Global Federated Identity & Privilege Management (GFIPM)
Part 1: The Federated System

The Current Information Sharing System

The Connecticut criminal justice community is made up of a variety of networks and information systems, some of them considered legacy by today's technical standards. Unlike other states, there is no standardized law enforcement Records Management System in place for all agencies to utilize. Hardware and software acquisitions were made independently as budgets allowed and the need dictated, so you have a mix of new and old systems that are unable to communicate with one another. Governance structures, trust relationships, cultures and protocols also evolved independently within each agency further complicating the ability for agencies to interact seamlessly. As a result, criminal justice information is organized into hundreds of smaller systems, each requiring separate registration and authentication processes. In many cases, users are not able to see all of what they need to see because of legacy systems that make information sharing very difficult. For systems that are open to sharing, users are required to have multiple security credentials (certificates, usernames, passwords, etc.) making information sharing tedious, expensive and time consuming. It also becomes an administrative burden, as it requires vetting ("Who are you?"), permissioning ("What can you access?"), and credentialing ("How do I know that it's you?") repetitively for each user. The extra work that it takes to provision users further complicates the process.

How the Federated System Works

The formation of a standardized global trust system streamlines the process for information sharing. Global Federated Identity and Privilege Management (GFIPM), a program directed by the Global Justice Information Sharing Initiative, enables information sharing for state and local agencies through a federated model that is secure, scalable, and cost-effective. The global part of Global Federated Identity &

GFIPM, continued from Page-1

Privilege Management (GFIPM) means that the standards set using GFIPM apply to everyone. Anyone who has the proper credentials will have access to information set up by the federated agencies.

A federation provides a standardized framework for allowing agencies to directly provide services for users that are trusted (managed) by their partner(s) yet not managed by the agency providing the service. "A federation is defined as 'a group of two or more partners who trust each other, and have business and technical agreements allowing a user from one federation partner (participating agency A) to seamlessly access information resources from another federation partner (participating agency B) in a secure and trustworthy manner.' Major organizational participants in a federation may vet and maintain information on the users they manage, yet each federation partner retains control over the business rules for granting access to the sensitive information it owns. The federation partners establish the electronic trust needed to securely allow access to information by sending standards-based electronic credentials to federation partner information service(s) as part of the authentication mechanism. The federation partner information service(s) evaluates the trusted electronic credential to determine whether to grant or deny access to the requested service or information." [1] For the CISS project, the federation partners are the criminal justice agencies.

Federated identity allows a user's roles, rights, and privileges to be communicated securely in the criminal justice community. GFIPM is about establishing a common identity framework across multiple identity providers. This allows systems to validate users from other agencies instead of requiring the users to log on to multiple systems or having to provide personal information to all of these different systems. The partnering organizations (federation) will implement a common, nationally defined structure for describing information about users. The identity provider will protect user information: any external system will be able to obtain only the information necessary to determine if the user is authorized to access those systems.

The GFIPM model includes the following federation security concerns:

• Identification/Authentication - Who is the end user and how were they

[1]*Global Federated Identity and Privilege Management,* Justice Information Sharing, Dept. of Justice. https://it.ojp.gov/gfipm.

CJIS Roadmap

GFIPM, continued from Page–2

authenticated?

- Privilege Management - What certifications, clearances, job functions, local privileges, and organizational affiliations are associated with the end user that can serve as the basis for authorization decisions?

- Audit - What information is needed or required for the purposes of auditing systems, systems access and use, and legal compliance of data practices?

GFIPM and the Passport Process

You can compare the GFIPM model to that of the global passport program. The federations in this case are the group of participating countries, each of which has a passport control agency to validate, authorize and disseminate passports to its national citizens. These agencies agree to vet and maintain information on each citizen that obtains a passport. They work with their country-specific law enforcement and criminal justice agencies to certify the identity and nationality of the passport holder. A border agent will evaluate the passport based on the trusted credential that was issued by the federation partner, who has researched the identity and citizenship of the passport holder and confirmed their information.

Compare GFIPM to the Passport Process

Traveler (User) — Applies for a passport

Government Agency (Federation Partner)

Researches/Stores:
- Authenticate applicant
- Privileges
- Audit

Denies a passport: unable to authenticate

Issues a passport based on authentication
Traveler enters Customs

Customs Officer (Federation Partner)

Customs Officer:
- Checks trusted credentials
- Applies country's rules for entry

Denies entry

Enters Country

There are international networks supporting the identification and trust mechanism for global passport authentication (US Passport Control, Canadian Border Services Agency, etc.) Each country participating with passports subscribes to a specific network which interconnects with other passport networks to route validations of passports. Based on the results, the border agent will either grant or deny access to the country. The destination country (federation partner) considering the traveler's passport information applies its own business rules based on the passport information and other properties known at the time of the request.

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. Certification processes are in place with numerous Federal and State agencies which would allow CISS to integrate and share information seamlessly with external partners as well as allowing credentialed users from those agencies to access CISS information.

Next month, the GFIPM Series: Part II will examine the role of claims in GFIPM. ❖
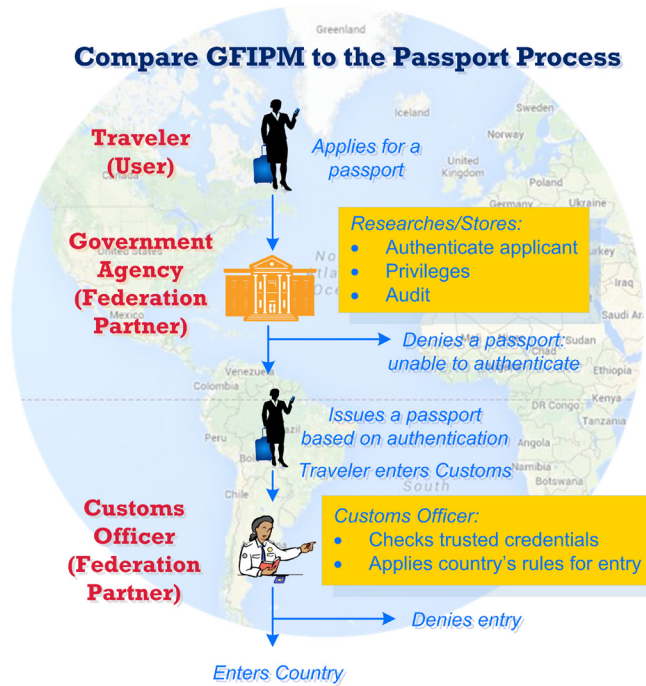
RMS Certification Update

The Business and Technology teams worked on the functional and system requirements used by local law enforcements' record management systems. In January, the Technology team met with the three Connecticut Police Chiefs Association (CPCA) pilot vendors; Hunt Computer Design, KT International and TriTech Software Systems. The objective was to walk through the technology guidelines, update documentation for clarification and obtain vendor feedback for overall feasibility and work effort estimates. CJIS will complete the vendor review and estimates in February. The Business team continued to work on the preliminary business requirements that will support the initiation of Information Exchanges by Uniform Arrest Reports (UARs) and Misdemeanor Summonses. ❖

CJIS Academy

The Coventry P.D. Hosts CISS Presentation

On January 7, 2014, Jeanine Allin, CJIS Public Safety Liaison, gave a presentation to the Coventry Police Department on the Connecticut Information Sharing System (CISS). The presentation described the background of CJIS and the reasons for the development of CISS as a comprehensive, state-wide information sharing system for Connecticut. Allin spoke about the major components of CISS, including Information Exchanges, Search Releases and Workflow Waves. Allin also talked about the CISS Community Portal, security and support plans, and CJIS Academy, the new CJIS educational and community outreach program. The twenty minute presentation, attended by sixteen police officers and two staff members, ended with a question and answer session.

If you represent a state or law enforcement agency and would like to know more about CISS, consider hosting a CISS presentation at your facility. To do so, please contact Jeanine Allin by phone: 860-688-2169 or email: Jeanine.allin@ct.gov.

For more information about training sessions or presentations, go to the CJIS Website and select CJIS Academy. ❖

For more information about CJIS Academy, contact Jeanine Allin, CJIS Public Safety Liaison:

Phone: 860-622-2169
Email: jeanine.allin@ct.gov
CJIS Support Group: 860-622-2000
CJIS Website: www.cjis.ct.gov

OBTS Certification Classes

CJIS offers certification classes three times a year for OBTS. The classroom is located at 99 East River Drive, 7th floor, East Hartford, CT 06108.

Training Dates

- February 11, 2014, 9 AM to 12 PM
- June 12, 2014, 9 AM to 12 PM
- October 16, 2014, 9 AM to 12 PM

For more information and to sign up, visit the CJIS Academy Webpage.

CISS Project Management Updates

Search Release 1 (SR1)
User search of criminal justice agency data systems.

During January, thanks to the concerted efforts of both the Department of Correction (DOC) and DAS-BEST, the CJIS Technical team downloaded the complete collection of inmate photographs. The system updates daily, keeping the collection current.

Xerox and CJIS agreed on which of the more than three hundred contract requirements would be delivered in Search Releases 1 and 2. This agreement outlines the features that will be given to users, and the computer operations that must be tested.

The DOC and the Court Support Services Division (CSSD) have each agreed to make their field supervision officers part of the audience for Search Release 2. This group is a good complement to the SR1 audience, which is local law enforcement.

In February, CJIS and Xerox will sign the Portal Taxonomy Specification for Search Release 1. This document defines the underlying technical structure of the User Interface, presents the initial search screens, describes error-handling conditions, and sets the overall structure for the SR1 user interface.

Xerox and CJIS will then collaborate on a limited-function prototype of the Search User Interface. CJIS will solicit stakeholder/user input for the screen design that will display information from the PRAWN and OBIS data sources.

CJIS and Judicial will continue work on the complex data requirements for Criminal and Motor Vehicle System (CRMVS) as part of SR2. ❖

Accomplishments

1. OBIS inmate photos are now in CISS servers.
2. Xerox and CJIS reached agreement on distribution of contract requirements in Search Releases 1 and 2
3. Added probation officers, parole officers, bail commissioners and related administrative staff to SR2

Next Month

4. Complete technical requirements for the User Interface
5. Xerox/CJIS to develop a prototype User Interface
6. Complete CRMVS data gathering requirements

January

1. OBIS inmate photos are now in CISS **Complete**

CISS

3. Added parole and probation officers, bail commissioners & staff to SR2 **Complete**

2. Xerox/CJIS agree on distribution of requirements for SR1, 2 **Complete**

We Are Here

CJIS SRs

February

5. Xerox/CJIS to develop prototype UI

4. Complete technical requirements for UI

6. Complete CRMVS data gathering requirements
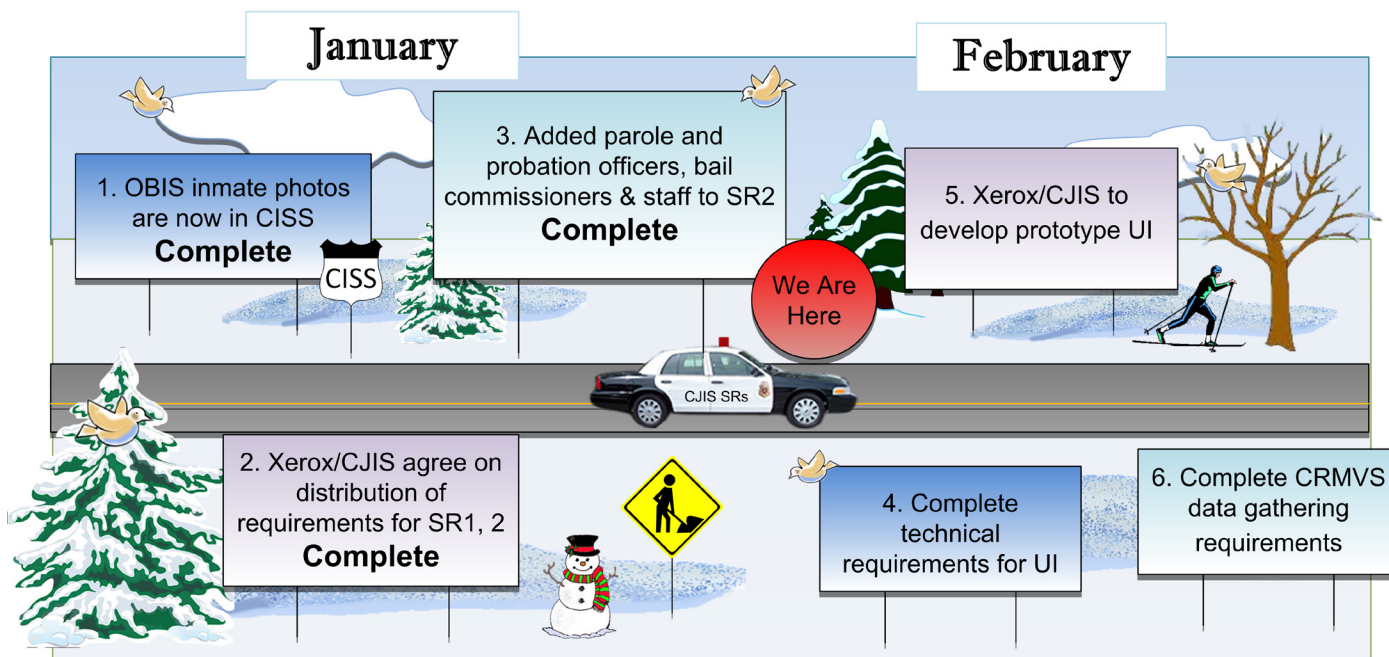
CISS Project Management Updates, continued from Page 5

Wave 0, Version 1.6 and Operations

Foundation and infrastructure of CISS, and Operational Support.

Wave 0, v. 1.6

In January, the CJIS technical team executed the initial performance benchmark for infrastructure and external information sources, including inmate photos. This provided a comparison of the system performance metrics and processes to current industry practices. CJIS also upgraded server operating system software.

The CJIS technical team also completed a feasibility study of deploying F5 application networking technology. This utility promotes system efficiency and security.

In February, for operation support, the team continues work on the configuration and integration of several Microsoft Systems Center software modules, including Operations Manager, Service Manager and Virtual Machine Manager. ❖

Operations

In January, CJIS submitted a deployment plan to the Nutmeg Public Safety Data Network (PSDN) Applications Review Board. The plan provides details for network connectivity between the CISS application and the LEAs' RMSs.

In support of operations, the CJIS team also drafted a collection of standard operating procedures (SOP). ❖

Accomplishments

1. CJIS technical team executed the initial performance benchmark for infrastructure and external information sources.
2. Upgraded server operating systems software.
3. Completed a feasibility study of F5 application networking technology.
4. Drafted standard operating procedures for CJIS Operations Management.
5. CJIS submitted a deployment plan to the Nutmeg PSDN Applications Review Board.

Next Month

6. Configure and integrate several Microsoft Systems Center software modules.

CJIS **Roadmap**
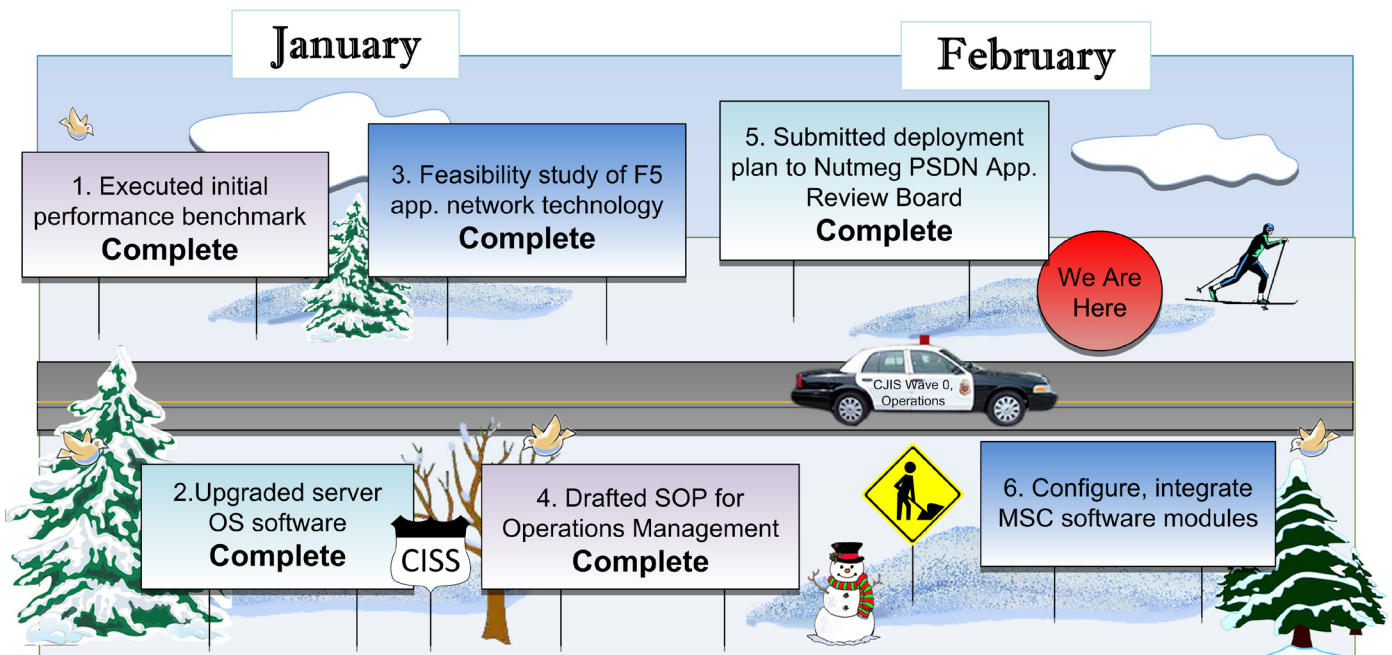
CISS Project Management Updates, continued from Page 6

Waves 1-3

Automatic electronic Information Exchanges

The CJIS Business and Technology teams held serveral informational sessions on GFIPM with stakeholders in January. The sessions addressed the reasons for using GFIPM, how it works, and how CJIS and stakeholders will apply GFIPM standards for the CISS project.

In February, CJIS will continue to review the GFIPM Control Policy Access spreadsheet with the Community to confirm Wave 1 report claims.

The team will continue integration zone activities for Workflow 1 and Information Exchange requirements for Workflow 2. This includes requirements gathering for transmitting data for use by state agencies. Work will continue with RMS vendors to ensure LEA information can be seamlessly integrated with CISS.

The CJIS Business team will begin to collect business requirements for infractions, which is part of the Wave 3 release.❖
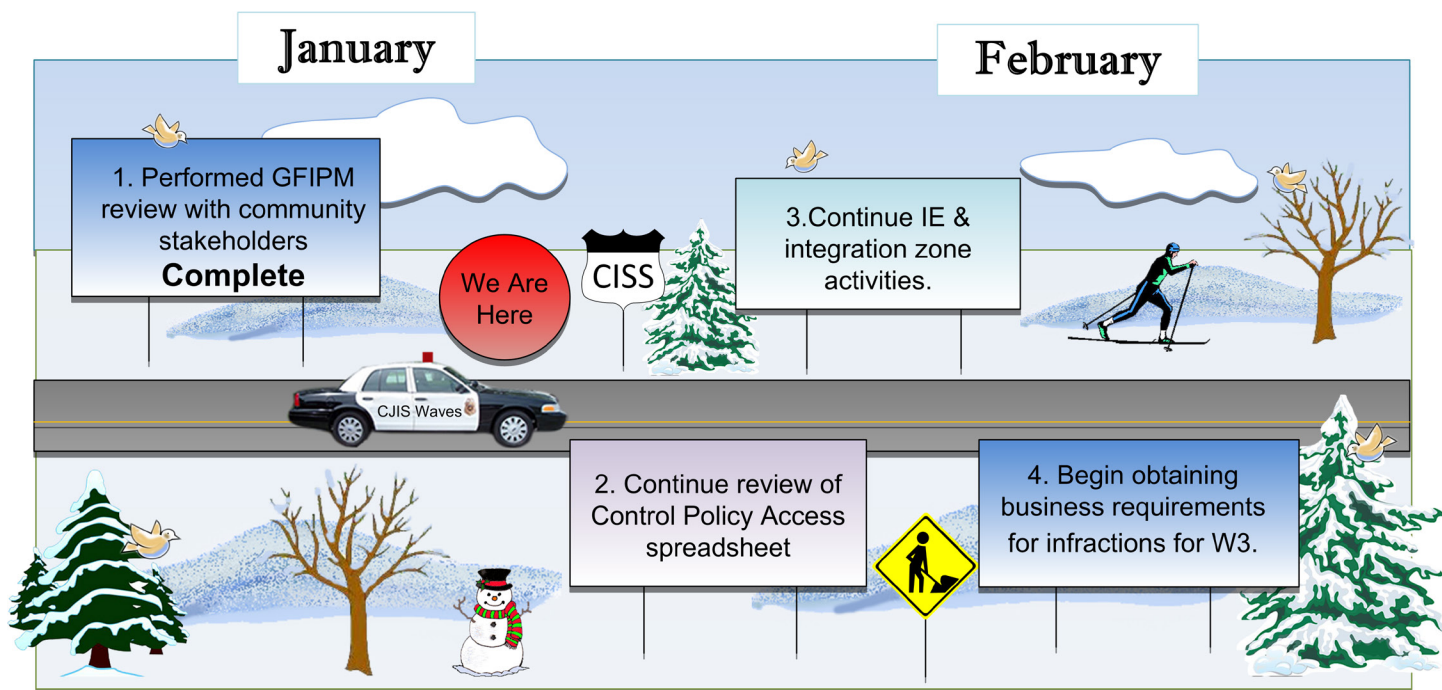
Accomplishments

1. Performed GFIPM review with community stakeholders.

Next Month

2. Continue review of Control Policy Access spreadsheet with Community.
3. Continue Information Exchange and integration zone activities.

Next Month (contin.)

4. Start gathering business requirements for infractions-Wave 3.

CJIS Roadmap

January Governing Board Meeting Highlights

The first Governing Board Meeting of 2014 was held on Thursday, January 16, 2014, at the Division of Criminal Justice in Rocky Hill, CT. Judge Patrick Carroll, III, and Mike Lawlor presided over a crowd of over forty Governing Board members and guests. Before the CISS project slides were presented, Judge Carroll and Mike Lawlor announced that while Dr. Schriro, the new Commissioner for the Department of Emergency Services and Public Protection (DESPP), could not attend this meeting, she will be participating in future meetings.

Lawlor also announced that the biweekly Governance Committee meetings would continue and address the most pressing issues. At the recent Governance Committee meeting, Rick Hegwood, Durational Project Manager, Joan Hilliard (DESPP), and a

Left: Melody Currey, Reuben Bradford, Garvin Ambrose, and Erika Tindill.

Above, Front: Judge Carroll, Mike Lawlor, Bob Kaelin Back: Ken Barrone, Jim Fazzalaro, Evelyn Godbout, John Russotto, and Sean Thakkar.

select number of the Governing Board members discussed the FBI's Management Control Agreement (MCA). The group will continue to have discussions on the CJIS Security Policy and the MCA in February.

Executive Director Sean Thakkar then reviewed the agenda for the presentation and introduced Rick Hegwood.

Hegwood recounted his meetings with the stakeholders and concluded that there needed to be additional time and involvement allotted for user testing and that special attention needed to be given toward agency resource constraints. He added that because of continued contract negotiations with Xerox, most of the original dates for implementation are no longer applicable.

To improve their relationships with stakeholders, obtain feedback, and incorporate more stakeholder involvement in the decision making process, CJIS has added a Community meeting that directly follows the CISS Monthly Status

Above: Darryl Hayes, Garvin Ambrose, Steve Spellman, and Joan Hilliard.

Meetings. This Community meeting addresses current technical and business subjects that are in line with the current stage of the project and also serves as an informal question and answer session. In December, the CJIS team shared information on Global Federated Identification and Privilege Management (GFIPM).

Hegwood talked about the Wave 1 scope and limiting the audience for Wave 1 Information Exchanges to Local Law

CJIS Roadmap

◆ Meetings ◆

The next **CISS Monthly Status Meeting** will be held on February 5, 2014 at 1:00 PM at 101 East River Drive, East Hartford. A **CJIS Community Meeting** will directly follow the CISS Monthly Status Meeting.

The next **CJIS Governing Board Quarterly Meeting** will be held on April 17, 2014 at 1:30 PM at the Office of the Chief State's Attorney, 300 Corporate Place in Rocky Hill.

Governing Board, continued from Page-8

Enforcement (LEA), Department of Emergency Services and Public Protection (DESPP), Department of Criminal Justice (DCJ), Judicial's Administrative Services Division (ASD) and Court Support Services Division (CSSD) and the Department of Correction (DOC). The list would temporarily exclude the Division of Public Defender Services (DPDS) and the Department of Motor Vehicles (DMV) until the MCA is finalized. A Governing Board vote was taken on this decision and a unanimous agreement was reached. Agencies not in Wave I would continue to see information as they do today, but they would not be able to use the CISS Information Exchange. Other topics included working with stakeholders on integrating Information Exchanges into their systems, and with designing a user interface for the CISS Community Portal.

Thakkar and Lawlor gave an overview of CJIS's participation with the Racial Profiling project. Two men, Ken Barrone and Jim Fazzalaro of CCSU, were introduced as leaders who are implementing the legislation. Lawlor went over the background of Racial Profiling, and emphasized that the CJIS Governing Board will collect and store the information electronically until e-Citation is capable of taking over and then CJIS will only provide a repository. There will be no access to CISS.

Bob Kaelin from MTG gave his Independent Verification and Validation Report. In the report, Kaelin noted that because of rescheduling due to vendor contract issues, the scope will change and dates will slip. The state is negotiating with Xerox on a contract amendment and should have a signed agreement shortly. He also said that without a full time project manager, there is a lack of oversight on the project. To alleviate this problem, Sean Thakkar and the Governing Board Co-Chairs are currently searching for a full time project manager to take the helm.

Kaelin emphasized the need to hire the planned staff as state employees rather than have them remain as consultants. He explained that there remains the potential loss of knowledge and expertise as contractors tend to be more transitory than permanent workers. Even so, it was noted that state job classifications often do not take into account the current technical skills needed for a state of the art system and pay scales are far below the current market offering. ❖

Happy Valentine's Day!

AG Recommendations and Plan of Action

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.

Action Item Description	Mitigation
AG Recommendation #1: 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).	1/24/14: The Governance Committee satisfies this recommendation.
AG Recommendation #2: 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.	1. Sean Thakkar to work with Karen Buffkin (OPM) and contact AG's office on how to proceed with Risk Assessment report. 2. Include CISS plain language description from Working Group on all future reports and presentations. 3. Provide update on major changes to the CISS project to the Board.
AG Recommendation #3: 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.	A Special Board meeting will be scheduled to finalize the agreement. Karen Buffkin will provide insight to the Board.
AG Recommendation #4: 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.	At the next regularly scheduled Board meeting, provide projected budget and project timeline (and possible project plan if agreement reached with Xerox.)
AG Recommendation #5: 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.	Update with more critical information, FBI letter and the project plan section and send to the Board for their approval, then to the AG's office.
AG Recommendation #6: Address and resolve all payment issues with Xerox.	In progress.

CJIS Roadmap

Recommendations, continued from Page–10

Action Item Description	Mitigation
AG Recommendation #7: Consider implementing frequent quality assurance reviews.	Holding monthly meetings between Sean Thakkar, Rick Hegwood and Bob Kaelin (MTG).
AG Recommendation #8: 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.	Potential candidates are being reviewed. The following is the three step process for hiring the next CISS project manager: 1. Interview with Rick Hegwood, Sean Thakkar, Mark Raymond (DAS-BEST) 2. Interview with Mike Lawlor, Judge Carroll and Karen Buffkin 3. Interview with key Board members - Kevin Kane (DCJ), Chief Mulhall (CPCA) and Dr. Dora Schriro (DESPP)
AG Recommendation #9: Evaluate whether changes, including the addition of personnel, are necessary in the CJIS Leadership and CSG.	This issue has been addressed due to changes already made and more that are forthcoming.

Farewells and Welcomes
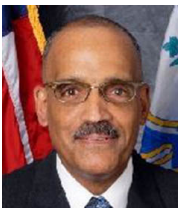
CJIS would like to extend their appreciation and best wishes to CJIS Governing Board member Reuben Bradford, who retired from office as Commissioner of the DESPP at the end of January 2014. Bradford was appointed as Commissioner of Public Safety by Governor Dannel Malloy in 2010 and has served on the CJIS Governing Board for more than three years. ❖

All CJIS newsletters and meeting minutes are posted on www.ct.gov/cjis

CJIS would like to welcome the new Commissioner for the DESPP, Dr. Dora Schriro. Dr. Schriro is a nationally recognized leader in corrections and detention, and is widely praised for development of definitive policy analysis in the nation's homeland security efforts and as an innovator in risk assessment and crime prevention. She worked closely on the country's homeland security efforts and is the only person in the nation to have led two state and two city correctional systems. Dr. Schriro comes to us from her position as Commissioner of the New York City DOC. Dr. Schriro will be representing the DESPP as a Board member of the CJIS Governing Board. ❖