CJIS
State of Connecticut
Criminal Justice Information System
Roadmap
Revolutionary Technology Linking Connecticut's Criminal Justice & Law Enforcement Community
October 2012 | Vol.1, No. 6

Agencies Choose User Security Models for CISS

The first step toward integrating the Connecticut criminal justice community's information system is underway.

For the agencies the first step was choosing the model by which their users will connect to CISS.

The principal agencies are: the Department of Corrections (DOC), Board of Pardons and Paroles (BOPP), the Department of Emergency Services and Public Protection (DESPP, aka, the state police), the Department of Motor Vehicles (DMV), the Judicial Branch, the Division of Public Defender Services (DPDS), the Division of Criminal Justice (DCJ), and the Office of the Victim Advocate.

Thirty-one massive data bases from these agencies, plus data from all "arresting units" will be funneled into CISS. Arresting units refers to all state police, local law enforcement, and the police forces of various other organizations, such as large universities or the Metropolitan District Commission.

But before anyone can use the system to access any of this information, there is the matter of security.

The manner in which each of the individual agencies interface with CISS is the first step in creating a secure system, and the first step in connecting with these agencies is setting up a system for provisioning their users.

It's kind of a big job. CISS is designed to serve 30,000 users, which is why the storage systems being created will hold petabytes of data. (See related story on page 4.)

Continued, page 2

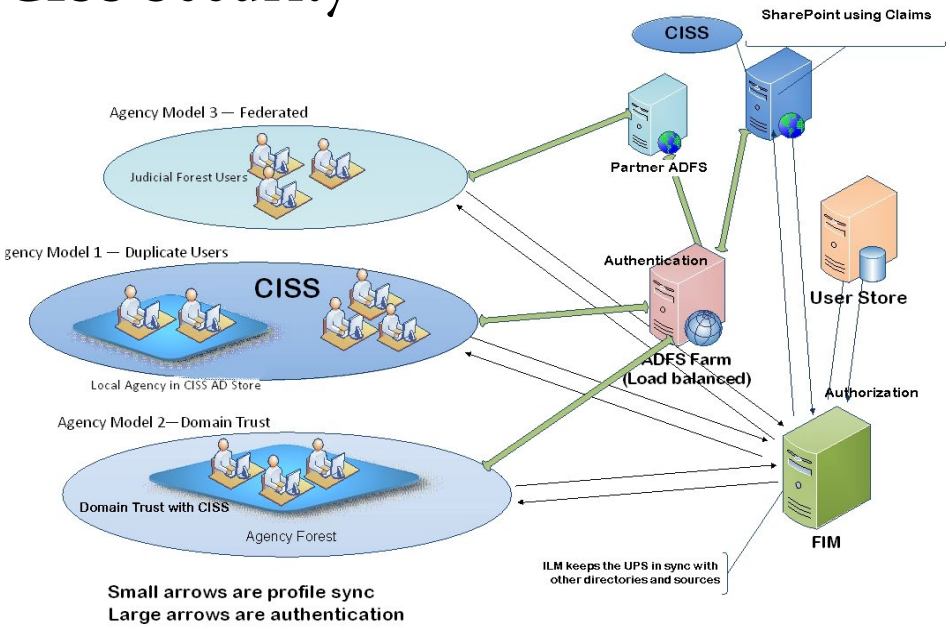
CJIS Governing Board Co-Chairs
Mike Lawlor,
Under Secretary, State of Connecticut OPM
and
Judge Patrick L. Carroll, III

Mike Lawlor, Under Secretary, OPM

IN THIS ISSUE

Agencies Pick Security Models 1
CJIS Governing Board 2
Technology Workshop 3
CJIS Program Overview 3
CISS Updates:
Timeline 4
Technology 4
Business 5
CIDRIS Update 5
OBTS Update 6
FAQs 7

CISS Security



The diagram above outlines the three basic models.

- Model One –The first model is for CISS-Managed Users, which are those who are provisioned in the CISS Active Directory (AD).
- Model Two — The second model is referred to as "Domain Trust." The users in this group are in a domain that CISS trusts (e.g., the Bureau of Enterprise and Systems and Technology or BEST).
- Model Three — The third model, "Federated," is for agencies who either do not support AD or do not wish to directly "trust" CISS. CISS will use Active Directory Federation Services (ADFS) — software and hardware that essentially serves as a translator between an agency database and CISS

As of the end of September, all of the agencies have decided on which model, or models to use. It will not be unusual for some agencies to select multiple models in their organizations.

Changes requiring a shift in the interface method — equipment upgrades, changes in business processes, statute changes, etc. — are inevitable, and so CISS will support security model changes for agencies as necessary.

For more information on CISS' security design, go to www.ct.gov/cjis.

Rick Ladendecker, CJIS Technology Architect, at the September 5th workshop

CISS Tech Workshop: Security, Part 1

The second in a series of workshops for stakeholders was held after the monthly status meeting for CISS on September 5.

Rick Ladendecker, CJIS Technology Architect, explained in depth claims-based security, the rationale for choosing it for CISS, and the various models agencies can use.

CISS Wave 0, Version 1 – First Deliverable is Coming

Mark Tezaris, CJIS Program Manager

As many of you know, the first Connecticut Information Sharing System (CISS) deliverable is the Search of the Offender Based Tracking System (OBTS) with over 140 million offender records using a Google-like search screen. We are calling this Wave 0 version 1 (W0v1). The follow up Wave 0 version 2 (W0v2) will complete the scope for CISS Search of OBTS and may include additional search sources.

The W0v1 encompasses most of the startup work required for a large project like CISS. This includes verification of all of the requirements, security design, search design, architectural design, identifying and ordering hardware, setting up the infrastructure and so forth.

The scope of W0v1 is a subset of the overall scope for Wave 0. At a high level the scope will include the following:

- Basic (i.e., natural-language) and advanced (i.e., fielded) search interfaces, ability to sort and narrow search results, and access to detailed records.
- Access to information contained in OBTS.
- Access to information contained in the CISS Person Index (i.e. Vision Ware MultiVue) based on content obtained from OBTS.
- Data security based on a single GFIPM claim (sworn law enforcement officers).
- Support for CJIS-managed users (i.e. security integration model 1).
- Creation of Audit logs for of login/logout events, searches performed, and records retrieved.

W0v1 will initially allow two Law Enforcement Agencies (LEAs) to log in and use it. Once this initial group uses CISS W0v1 for a short period and gives us their feedback, a rollout schedule will be published and we will continue the rollout to other agencies.

Given the complexity, scale, dependencies of tasks for CISS and the holiday season, the target date for W0v1 production will be moved about two weeks from November 30 to mid-December 2012.

The CISS team is exploring adding additional search sources to OBTS for W0v2. The W0v2 scope and schedule are being finalized and will be published as soon they are completed.

Another effort is underway to create the "wire plan" that is, the high level plan with target dates for the complete CISS phase 1 project contracted with Xerox which includes the Search of CJIS systems , about 60 data exchanges and connection to the current CAD/RMS systems being used by LEAs including State Police. Once complete, we will publish it to the CJIS community. ■

CISS Technology

In September, the CISS project took a couple of big steps forward. The CISS storage subsystems were acquired in September. This storage is the foundation for the entire CISS project supporting the databases and data repositories. The hardware, which can provide electronic document storage into the petabyte range (see box)—is designed for *big data*, meaning documents, images, video, audio. We are also in the process now of acquiring our switches and firewalls. These devices that we refer to as switches in Technical architectures connect computers to each other and to the storage arrays. We hope to have these technologies in place in the next several months. Together—the storage, connectivity, security tools, built-in redundancy, cables, and related hardware—all represents the foundation and framework of CISS from a hardware architectural standpoint.■

~*Rick Ladendecker*

Bytes

http://www.whatsabyte.com

Disk Storage

1 Bit = Binary Digit
8 Bits = 1 Byte
1000 Bytes = 1 Kilobyte
1000 Kilobytes = 1 Megabyte
1000 Megabytes = 1 Gigabyte
1000 Gigabytes = 1 Terabyte
1000 Terabytes = 1 Petabyte
1000 Petabytes = 1 Exabyte
1000 Exabytes = 1 Zettabyte
1000 Zettabytes = 1 Yottabyte
1000 Yottabytes = 1 Brontobyte
1000 Brontobytes = 1 Geopbyte

Processor or Virtual Storage

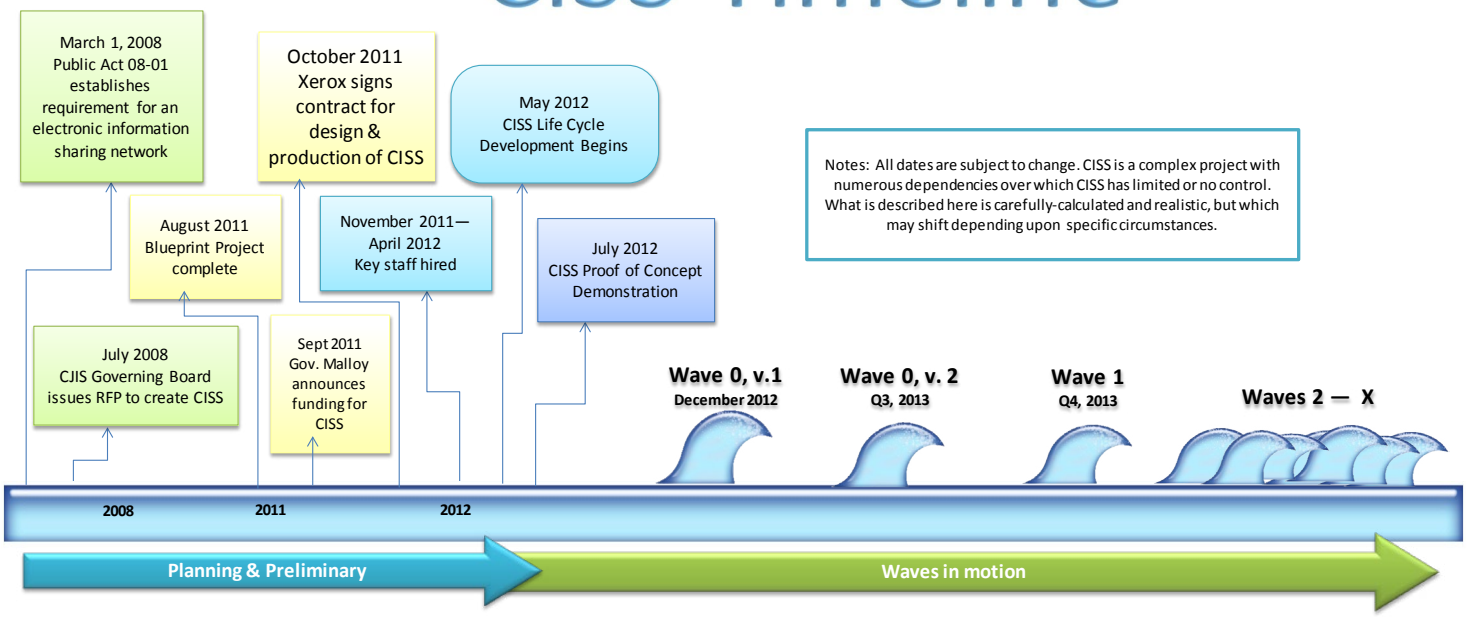
1 Bit = Binary Digit
8 Bits = 1 Byte
1024 Bytes = 1 Kilobyte
1024 Kilobytes = 1 Megabyte
1024 Megabytes = 1 Gigabyte
1024 Gigabytes = 1 Terabyte
1024 Terabytes = 1 Petabyte
1024 Petabytes = 1 Exabyte
1024 Exabytes = 1 Zettabyte
1024 Zettabytes = 1 Yottabyte
1024 Yottabytes = 1 Brontobyte
1024 Brontobytes = 1 Geopbyte

CISS Business

In Brief

- Feedback on CISS screen mock ups was consolidated and distributed to the CISS Workflow Group in preparation for a meeting to finalize the Basic and Advanced Search screens.
- The CJIS Business Team and Collin Evans from the Xerox Team conducted additional GFIPM data source mapping sessions with Judicial for the CRMVS system and with DESPP for the MNI/CCH system that currently send data to OBTS.
- The GFIPM claim documentation has been provided to each agency for review and comments.
- Non-Disclosure Agreements for Employees and Vendors have been drafted for review and approval by the Administrative Committee; with subsequent approval by the CJIS Governing Board at their Quarterly meeting in October. The CJIS Team continues to work on the RMS Vendor Certification ☞

CISS Timeline



continued from previous page

- document to be distributed to the RMS vendors.
- The CJIS and Xerox teams are collaborating on the test and training plans for CISS Wave 0 – Search OBTS.
- **Field Observations** — The CJIS Business Team visited the Meriden, New Britain, and Waterbury courts to observe Division of Criminal Justice business processes in September. The observations were very informative and underlined the need for sharing information electronically between the agencies through the CISS Project.
- Field visits will be scheduled with the Department of Motor Vehicles in the month of October.
- Field visits with the Department of Corrections/Board of Pardons and Parole and the Court Support Services Division will be scheduled over the next couple of months. ■

Nance McCauley

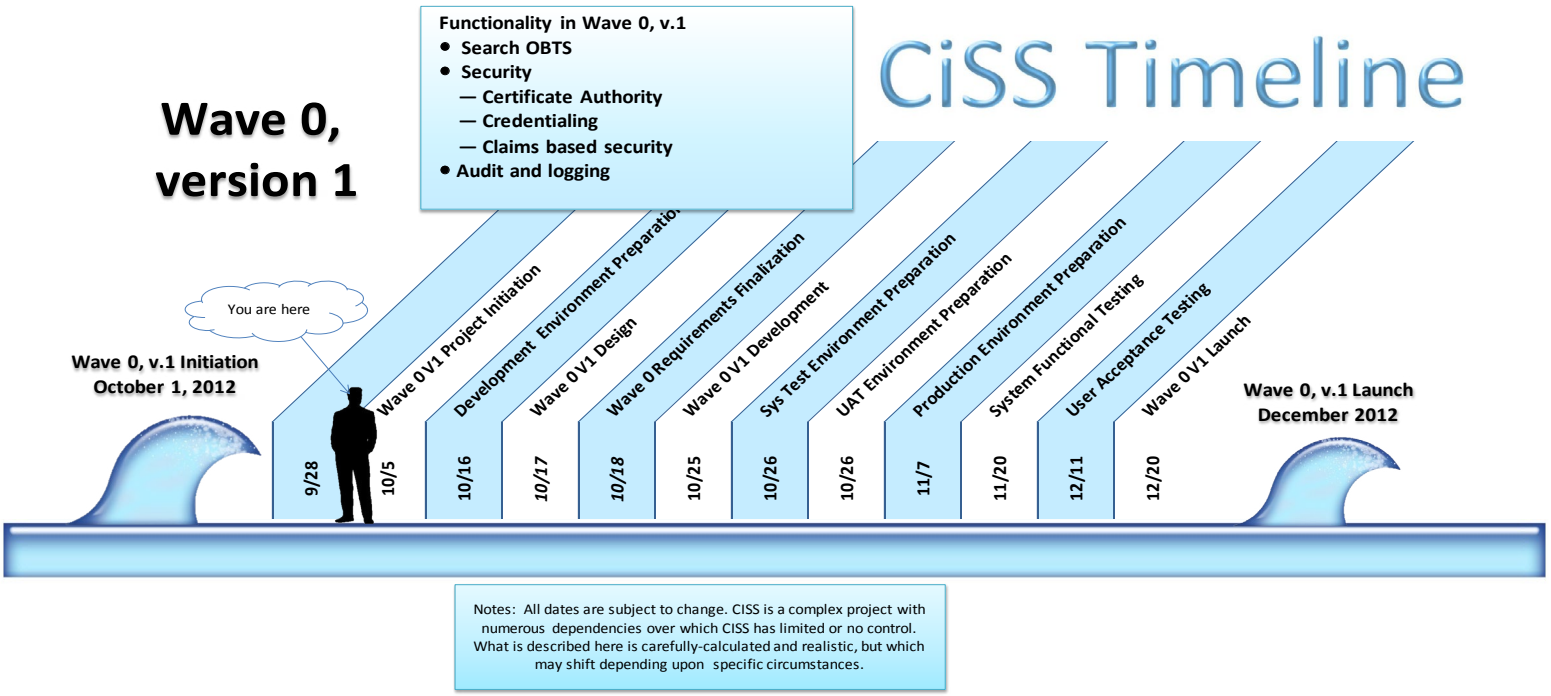
CIDRIS IN BRIEF

John Cook, CIDRIS Project Manager

Just Finished

- CIDRIS is now receiving new message submissions from Troops D, E, F and G. Based on review of OUI submissions across several weeks during August and September; combined activities for each of these troops demonstrate a success rate of approximately 80 percent for initial OUI submissions. This is a substantially higher level than previously reported by earlier Troop implementations.
- Judicial and DESPP worked together to develop a software program to automatically update Surety Bondsman and Insurance data. The new system now provides state police with the most up-to-date information to help troopers conveniently and quickly determine bondsman eligibility status.
- DESPP has updated their CAD-RMS automation system to help streamline OUI submissions. The new software update includes additional software to enhance the document submission process by checking to ensure all attachments selected to be sent to Judicial are accounted for and included in the electronic XML message package.
- CJIS and DMV have completed two CIDRIS system related software updates. One update is designed to support a new case disposition type that will be used to track suspended drivers' licenses and disqualified commercial drivers' licenses. The other update will eliminate duplicative and unnecessary document attachments.

Continued on page 8



OBTS Release 7.3

The OBTS Quarterly Release 7.3 was deployed to production on September 8, 2012. The key changes for this release are:

Enhancements for End Users

- *Exact Name Search Redesign.* The functionality includes moving an application software procedure to execute directly inside the database store to improve inquiry performance.
- *Smart Name Search.* In the May release, the functionality was also moved to execute as a stored procedure. In this release the code was further refined to improve Smart Name inquiry response time.
- *Case Activity*. Event 18 from CRMVS. Modifications were made to correct how the application processes and displays description information located within the inquiry Manager's OBTS Court Case Activities tab.

Enhancements for System Maintenance-Related Activity

- A statistical reports key table was added to the database to improve LogiXML reporting processing speeds.
- Log file storage was enhanced to maintain log files in a central location. This was done to streamline future software deployments.
- A reporting interface was added to help monitor OBTS health status.
- A defect was corrected to allow the application's Message Request Manager (MRM) to start correctly in the event that the State's eDirectory service is not available.

The OBTS support team is currently constructing the deliverables for the 7.4 OBTS quarterly release; deployment is scheduled for November 2012.

Data Purity Initiative Update

The OBTS data purity team has completed a technical review of OBTS/Judicial systems and is currently documenting the findings. In parallel, the team is performing a data comparison and evaluation effort and has identified several data error types that will be corrected in the 7.4 OBTS quarterly release. ■ ~ *Shirley Medeiros*

CISS Technology Workshops

The CJIS Technical Team will be conducting Technology Workshops into the forseeable future for our stakeholders and their technical staff to familiarize them with CISS technology. Several of these technology topics will be divided into varying levels of proficiency to allow stakeholders with differing technical knowledge to absorb the content.

- **CISS Security, Part 2 — Service Oriented Architectures** (SOA) — including NIEM, LEXS, JIEM (October, TBD)
- **SharePoint** — for new, intermediate and power users, including advanced & customization examples for administrators (date TBD)
- **SQL Server** — for new, intermediate & advanced users, covering object broker, SQL Server Integration Services (SSIS), SQL Server Reporting Services (SSRS), SQL Server Analysis Services (SSAS), security, performance
- **Enterprise Service Bus** — WebMethods — Integration for intermediate and advanced technical staff who may be using Software AG's WebMethods products.

We will post workshop dates as they are scheduled. ■

OBTS IN BRIEF

Just Finished

- 7.3 OBTS quarterly release deployed to production on September 8.
- OBTS certification training was conducted at the Judicial's Learning center on September 12. Fourteen students successfully obtained their certification.

Next Month

- Continue constructing deliverables for Release 7.4
- Finalize Release 7.5 deliverables
- Document data purity technical review findings for OBTS/Judicial systems
- Continue data comparison and evaluation exercises
- Use the Nastel performance tool in the Production environment to identify problem areas.

CJIS wants to recognize Lieutenant Mark Panaccione with the DESPP Bureau of Infrastructure, Transportation & Communication and Sergeant Chick Bistany, DESPP Bureau of Communications & Technology, for their assistance with implementation of CIDRIS in the state troop barracks. Because of their efforts, Connecticut's Criminal Justice agencies are now better positioned to begin to coordinate efforts to implement additional electronic forms.

FAQs

Data Replication is going to be an ongoing topic of discussion in coming months. The following is what most mortals need to know about data replication.

Data Replication is the process of copying data from one data source to another while maintaining identical copies of the data that are synchronized.

Extraction, Transformation, and Load (ETL): ETL is the process of extracting data from an environment, transforming elements, and loading the data into another environment.

The ability to access information, from any type of data environment and to replicate it into a common structure, is vital to the success of CISS. The CISS community currently supports data structures ranging from flat and indexed files on IBM and HP mainframe/super-mini systems to databases including SQL Server, Oracle, Microsoft Access; there is even a Lotus Notes application within our world.

Linking connected/disconnected "Clouds of data" into unified target environment(s) with or without naming transformations

- Supports direct integration of legacy data into any relational database
- Facilitates Automated Data Synchronizing
  - Highly customizable
  - Automated failure control
  - Unlimited capabilities including scripting, triggers, external applications
  - Immediate integration with NIEM naming conventions via templates
- Eliminates resources (coding)
  - No legacy coding structures
  - No user-developed coding points of failure
  - Widely utilized technologies (adopted by Federal and State Agencies)
  - Facilitates RAD concepts
  - Single point of maintenance/configuration
- Automates information streams (indexes, partial, incremental, full)
- Supports most commonly used DBs and data file structures
- Oracle, SQL Server, RMS, DB2, VSAM, ISAM, Sequential, Indexed, Adabase, Lotus Notes
- Group entities (agencies, tables, files, etc.)
- Linking connected/disconnected "Clouds of data" into unified target environment(s) with or without naming transformations

There are three options from which Agency Stakeholders can choose to support CISS searching their data environments. The three options give our CISS community flexibility to decide what method to use, each with differing levels of complexity for integration — Federated Search, Agency Replicates Data, and Crawling Agency Data.

Option 1, Federated Search

Data from a stakeholder's environment is accessed from CISS via Web Service query. The CISS Team will work with each agency to create Web Service interfaces to be used by CISS. These services will respond to query requests from CISS, which will generate data extractions via views, stored procedures, or other methods an agency prefers to use.

The selected data will then be returned via the original request, synchronously. Each table to be searched by CISS will require a distinct Web Service.

This Federated Search option requires the most effort by the agency and CISS and impacts the ability of CISS to respond to a query request rapidly. In effect, CISS does not recommend this option unless it is absolutely necessary to interface in this manner. In this scenario, for each search request made by a user within CISS, each of the agencies will be required to respond to a search request via web services and respond with the appropriate data. These queries are for initial and detailed search requests.

As an example: if there are 5,000 search requests (initial or detail) per hour, the agencies using the Federated Search will be required to respond to each request – receive the request, query their data environments,

Continued on page 8

Data Replication, *continued from page 7*

build an XML message, and send the response via web service response. This scenario will significantly impact agency storage throughput, both theirs and the State of Connecticut's network, affects Search response times and is a significant point of maintainability and failure in the Search segment of CISS.

Option 2, Replicated Data

This option requires an effort by an agency to provide a mechanism to extract portions of their data into one of several structures (Database, index or flat file, XML, etc.) and to make the data available to CISS.

Data from a stakeholder's environment is replicated (copied) by the agency and either put on a common network drive for CISS Access, placed on a FTP site for CISS to retrieve, or put into another data environment where CISS can replicate the data. A schedule to support collecting the replicated data will be arranged between CISS and the respective agencies.

Disadvantages to this option include delays in indexing and searching stale data, storage requirements for the agency to "hold" the replicated data and the repetitive process of building container(s) to retrieve updated data records.

If the agency cannot identify the changed records efficiently, then the entire database (only necessary fields) will need to be replicated, repetitively, throughout the day. Lastly, the overhead and impact to re-index all the data from an agency will impact the agency's and CISS's systems and the State of Connecticut's Network.

Option 3, Crawling production data sources

This option is the most efficient scenario and has the lowest impact to the stakeholder's and CISS's environments and minimizes impact to the State of Connecticut's networks. It offers the ability to support agency governance of data, the encryption of data, minimizes network traffic, is a single point of configuration, is auditable, and secure.

To support this option, CISS works with an agency to identify the pertinent data to be replicated (tables, fields, data files, etc.). The agency provides a User ID/Password with Read-Only access to their data environment (SQL, Oracle, O/S) and depending on their environment, may be required to install a listener service on their system. This listener service applies to VAX/Alpha systems and IBM environments using VSAM/ISAM for their data file structures. Oracle and SQL Server environments require only access to their respective Database's IP Port Number (Oracle=1521, SQL Server=1433).

Crawling production data sources CISS to scan the agency's selected data environments on a predetermined schedule. Data environments which have a large number of changes or additions and/or have data where the nature of the information is relevant and subject to change will be scanned more frequently. Environments which have infrequent updates will be scanned infrequently. The frequency in either scenario depends on the size of the database, the nature of the data and necessity to have visibility to the data.. ▪

CIDRIS, *continued from page 5*

CIDRIS — Next Month

- DESPP is developing an electronic coversheet to help reconcile CIDRIS OUI documents with their paper equivalents. The new coversheet provides several benefits including a PDF document format that is user friendly and can be printed on demand.
- Judicial is planning to pilot a new CJIS Forms-Viewer application. The CJIS Forms Viewer is a new web-based application that allows authorized CIDRIS stakeholders to view, retrieve, and print agency documents by UAR and Misdemeanor Ticket Numbers. After testing is complete, the implementation team will continue work to expand CIDRIS to support additional stakeholders.

CIDRIS — Next Three Months

- CJIS staff to continue review of paper document submissions to promote continual improvement processes for the DESPP, Judicial and DMV agencies. Consideration will also be place on developing additional forms that can be used in place of scanned document images. ■