two teams clarified important business and technical requirements. The teams also developed new test cases to ensure CISS application security rules work in a similar manner as originally implemented in OBTS.

- The team completed the data purity data comparison evaluation of the OBTS/Judicial systems. At the same time, the team is now performing a technical review of Department of Correction systems. Identified data errors will be corrected and implemented during planned software releases.

OBTS Anticipated Activities – Next 180 Days

- OBTS Team continues to define OBTS 7.6 requirements and construct, test and deploy new software functionality. OBTS Version 7.4 is scheduled to be deployed as version 7.5 during month of February.

- OBTS Team to continue work on the data purity evaluation exercises of the Judicial branch's source systems, and document the findings.

- Initiate the OBTS data purity effort for the Offender Based Information System (OBIS) with DOC.

- Use of the Nastel monitoring system will be helping us to identify additional system performance areas for the OBTS production environment.

OBTS Application Release Schedule

The following release schedule is planned over the coming 12 months. To provide a more stable and predictable product upgrade cycle for OBTS, the content of each maintenance release will be guided by the priorities identified by the OBTS/CIDRIS User Group. This group will meet quarterly to review program accomplishments, re-assess program priorities and approve proposed release schedules.

Release Dates	Release Objectives
OBTS R7.5 February 2013	Maintenance Release – Defect corrections, reporting enhancements, and data purity efforts.
OBTS R7.6 May 2013	Maintenance Release – Final release content to be determined based on the priorities of the OBTS community.
OBTS R7.7 August 2013	Maintenance Release — Final release content to be determined based on the priorities of the OBTS community.
OBTS R7.8 November 2013	Maintenance Release — Final release content to be determined based on the priorities of the OBTS community.

OBTS Program Issues and Risks with Mitigation Strategy

Issue:

The Project Team is dependent on access to and cooperation of subject matter experts residing in source agencies. Due to current workload activities and changing priorities, subject matter experts may not be available as needed.

Mitigation:

The mitigation strategy is to closely monitor work efforts and take prompt corrective action as necessary.

OBTS — Conclusions

CJIS is working to further integrate OBTS with CISS. As CISS development continues, CJIS will continue to engage with and solicit feedback from the OBTS User Group. The OBTS Operational Team will also focus future application maintenance releases on enhancing performance and data quality in OBTS. With the new platform in place and the User Group engaged, the OBTS Operational Team will focus future application maintenance releases on improving performance and data quality in OBTS.

Connecticut Impaired Driver Records Information System (CIDRIS) Status Report

CIDRIS — Background

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 Agency 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 Key Accomplishments — Period Ending December 2012

- CIDRIS is increasing the accuracy and volume of successfully transmitted messages.

- All 10 troop barracks are actively submitting OUI cases. Between October 1 and November 20, state troops submitted approximately 176 OUI messages. This is a 17 percent increase, compared to the number of cases submitted during the 3rd Quarter.

- The accuracy of electronic OUI messages also improved. The number of messages correctly submitted to and processed by CIDRIS during the October - November period was approximately 85 percent. This is up 23 percent, as compared to the success rate during the 3rd Quarter reporting period totaling 69 percent.

- The CJIS team continues to work with DESPP troops to better understand the difficulties of submitting accurate electronic OUI messages outside troop barracks.

- Troopers can experience technical and logistical challenges with completing and submitting electronic OUIs. Transmitting incomplete messages causes the system to automatically reject them and negatively affects overall OUI submission rates. To help improve the electronic submission process, DESPP has created an exceptions list to help state troopers identify and remedy some of these issues.

CIDRIS Anticipated Activities – Next 180 Days

- CJIS to begin work to expand the CIDRIS program with Division of Criminal Justice.

- Testing for the new Forms Viewer program is expected to begin in January 2013.

- The CIDRIS team will continue to review and promote good practices for process improvements with DESPP, Judicial and DMV agencies.

- The CIDRIS team continued work on a new CJIS Forms Viewer. The Forms Viewer is software developed by Judicial that allows CIDRIS users to search OUI document attachments by UAR and misdemeanor ticket numbers and print agency documents on demand. The application

has been tested internally by CIDRIS team members and is being prepared for testing by Judicial General Area clerks.

- The CIDRIS implementation team will continue work to expand the collection of electronically-submitted OUI documents. For the initial Implementation roll-out, DESPP focused on electronic submission of mandatory forms including the Officers' OUI Arrest and Alcohol Test, Notice of Rights, Appearance Bond and Initializer Slip. As success rates for initial submissions increase to nearly-perfect levels, DESPP will broaden electronic document submissions to include the Blood and Urine Test Report, Misdemeanor Summons and Complaint, Officer Written Statement and other Judicial Arrest forms as determined by Warrant or without Warrant.

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). 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

DESPP, DMV, Judicial, and the CJIS Operational Team have committed to expanding use of the CIDRIS system. The CIDRIS implementation of the State Troop Barracks is complete. CJIS is now working with assisting the stakeholders for OUIs to go paperless using CIDRIS. All stakeholders will have to agree on the solution.

CJIS Governing Board Committee Updates

Administrative Committee

The committee met in October 2012 to finalize a Non-Disclosure Agreement for employees, consultants, and vendors; the forms were approved by the CJIS Governing Board at the October meeting. The Committee agreed that the CISS recertification period was two years; users will be notified 30 days in advance of their credentials expiration date. Recertification is required any time a user's claim (access rights) changes. The Committee discussed the need for CISS to send notices to CISS system administrators on all CISS users with one year of inactivity.

The CISS system administrator will be responsible for deactivating the account if necessary. CISS system changes will appear as notifications on the CISS default screen. The Committee discussed

the subject of retention of documents and data in CISS. Committee members agreed that each agency should determine the retention periods for its own data and documents within CISS. Committee members will discuss this subject with the appropriate persons in their respective agency to determine the position of that agency. An agency might want all of its documents and data retained indefinitely unless there is a statute, rule, regulation, or policy that requires destruction of a specific document or data; or an agency might want to establish other retention periods for their data and documents within CISS. The CJIS Team will follow up with each agency as to the agency's decision on this subject which will be discussed at the next Administrative Committee meeting in January.

Technology Committee

CJIS Security Policy has been drafted and will be submitted to the Administrative sub-committee for review and approval. Then it will be forwarded to the CJIS Governing Board for approval and acceptance targeted for the January 2013 Governing Board meeting.

Implementation Committee

Mark Tezaris, CJIS Program Manager, will be working with Chief Richard Mulhall, head of the Connecticut Police Chiefs Association, to develop the CISS implementation schedule for Connecticut municipal police departments going forward.

■ ■ ■

Appendix — Acronyms

AFIS = Automated Fingerprint Identification System
AST = Application Support System
BEST = Bureau of Enterprise Systems and Technology
BICE = Bureau of Immigration & Customs
  Enforcement
BOPP= Board of Pardons and Paroles
CAD = Computer Aided Dispatch
CCH= Computerized Criminal History (DESPP)
CIB = Centralized Infraction Bureau (Judicial)
CIDRIS = CT Impaired Driver Records Information
  System
CISS = CT Information Sharing System
CIVLS = CT Integrated Vehicle & Licensing System
CJIS = Criminal Justice Information System
CJPPD = Criminal Justice Policy Development and
Planning Division
CMIS = Case Management Information System
(CSSD)
COLLECT = CT On-Line Law Enforcement
  Communications Teleprocessing network
CPCA = Conn. Police Chiefs Association
CRMVS = Criminal and Motor Vehicle System
  (Judicial)
CSSD = Court Support Services Division (Judicial)
DCJ = Division of Criminal Justice
DAS = Dept. of Administrative Services
DESPP = Dept. of Emergency Services & Public
  Protection
DEMHS = Dept. of Emergency Management &
  Homeland Security
DMV = Dept. of Motor Vehicles
DOC = Department of Correction
DOIT = Dept. of Information Technology
DPDS = Div. of Public Defender Services
FOIA = Freedom of Information Act
IST = Infrastructure Support Team
JMI = Jail Management System
JUD = Judicial Branch

LEA = Law Enforcement Agency
LIMS = State Crime Laboratory Database
MNI = Master Name Index (DESPP)
OBIS = Offender Based Information System (DOC)
OBTS = Offender Based Tracking System
OCPD = Office of Chief Public Defender
OVA= Office of the Victim Advocate
OVS = Office of Victim Services
OSET = Office of Statewide Emergency
  Telecommunications
POR = Protection Order Registry (Judicial)
PRAWN = Paperless Re-Arrest Warrant Network
  (Judicial)
PSDN = Public Safety Data Network
RMS = Records Management System
SCO = Superior Court Operations Div. (Judicial)
SLEO = Sworn Law Enforcement Officer
SOR = Sex Offender Registry (DESPP)
SPBI = State Police Bureau of Identification (DESPP)
SLFU= Special Licensing of Firearms Unit (DESPP)
UAR = Uniform Arrest Record

Technology Related

ADFS = Active Directory Federated Services
COTS = Computer Off The Shelf (e.g., software)
ETL = Extraction, Transformation, and Load
FIM = Forefront Identity Manager (Microsoft)
GFIPM = Global Federated Identity & Privilege
Management (security standard used by FBI)
IEPD = Information Exchange Package Document
LAN = Local Area Network
PCDN = Private Content Delivery Network
POC = Proof of Concept
RDB = Relational Database
SAN = Storage Area Network
SDLC = Software Development Life Cycle
SOA = Service Oriented Architecture
SQL = Structured Query Language