

GFIPM Part II: Understanding Claims

GFIPM Components

Last month's article on GFIPM Part 1: The Federated System introduced Global Federated Identity & Privilege Management (GFIPM) and described how a federated security system works. The article gave the international passport system as an example of how the GFIPM federal security system is constructed. In this second series, Understanding Claims, we will explore the components of GFIPM, the role of a claim in the passport system, the definition of a claim versus a role, and which GFIPM claims are being assigned to data in criminal justice source systems.

Claims are the building blocks that make up the foundation of the GFIPM model. "At the highest level of concept within the GFIPM model, there are three vital components that must interact between users of multiple systems. Each plays a role in the claims identity and transmittal process.

- Identity Provider (IDP) – (Stakeholders, for example, Judicial, DESPP, etc.)
- Service Provider (SP) – (CISS)
- User Credential Assertions (Metadata) – Security Token (claims)

The **identity provider** is the authoritative entity responsible for authenticating an end user and asserting an identity for that user in a trusted fashion to trusted partners. The identity provider is responsible for account creation, provisioning, password management, and general account management. This may be achieved with existing locally accepted security mechanisms and tools.¹ For the CISS project, the Identity Provider will be the authorized administrator for each agency. This administrator will be in charge of assigning credentials or claims to each user in his agency.

Federation partners who offer services or share resources are known as **service providers**. The service provider relies on the identity provider to assert information about a user using an electronic user credential (secure token), leaving the service provider to manage access control and dissemination based on a trusted set of user credential assertions.² CISS is a service provider and it stores claims for each user (as assigned by agency system administrators).

GFIPM establishes a standard, well-defined set of **user credential assertions (metadata)** about users, including a common framework (semantics and representation) for all organizations to describe basic user identity, such as certifications, memberships, affiliations, and contact information. "Metadata is data that describes other data. Meta is a prefix that in most information technology usages means 'an underlying definition or description.' Metadata summarizes basic information about data, which can make finding and working with particular instances of data easier."³ Within the metadata are the claims.

Continued on Page-3

^{1,2} *Global Federated Identity & Privilege Management*. Justice Information Sharing, US Department of Justice, Office of Justice Programs, National Initiatives. <http://it.ojp.gov/gfipm>.

³ *Metadata*. Taken from Whatis. <http://whatis.techtarget.com/definition/metadata>.



CJIS Governing Board
 Revolutionary Technology Linking
 Connecticut's Criminal Justice &
 Law Enforcement Community
 March 2014 Vol. 3 No. 3
www.ct.gov/cjis

Co-Chairs

Mike Lawlor, Under Secretary,
 Office of Policy & Management

Judge Patrick L. Carroll, III,
 Chief Court Administrator

MEMBERS

- Garvin G. Ambrose, Esq., *Victim Advocate,*
Office of Victim Advocate
 Eric Coleman, *Senator,*
Co-Chair, Joint Comm. on Judiciary
 Melody Currey, *Commissioner,*
Dept. of Motor Vehicles
 Donald DeFronzo, *Commissioner,*
Dept. of Admin. Services
 James Dzurenda, *Commissioner,*
Dept. of Correction
 Gerald M. Fox, *Representative,*
Co-Chair, Joint Comm. on Judiciary
 Kevin Kane, Esq.,
Chief State's Attorney,
Office of Chief State's Attorney
 John A. Kissel, *Senator,*
Ranking Member, Joint Comm. on Judiciary
 Richard C. Mulhall, *Chief,*
CT Police Chiefs Association
 Rosa C. Rebimbas, *Representative,*
Ranking Member, Joint Comm. on Judiciary
 Dr. Dora Schriro, *Commissioner,*
Dept. of Emerg. Services & Public Protection
 Susan O. Storey, Esq.,
Chief Public Defender,
Division of Public Defender Services
 Erika Tindill, Esq., *Chair,*
Board of Pardons and Paroles
- CJIS SENIOR MANAGEMENT**
 Sean Thakkar, *Executive Director*
 Mark Tezaris, *Program Manager*

Comments, corrections, and inquiries
 about this newsletter should be directed to:
 Sean Thakkar, *CJIS Executive Director,*
Sean.Thakkar@ct.gov, or
 Patty Meglio, *Technical Writer,*
Patricia.Meglio@ct.gov

Connecticut Racial Profiling

Connecticut Racial Profiling Prohibition Project (CTRP3), the Institute for Municipal and Regional Policy (IMRP) at Central Connecticut State University (CCSU), 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.

Ken Barone, Policy & Research Specialist at the IMRP, and Jim Fazzalano, Project Manager at CCSU with the assistance of CJIS, has successfully completed work on the technical infrastructure, Web application and help desk support required for this project. The CJIS Governing Board will collect and store the information until e-Citation is capable of taking over. When e-Citation is capable of supporting CT Racial Profiling, CJIS will only provide a repository. This is a standalone database, unrelated to other CJIS projects. ❖



In This Issue

- GFIPM Part II: Understanding Claims
Page-1

- Connecticut Racial Profiling
Page-2

- CJIS Academy
Page-2

- CISS Project Management Updates
Page-5

- CJIS Project Positions for Approval
Page-9

- RMS Certification and Network Update
Page-9

- CJIS Crossword Puzzle
Page-10

CJIS Academy

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

- 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](#).

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

GFIPM, continued from Page-1

The international passport provides a good example of how each role follows the GFIPM model.

The Passport is a Claims-Based Model

A passport is an internationally recognized and trusted (federated) travel document that verifies a person's identity and nationality. A passport, when issued, is also a claim. Administered by each country's IDP, a passport validates the identity of the individual based on that country's unique identity documentation. In the U.S., this documentation would be a driver's license, a social security number, and a photo ID. It is accepted globally by all countries for travel by air, land and sea. Upon researching an application for a passport, an individual's background is checked to see if there are any outstanding warrants for their arrest and if there are any other travel restrictions imposed by law enforcement agencies. These restrictions are claims against the individual.

A Type of Passport is a Claim

There are several types of passports, each of which is a type of claim that represents certain conditions and privileges. Three of the most familiar types are Regular, Diplomatic, and Official.

Regular (dark blue cover): A Regular passport is issuable to all citizens and non-citizen nationals. A sub-type of regular passports is no-fee passports, issuable to citizens in specified categories for specified purposes (claims). For example; an American sailor, for travel connected with his duties aboard a U.S.-flag vessel.

Diplomatic (black cover): A Diplomatic passport declares that this individual is immune from lawsuit or prosecution under the host country's laws. It is only issued to government

diplomats and their immediate families. When applying for this type of passport, an individual must provide proof of diplomatic status.

Official (brown cover): An Official passport is issuable to citizen-employees of the United States assigned overseas, either permanently or temporarily, and their eligible dependents, to members of Congress who travel abroad on official business, and to US military personnel when deployed overseas.

Claims in the Passport Process



How Claims Support Passport Security

When a ticket is purchased to travel to a foreign country, the ticket seller asks for the individual's passport number. When the individual checks in to the airport, he must present his passport. The flight information is logged in your passport records at this time. Every person arriving at a port-of-entry into a country (land, sea, or airport) is inspected by a customs officer and everyone must present a valid passport.

There are five international database centers for passports. When a person submits a passport during travel, the customs officer checks the passport against one of these databases for restrictions. Information (claims) that might appear in someone's passport records could be outstanding, such as driving tickets, criminal records, or federal wanted notices. The photo in the passport (claim) is compared with the photo in the database and with the live person standing before the customs officer. The individual's passport is checked again when he leaves the country and returns home. The custom agent checks for any claims made toward the individual in that country.

Roles versus Claims

Claims should not be confused with **roles**. Roles are general identifiers or functions, while claims contain unique personal identifiers.

Continued on Page-4

GFIPM, continued from Page-3

When analyzing multiple criminal justice agencies with separate and diverse systems, roles are often broadly defined and lack common definition (e.g., analyst). Because of this, it would be difficult to apply a role-based system to users from multiple agencies, multiple states, and federal agencies.

Like a passport, a claim is more uniquely delineated in comparison to roles. GFIPM defines a common vocabulary of claims for the criminal justice and law enforcement communities. For example, instead of defining a person as an “analyst,” an authorized agent would maintain that the person has the privilege to search criminal history and/or criminal intelligence data. The criteria that the authorizing agent would use to make this decision would be based on a specific clearance level, certification, and/or privilege. An individual can have access to one or multiple data sources, based on their agency authorized claims. Like the passport model where there are different types of passports, there are different types of claims.

GFIPM Claims in CISS

GFIPM claims are currently being assigned to data by agencies who own the data, based on their interpretation of the sensitivity of the data that will be accessed by the CJIS community. As the CISS project progresses, more GFIPM claims will be added and assigned to data.

The four GFIPM claims currently being assigned to data at this time are:

- Public Data Self Search Home Privilege Indicator
- Sworn Law Enforcement Officer Indicator
- Criminal Justice Data Self Search Home Privilege Indicator
- Youthful Offender Data Self Search Home Privilege Indicator

Public Data Self Search Home Privilege Indicator

The GFIPM standard for public data is non-classified information. A user with this claim would be any user with a valid CISS user account. This would include users from any

agency or branch that is represented in the CJIS Governing Board.

Sworn Law Enforcement Officer Indicator

This GFIPM claim defines a Sworn Law Enforcement Officer (SLEO) as:

- Full time employee of state recognized LEA
- Authorized to make an arrest
- Certified by state certifying authority

Criminal Justice Data Self Search Home Privilege Indicator

The Criminal Justice Data Self Search Home Privilege Indicator claim authorizes a user to view criminal justice data from law enforcement agencies, administrative agencies, courts, and correction agencies regarding arrests, investigation, conviction, and sentencing for violation of a federal, state, tribal or territorial criminal law, including post-conviction correctional supervision during incarceration, supervision after release from incarceration and performance of restitution.

Youthful Offender Data Self Search Home Privilege Indicator

The Youthful Offender Data Self Search Home Privilege Indicator is a custom claim, since GFIPM does not have a standard claim pertaining to youthful offenders. As stated in CGS Section 54-76b, youthful offender data is information that pertains to an individual with youthful offender status. Youthful offender data is usually coupled with another claim, for example, criminal justice data.

So far, the CRMVS, CIB, MNI/CCH, OBIS, OBTS, POR, and PRAWN source systems in CISS will include data that was assigned GFIPM claims (governed by the GFIPM security policy) by authorized agency administrators. ❖

Next month, the GFIPM Series: Part III will examine how claims are assigned in CISS.



CISS Project Management Updates

Search Release 1 (SR1)

User search of criminal justice agency data systems

In February, the CJIS Business team, the Judicial Information Technology Division (ITD), and the Court Operations (CO) team concluded months of work and agreed on the basic search source requirements for Judicial's Criminal Motor Vehicle System (CRMVS). This massive, complex data system underlies all of Court Operations, and feeds other Judicial and non-Judicial data systems. All teams invested many hours into mapping the data and understanding its underlying business rules.

CJIS took a deeper look at the Offender Based Information System (OBIS) data system, responding to invitations from the system's owner (DOC) that we refine our data requirement documents. As a result, additional fields and business rules will be available for CISS search.

In March, the CJIS technical team will update technical requirements for the user interface screens for OBIS and Paperless Re-Arrest Warrant Network (PRAWN).

Additionally, the CJIS Technical team will begin discussions with the Judicial Technical team on how to replicate the massive CRMVS system. This initiative will require extensive work and time to complete.

Anticipating the approval of the Xerox contract amendment, CJIS and Xerox will work to ensure that the contract requirements scheduled to be addressed in Search Release 1 are completely documented and ready for Xerox design work. ❖

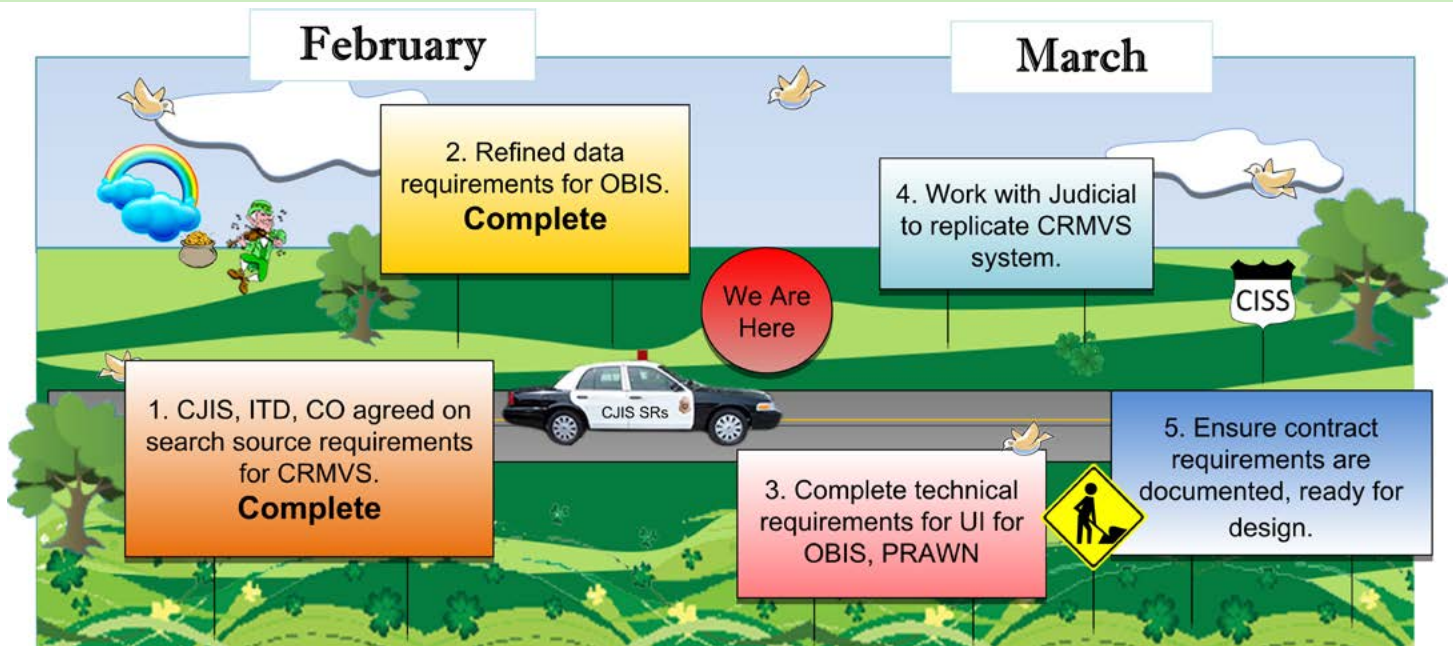
PM Updates, continued on Page-6

Accomplishments

1. CJIS, ITD, CO agreed on search source requirements for CRMVS.
2. Refined data requirements for OBIS and PRAWN.
3. Complete technical requirements

Next Month

- for UI for OBIS, PRAWN.
4. Work with Judicial to replicate CRMVS system.
5. Ensure contract requirements are documented, ready for design.



CISS Project Management Updates, continued from Page 5

Wave 0, Version 1.6

Foundation and infrastructure of CISS, and Operational support

In February, the CJIS Technical team performed a variety of service requests used to maintain the CISS server infrastructure. Some of the work performed was used to enhance the performance of the virtual servers and disk storage systems. The team also prepared additional system monitoring capabilities and documentation of infrastructure operating procedures for use by the CJIS operations team.

The CJIS Technical team, along with the DAS-BEST technology staff, also met with Microsoft and F5 Networks technology subject matter experts to begin work on a series of high-level system designs. The result of this collaboration will support a new application networking technology that will enhance security, availability, and performance for the CISS system.

This new networking technology

benefits CJIS users by optimizing the delivery of the CISS applications.

Both CJIS and DAS-BEST conducted planning sessions to support off-site data storage options.

For March, the team plans to continue documentation of operating procedures and release plans of the four SDLC environments.❖

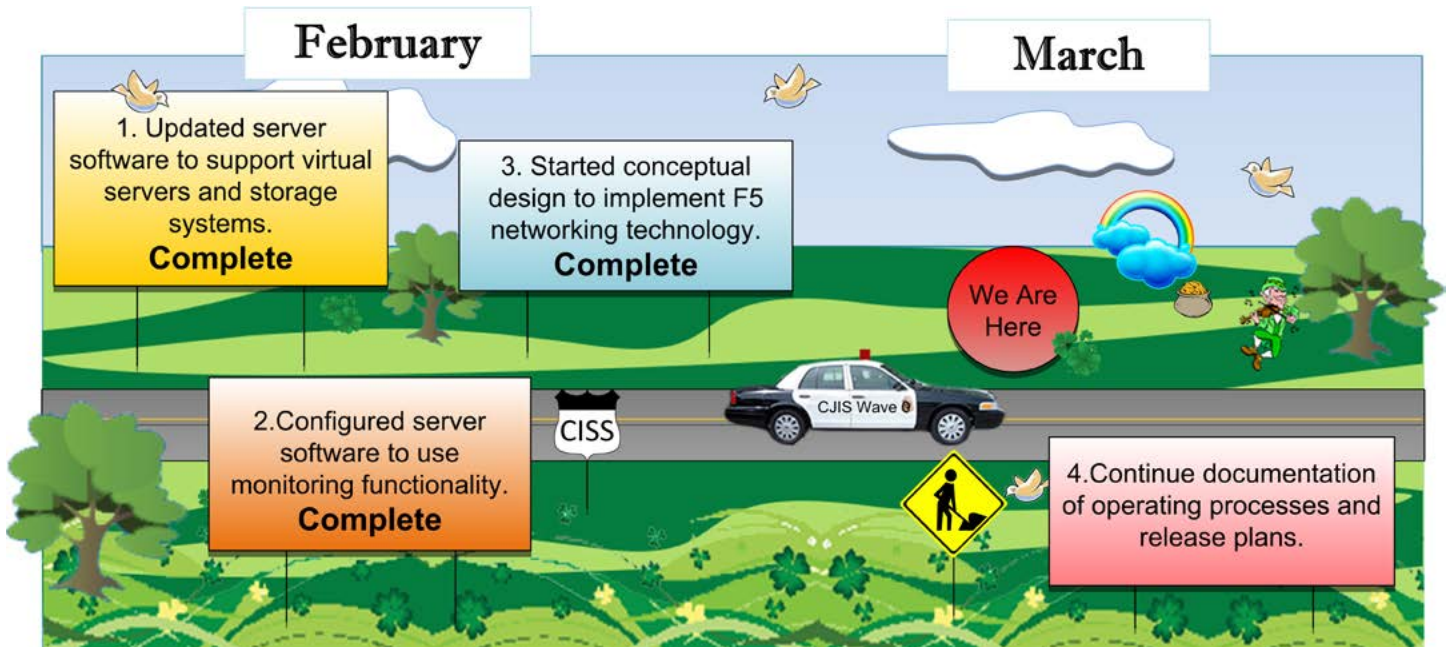
PM Updates, continued on Page-7

Accomplishments

1. Updated server software to support virtual servers and storage systems.
2. Configured server software to use monitoring functionality.
3. Started conceptual design to implement F5 networking technology.

Next Month

4. Continue documentation of operating processes and release plans.



CISS Project Management Updates, continued from Page 6

Operations Management Support and systems management

The CJIS Operations team is working diligently to prepare for the CISS SR1 release. This includes filling state positions, implementing support tools, building a help desk, and creating project dashboards.

Management is in the process of requesting nineteen state employees for operations and development (see page 9). Currently, more than half of the CJIS employees are short term consultants who have specific technical skill sets. In order to retain the skill sets and domain knowledge already acquired, it is critical that these positions are filled by the state

as soon as possible. This will help to ensure knowledge retention. Current CJIS consultants will be able to apply for these positions.

The CJIS Operations team is also implementing monitoring tools that will support the CISS system, including the software, hardware, and real-time network connectivity. While this work is being done behind the scenes, users will benefit from the way that CISS will run smoothly, securely, and with little or no interruption.

Discussions are underway and plans are being drafted to create a strong

and efficient help desk to support the CISS software and hardware systems, including the hiring and training of state employees. The CJIS Operations team is also exploring several options for the right help desk tools to aid users once they start using CISS.

To better communicate with criminal justice stakeholders, CJIS is creating new dashboards (available online) that will be updated in near real time. The first dashboard, due out in April, will be the CISS Project Dashboard. This will provide regular updates on the CISS project as work progresses. Other performance indicator dashboards will be added later in the year. ❖

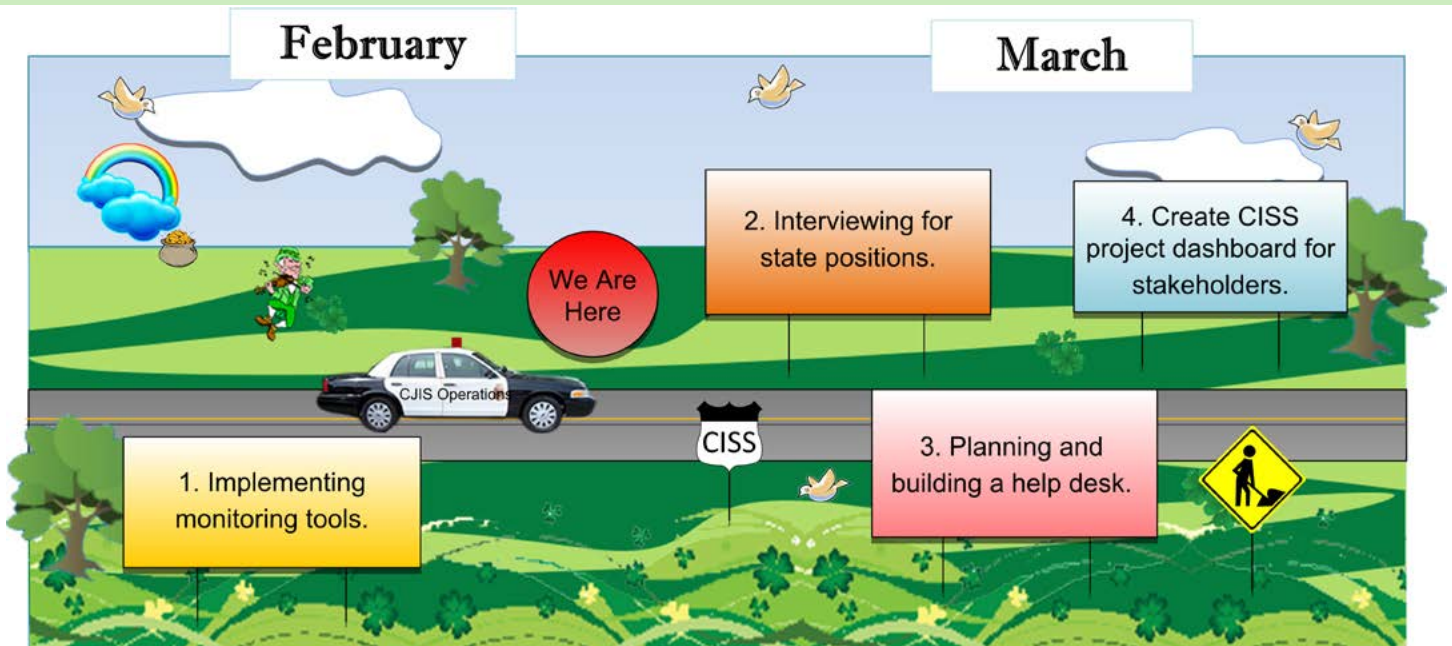
PM Updates, continued on Page-8

Accomplishments

- 1. Implementing monitoring tools.

Next Month

- 2. Interviewing for state positions.
- 3. Planning and building a help desk.
- 4. Create CISS project dashboard for stakeholders.



CJIS Project Management Updates, continued from Page 7

Waves 1-3

Automatic electronic Information Exchanges

During February, the CJIS Business team continued work on gathering business requirements for Uniform Arrest Report (UAR), Misdemeanor Summons and Infractions Workflow Waves. The scope of the requirements includes the collection of incident arrest information submitted to the

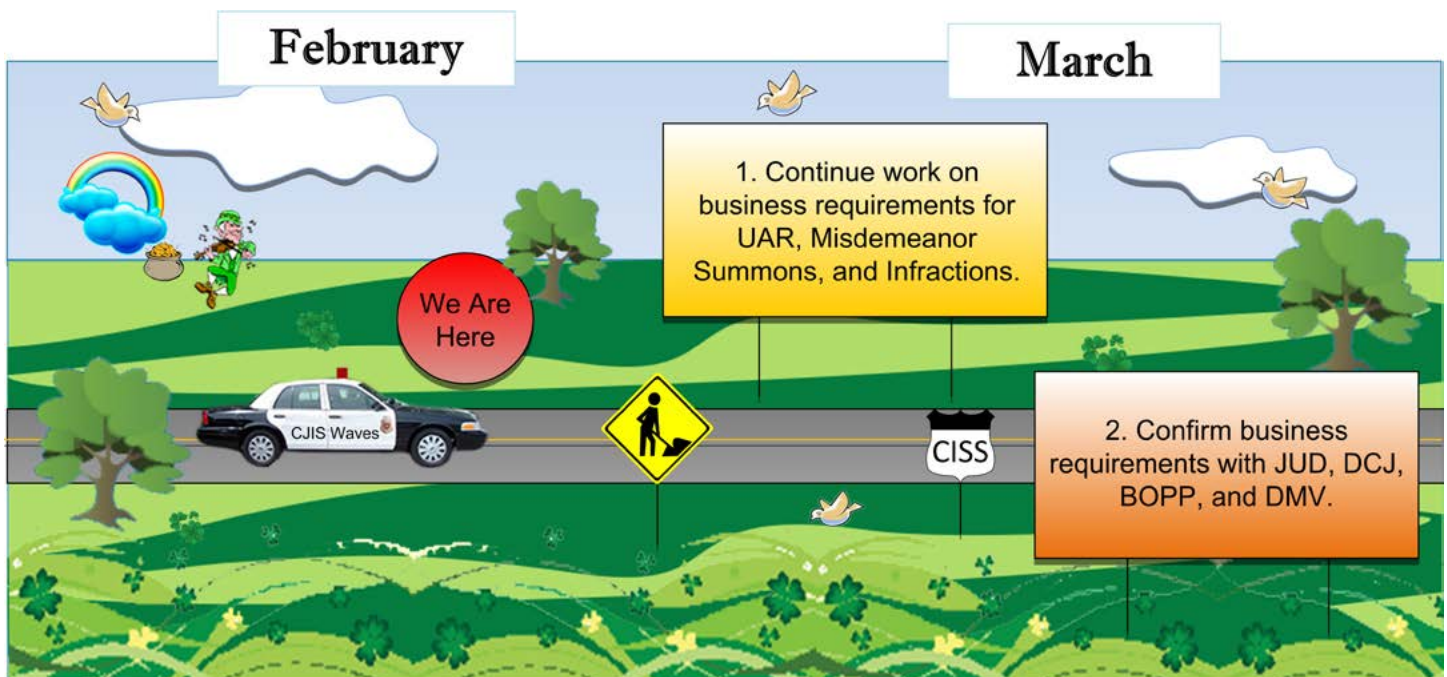
CJIS application by local law enforcement systems, along with the activities associated with consuming the information by agency stakeholders.


Topics discussed included confirmation of arresting data elements and documents, agency notification and transformation of data using national information exchange standards.

Work efforts to confirm the Waves 1, 2 and 3 business requirements with Judicial (JUD), Division of Criminal Justice (DCJ), Board of Pardons and Paroles (BOPP) and Department of Motor Vehicles (DMV) is expected to continue through March. ❖

Next Month

1. Continue work on business requirements for UAR, Misdemeanor Summons, Infractions.
2. Confirm business requirements with JUD, DCJ, BOPP, DMV.



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

CJIS Project Positions for Approval

A meeting with CJIS, OPM, DAS-BEST, and DAS resulted in an agreement to open all nineteen remaining positions held by consultants. In late 2013, CJIS began discussions on the nineteen positions, with targeted dates in 2014. The following is a table that shows the positions being requested. All of the nineteen positions will require DAS and OPM approval.

Order of Hiring	Position Name	Projected Roll-Out Dates
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

RMS Certification and Network Update

Last month, the CJIS Business and Technology teams continued work on the RMS certification project. To enhance the business requirements documentation, the team designed several use case scenarios to describe general types of incident and arresting events that occur locally and how the information of the criminal events are captured and processed by law enforcement record management systems. The objective of the exercise is to document a general understanding of how data and paperwork to support the uniform arrest report, misdemeanor and infraction charging documents are collected, organized, and reported by the local law enforcement officers.

The Technology team also continued a joint review of the certification package with three Connecticut Police

Chiefs Association (CPCA) selected pilot vendors. The review covers the general design and implementation of the National Information Exchange Model (NIEM) and Information Exchange Package Documentation (IEPDs) used to send and receive incident arrest information between Records Management Systems (RMSs) and CISS.

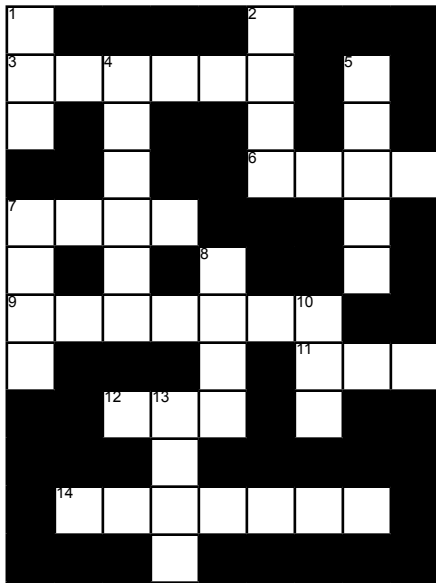
RMS Network

During February, CJIS and DAS-BEST technology teams began the general deployment of the CISS network. To start, the team confirmed CJIS network requirements, IP address schema, initial software configuration, and installation schedule for seven police departments having equipment ready for deployment. Towns include Manchester, East Hartford, Windsor Locks, East Windsor, Enfield, Simsbury

Continued on Page-10

CJIS Crossword Puzzle

Test Your Knowledge and Skill on Criminal Justice Vocabulary!



Across

- 3. To set aside a judgment that a judge finds improper
- 6. A court-ordered delay in judicial proceedings to give a losing defendant time to arrange for payment
- 7. A formal written order issued by a judicial jurisdiction
- 9. To cancel a contract
- 11. Short for order to show cause
- 12. To have legal title to something
- 14. A court order directing a peace officer to arrest and bring a person before the judge

Down

- 1. Short for department that services victims of crime
- 2. Peace officer organization
- 4. Collection of information attributes
- 5. Database that contains re-arrest warrants.
- 7. To secretly record a conversation with another person
- 8. Official claim against property for payment of a debt for services rendered
- 10. Organization for reparation
- 13. A person (usually a minor) who has a guardian appointed by the court to care for and take responsibility for that person

Answers will appear in the April issue of CJIS Roadmap.

RMS, continued from Page-9

and Granby. Use of the CISS application across the Public Safety Data Network (PSDN) was also approved by the PSDN Governing Board.

Next steps are to confirm the installation schedule for the remaining towns currently 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. ❖

◆ Meetings ◆

The next **CISS Monthly Status Meeting** will be held on March 12, 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.

