CJIS Roadmap
State of Connecticut
Criminal Justice Information System
April 2014 Vol. 3 No. 4

GFIPM Part III: Claims Authentication and Assignment

In GFIPM Series Part I, we described the GFIPM model and how a federated system works. Using the passport process as an example of a federated model, we compared it to the way it will be applied in the CISS project. In Part II of the GFIPM series, Understanding Claims, we went into more detail about claims, including the components of the GFIPM model and their role in the claims process. Continuing with the passport example, we described how claims support passport security as a person arranges and proceeds to travel to and from another country.

In Part III of the series, we will explore how users are authenticated and claims are assigned. Just as federated claims in the passport process provide security and claims authorization on travelers systematically, in the CISS model, federated claims provide security and claims authorizations when a user attempts to access CISS.

Authenticating CISS Users

The CISS application attaches claims to a security token based on user information contained in the user store. The user action (searches, information exchanges) allowed in CISS will depend on the claims attached to their token.

Figure 1 shows how a user obtains authentication with an Identity Provider (IDP) (the authoritative entity for each agency responsible for authenticating an end user) in order to access a secured resource in CISS. When the user attempts to access CISS (Step 1) and selects their IDP (Step 2), the IDP will direct the user to the login process (Step 3).

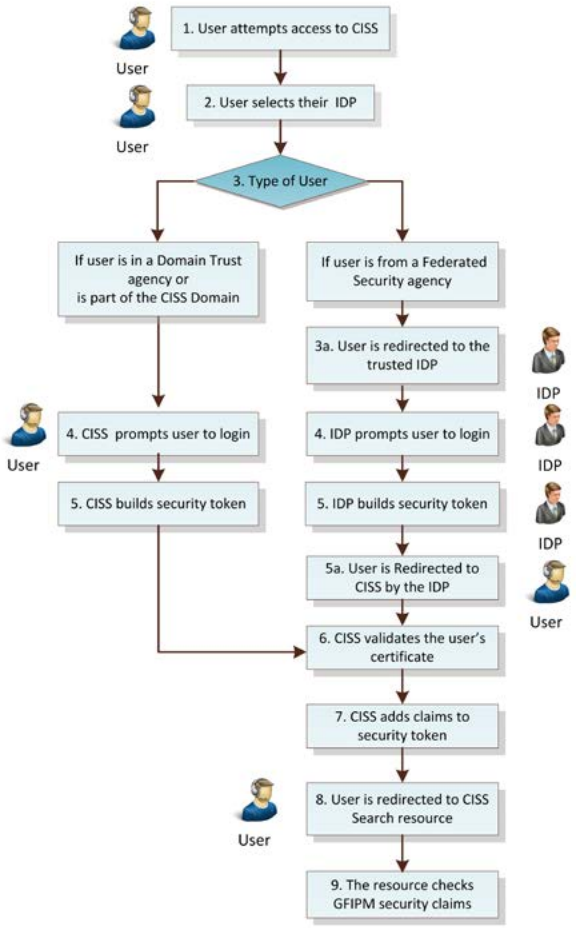


Figure 1: Process flow for authenticating users and adding claims.

There are three different models for the authentication to accommodate agencies of different sizes and technical capability: CISS Active Directory, Domain Trust, and Federated Security. If the user is part of CISS Active Directory, the user is maintained in an Active Directory (a

Continued on Page-3

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

CJIS Records Retention

On March 6th 2014, Jeanine Allin, CJIS Public Safety Liaison, met with Le Ann Power, the Public Records Administrator at the State of Connecticut Library, and members of her staff to talk about records retention related to CJIS projects. It was determined that CJIS will need its own retention and disposition schedule that will be coordinated to follow each stakeholder agency's retention schedule. CJIS will work with Connecticut Public Records to accomplish this task.

Representatives from Connecticut Public Records will host a training session on records retention scheduling for the CJIS staff in early May. Meanwhile, the CJIS staff will work with stakeholders to collect pertinent requirements on their retention and disposition schedules. Some of the agencies will have unique rules for records retention that will need special consideration.

Once CJIS completes its requirements gathering with stakeholders, the CJIS staff will work with Connecticut Public Records to draft a retention and disposition schedule for project records. The schedule will then be presented to the stakeholder community and Xerox for their review and sign-off. ❖

In This Issue

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

structured repository of information on people and resources within an organization) that is hosted in CISS and authenticated by a CISS security service. If the user is in a Domain Trust agency, the user account is maintained in the Active Directory domain hosted by the agency and trusted by CISS. If the user is supported in a Federated Security, a federated trust is established between the agency Active Directory and the CISS Active Directory and the user is then redirected to the trusted IDP (Step 3a).

The user is prompted to login (Step 4). Next, a security token is built, depending on the type of security model (Step 5). If the user is in a Domain Trust or CISS domain agency, CISS builds the security token. If the user is in a Federated Security agency, the IDP builds the security token and then directs the user to CISS (Step 5a).

CISS validates the user's certificate (Step 6) and adds claims to the security token (Step 7). The user is then redirected to the Search resource (Step 8). Finally, the resource checks the GFIPM security claims and grants or denies the user access to CISS (Step 9).

GFIPM Claims: The User Assignment Process

CJIS is currently working with four GFIPM claims that will be assigned to agency users that are related to the criminal justice community. They are:

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

Because public data is non-classified information, all users with a CISS user account will have the Public Data Self Search Home Privilege Indicator claim. The other three claims are more restrictive based on privileges and security clearance.

Within each agency, there will be authorized Administrator(s) who will assign one or more of the GFIPM claims to their agency users' profiles, which are retained in the User Store within CISS. For example, a person who is a chief, dispatcher, police officer, detective, or records clerk would have the claim Criminal Justice Data Self Search Home Privilege Indicator as well as the Public Data Self Search Home Privilege Indicator and Sworn Law Enforcement Officer Indicator. In this case, a records clerk and dispatcher would be acting on behalf of a SLEO.

As the CISS project progresses, more GFIPM claims will be added to the list. For a complete description of the current GFIPM claims, go to GFIPM Claims in CISS.

Mapping Claims to Data Elements

To ensure that a user receives only the data that he is authorized to view, data elements must first be mapped to a specific GFIPM claims classification and business rules must be written for the delivery of the data.

All data is being assigned GFIPM claims by agencies who own the data, based on their interpretation of the sensitivity of the data that will be accessed by the CJIS community. The exception: Judicial will be assigning law enforcement agency data to claims. To prepare data emanating from the data source systems for searches, the CJIS Business team is working with the owners of data to match the elements (or

Continued on Page-4

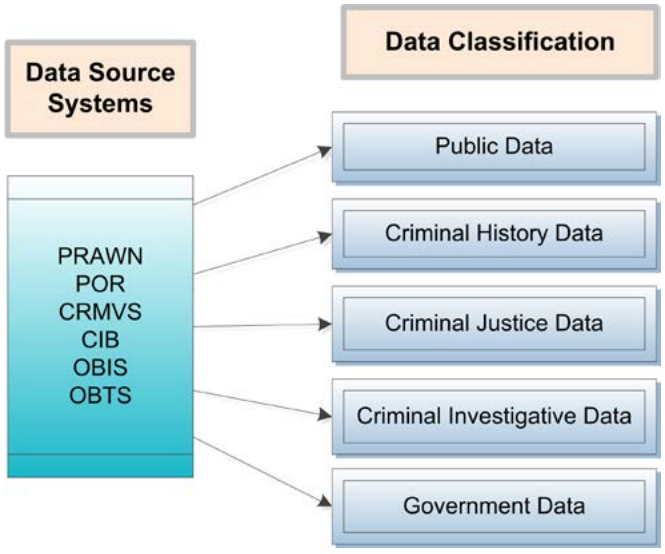


Figure 2. Mapping source systems to data classifications.

GFIPM, continued from Page-3

fields) in the records to specific classifications. If a document is scanned in and saved as a graphic (i.e., .jpg, .gif, .png, .bmp), the highest claim level (most secure) will be applied. So far, there are five types of data classifications as defined by GFIPM:

- Public Data
- Government Data
- Criminal Justice Data
- Criminal History Data
- Criminal Investigative Data

To prepare data emanating from the data source systems for searches, the CJIS Business team is working with the owners of data to match the elements (or fields) to specific classifications.

Some data may require additional privileges. For example, public defenders will only be able to view cases that are assigned to them, and can view only youthful offenders cases assigned to them. In either case, it would be a subset of data in the criminal justice data classification.

Data can have one or several types of data classification. For example, data that contains arrest information will have specific elements in Criminal History, Criminal Justice, and Public data classifications.

CJIS will write business rules that will dictate when and how the data is stored in CISS for the Information Exchanges and for Searches. In CISS, data is available in two ways: Information Exchanges between criminal justice agencies, and replicated data from the CJIS Community data sources.

Every data source has business rules that classify the data and define security restrictions. Once data is assigned from the data source systems to GFIPM data classifications, it is ready for users to access. Users are allowed access to data based on the GFIPM claims indicators in their user profile. These GFIPM claims indicators will ensure that users can receive and search for information pertinent to their authorization.

Summary

The GFIPM model is a standardized global trust system that streamlines the process of information sharing. It employs a federated identity that provides a standardized framework to allow agencies to provide services securely to users who are trusted by their partners, though not managed by the agency providing the service. Like the passport model, the GFIPM model provides identification and authorization, privilege management, and auditing best practices.

When a user attempts to access CISS, federated claims provide security and authorization. Currently, four GFIPM claims will be assigned to stakeholder agency users by an authorized administrator from each agency. To ensure that a user receives only the data that he is authorized to view, CJIS will work with stakeholders to map their data elements to five GFIPM claims classifications, based on their interpretation of the sensitivity of the data. Business rules will be applied to direct storage and set restrictions on sensitive data.

The GFIPM trust model is implemented seamlessly in the CISS architecture, resulting in secure, rapid and comprehensive information exchanges and searches. ❖

For more information on GFIPM, refer to CISS Documentation in the CJIS Publications page on the CJIS Website.

RMS Network

Over the past few months, CJIS and DAS-BEST technology teams worked with local law enforcement agencies (LEAs) to install a modern routed Internet Protocol (IP) data communications network that would support CISS Information Exchanges. Fifteen more towns were deployed in March, including Avon, Bristol, Berlin, and Farmington, bringing the total of installations to date to nineteen.

The CJIS teams are scheduling deployments with the remaining towns currently participating in the CJIS RMS Network. ❖

CISS Project Management Updates

Search Release 1 (SR1)

User search of criminal justice agency data systems

During March, the Department of Correction (DOC) and CJIS teams succeeded in loading nearly two million inmate photos into the CISS servers. Additionally, the photo database is updated daily by photos of new prisoners or updated photos of existing inmates. Approximately 260 new photos are imported daily.

CJIS staff members met with the DOC IT, Classification and Records staff members and completed technical documentation of the Offender Based Information System (OBIS). As a result, new fields will be added to the OBIS replica.

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

Additionally, the CJIS Technical team will begin discussions with the Judicial Technology team regarding how to replicate the massive Criminal and Motor Vehicle System (CRMVS).

Information about DOC inmates' visitors is useful to law enforcement, probation and parole officers in their investigations. The CJIS Technical Team and the DOC IT staff members are developing a procedure that will populate CISS servers with visitor information, both historical and current, a process that is similar to the uploading of inmate photos.❖

PM Updates, continued on Page-6

Accomplishments

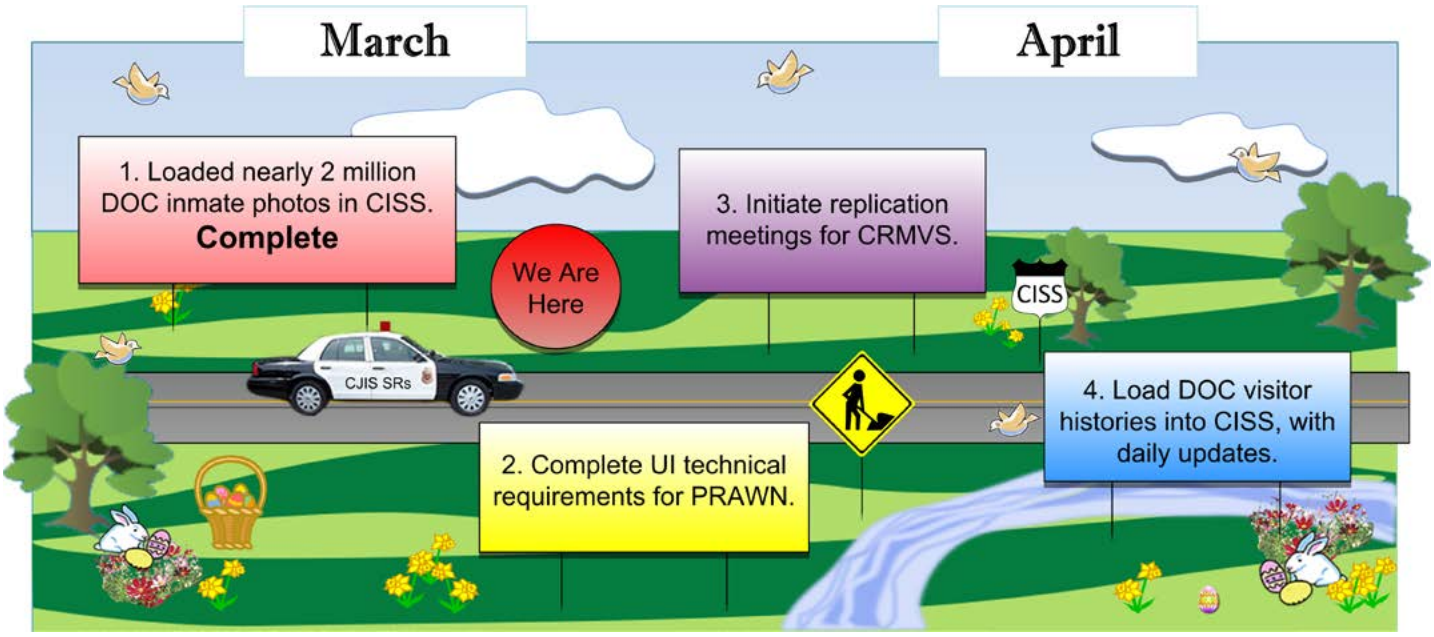
1. Loaded nearly two million DOC inmate photos to CISS servers.

Next Month

2. Complete the UI Technical Requirements for PRAWN.
3. Initiate replication meetings for CRMVS

Next Month

4. Load DOC visitor histories into CISS, with daily updates.



CISS Project Management Updates, continued from Page 5

Wave 0, Version 1.6

Foundation and infrastructure of CISS, and Operational support

Over the past month, the CJIS Technical team continued to configure Microsoft server software and cluster functionality to provide a highly available environment. The team also installed additional disk drives, increasing available storage for the User Acceptance Testing (UAT) and Production environments.

The CJIS and DAS-BEST Technical teams met with Microsoft and F5 Networks technology subject matter experts to design support for the new application networking technology. Discussions to support off-site data storage options were conducted with DAS-BEST.

The CJIS Technical team will continue to document technical operating procedures and release plans to support the CISS application.

The CISS Project Managers will meet with stakeholders to review the project schedule and address any concerns.❖

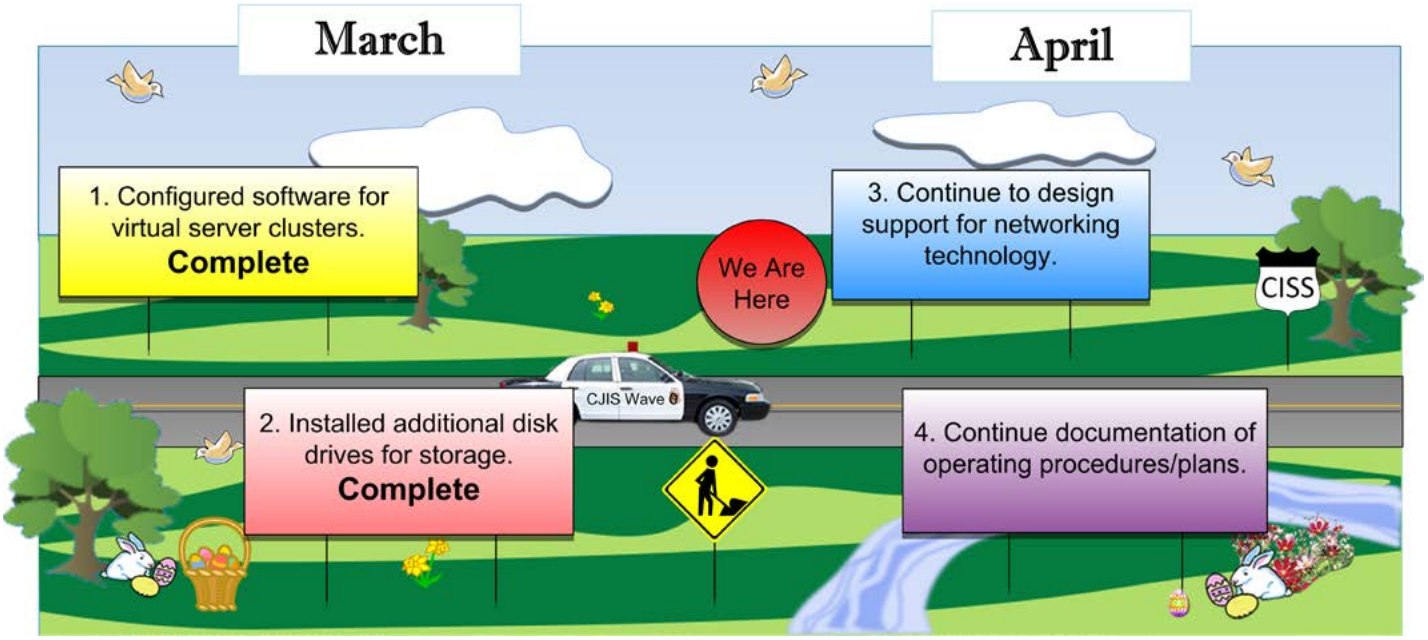
PM Updates, continued on Page-7

Accomplishments

1. Configured server software to support virtual server clusters and high availability.
2. Installed additional disk drives for storage.

Next Month

3. Continue to design support for F5 networking technology.
4. Continue documentation of operating procedures and release plans.



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

CISS Project Management Updates, continued from Page 6

Waves 1-3

Automatic electronic Information Exchanges

During March, the CJIS and Xerox teams continued to collect and confirm requirements for Uniform Arrest Report (UAR), Misdemeanor Summons and Infractions workflows. For Wave 1, UAR workflow, CJIS and Xerox completed an interim review to affirm the high-level workflow requirements submitted in November 2013.

For Wave 2 Misdemeanor Summons workflows, the CJIS Business team worked on completing documentation updates and obtaining stakeholder concurrence for receipt of summons notifications and associated paperwork. The CJIS Business team also completed the base documentation for business requirements for Wave 3, Infractions. The team will meet with stakeholders to review this documentation.

The CJIS Technical team continued to document the CISS Community Portal functionality. This will provide information on accessing paperwork and other content submitted through CISS Information Exchanges.

The CJIS Technical team is preparing to start the design stage for Wave 1. The team is working on Integration Zone requirements, which focuses on converting agency data formats that are unique to each agency to a single national information exchange format.

The CJIS Business team and Xerox will host a presentation and community discussion on the GFIPM claims process (GFIPM 101) on April 23rd at 101 East River Drive, East Hartford. ❖

PM Updates, continued on Page-8

Accomplishments

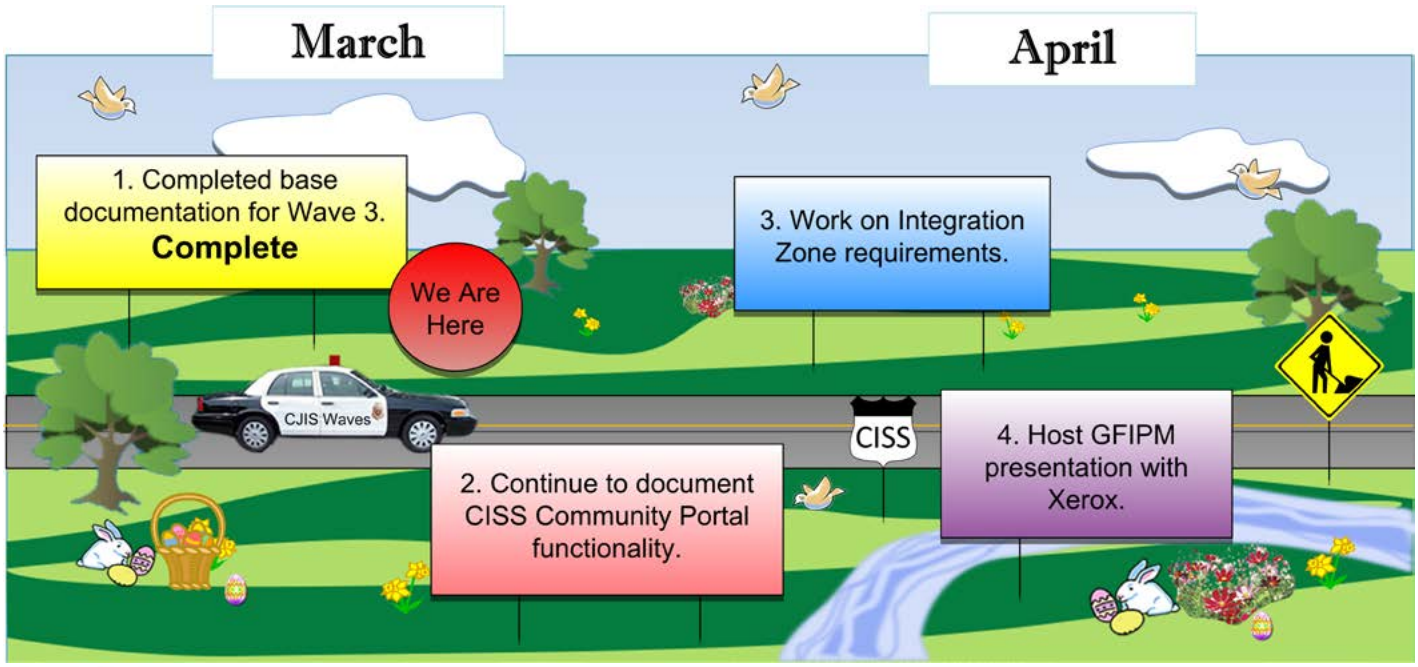
1. Completed base documentation for business requirements for Wave 3.

Next Month

2. Continue to document CISS Community Portal functionality.
3. Work on Integration Zone requirements for agency data.

Next Month

4. CJIS, Xerox will host GFIPM presentation.



CISS Project Management Updates, continued from Page 7

Operations Management

Support and systems management

The CJIS Operations team continues to prepare for the CISS SR1 release. This includes drafting state positions, implementing support tools, adding resources, and building a help desk.

The nineteen state employee postings have been drafted and provided to DAS. These job postings are currently navigating through the approval process.

The CJIS Operations team has implemented Microsoft System Center Operations Manager (SCOM), a monitoring tool that will support the current version of CISS. It will act as a detection and reporting instrument for system operations.

New software was chosen for the CJIS help desk to aid users once they start using CISS. Microsoft System Center Service Manager will provide management support when questions arise on CISS.

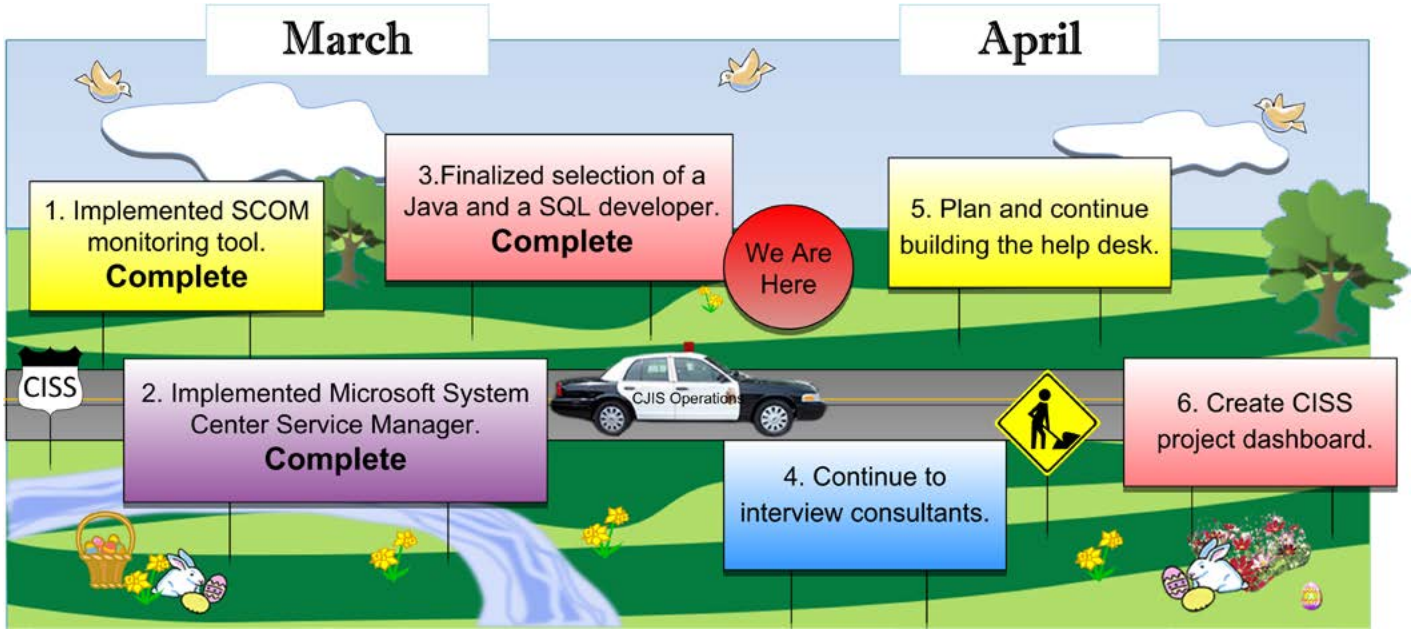
Next month, the Operations team will interview consultants for support positions, plan and begin to build a help desk for CISS and create a CISS project dashboard that will display milestones and Key Performance Indicators (KPIs).❖

Accomplishments

1. Implemented SCOM, a monitoring tool, for the current production of CISS.
2. Implemented and configured Microsoft System Center Service Manager, a help desk tool.
3. Finalized selection of a Java and a SQL Developer (consultants).

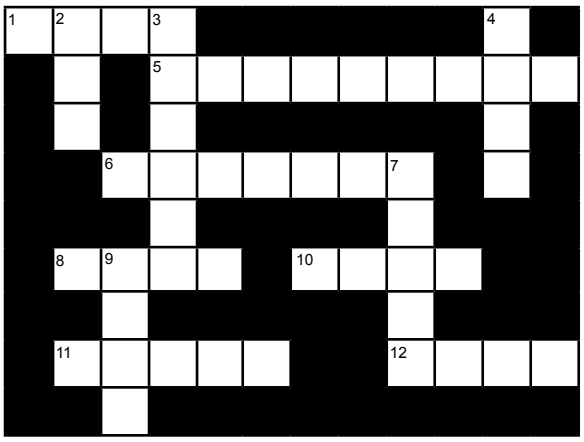
Next Month

4. Continue to interview key positions for Operations (consultants).
5. Plan and continue building the help desk.
6. Create a CISS project dashboard with milestones and KPIs.



CJIS Crossword Puzzle

Test Your Knowledge and Skill on Criminal Justice Vocabulary!



Answers will appear in the May issue of CJIS Roadmap.

Across

1. Agency with authority to grant pardons and parole to eligible and appropriate offenders in the community.
5. Written statement of facts voluntarily made by a sworn attester.
6. A record of an arrest made in a police station.
8. Acronym for a sworn officer of the law.
10. Acronym for community-driven, government-wide, standards-based approach to exchanging information.
11. Electronic weapon.
12. A formal document used to present a convicted defendant to the DOC for incarceration.

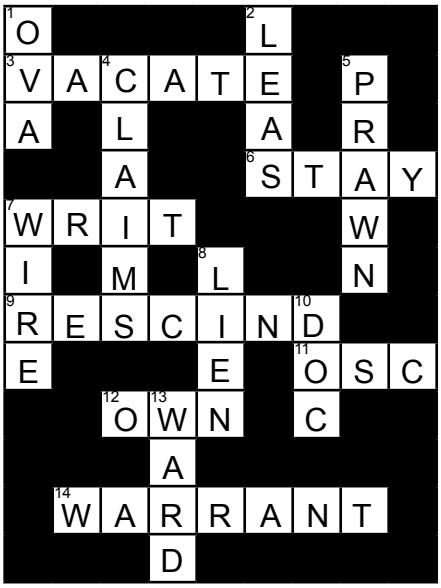
Down

2. Agency that provides the information used to formulate and implement public policy for the state on the Governor's behalf.
3. Permission to leave prison before the official time.
4. A violent disturbance of the peace by an assembly of people.
7. Guidelines and standards for establishing, implementing, and governing federated identity management approaches.
9. Acronym for district police agencies.

CJIS is Moving!

CJIS will be moving to 55 Farmington Ave., 11th Floor, Hartford, CT at the end of May. All phone numbers will remain the same. Stay tuned for information updates.

Answers to the March crossword puzzle.



Meetings

The next **CISS Monthly Status Meeting** will be held on April 9, 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.