CJiS

Global Federated Identity & Privilege Management (GFIPM)

Implementation in the

Connecticut Information Sharing System (CISS)

Table of Contents

Introduction

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 there is a mix of new and old systems that are unable to communicate with one another. Governance structures, the separation of state and local government, 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. To further complicate this situation, the varying age and differences in security frameworks of these agencies' systems adds to the constraints.

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, and funded jointly by the U.S. Department of Justice (DOJ) and the U.S. Department of Homeland Security (DHS), enables information sharing for state and local agencies through a federated model that is secure, scalable, and cost-effective." [1]

The **Global** part of GFIPM is the Global Justice Information Sharing Initiative. It serves as a Federal Advisory Committee (FAC) and advises the U.S. Attorney General on justice information sharing and integration initiatives. Global was created to support the broad scale exchange of pertinent justice and public safety information. It promotes standards-based electronic information exchange to provide the justice community with timely, accurate, complete, and accessible information in a secure and trusted environment.[2]

A **Federation** is a group of two or more partners who trust each other, and have business and technical agreements allowing a user from one federation partner to seamlessly access resources from another partner in a secure and trustworthy manner.

Identity is the authorization process of the user, including attributes that can identify the user.

Privilege refers to the list of privileges, or access restrictions based on some combination of the user characteristics, such as rank and certifications. A set of authorization context attributes are defined based on some general data categories by Identity Providers (IDPs) (a third party trusted authority) based on the user's job

[1] *About the GFIPM Program*. http://www.gfipm.net/about/.

[2] https://it.ojp.gov/global

function and a minimal set of well-understood eligibility requirements.

Management pertains to the administration and supervision of these standards.

Benefits

There are many benefits to using the GFIPM model with CISS. Secure federated and trusted domains can decrease the propagation of personal identity information, reduce the redundant capture and storage of personal identity information, and depersonalize data exchanges across domains.[3]

Other benefits include:

1. **Security** – ensures a more secure level of authorization.
2. **Standardized Security Specifications** – provides a standard framework for the authentication process.
3. **Information Sharing** – facilitates information sharing between federated agencies.
4. **Dynamic Account Provisioning** –Using a login, dynamic account provisioning will eliminate the need for manual account setup between the user and CISS during the account provisioning process.
5. **Dynamic Account Updates** – ensure that important changes to user data (such as a change in the user's rank or privilege information) are made available from IDPs to CISS quickly, thereby helping to ensure that a user's local account is current.
6. **Federated Privilege Management** – facilitates assignment of users to claims. CISS can use information in a user's trusted metadata to quickly grant to the user access to information that they need.
7. **Audit Logs** – stores information that can be used to build very comprehensive audit logs containing the user's identity and actions. It can also be used to gather and construct statistics models.

[3] *Global Federation Identity and Privilege Management (GFIPM) Security Interoperability Demonstration*, Georgia Tech Research Institute. https://it.ojp.gov/documents/GFIPM_Security_Interoperability_Demonstration_Project_Report_2007-08-30.pdf. Page 19.

The Federated System

How the Federated System Works

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. " [4] For the CISS project, the federation partners are the criminal justice agencies and organizations.

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 can disseminate or 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 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 (Figure 1). The federation in this case is 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

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

the identity and citizenship of the passport holder and confirmed their information.

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.

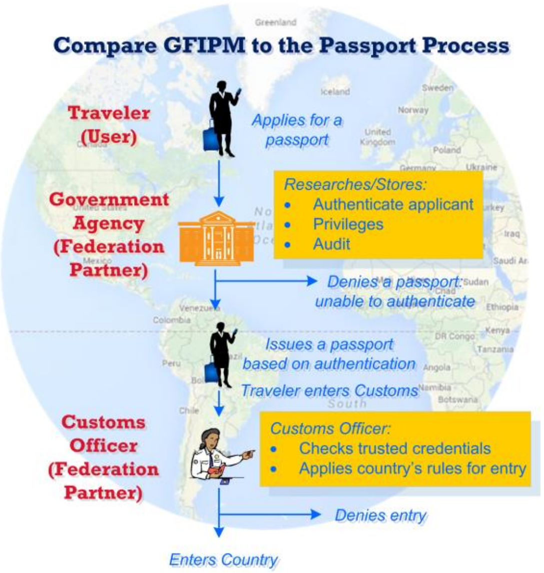
Compare GFIPM to the Passport Process
Traveler (User)
Applies for a passport
Government Agency (Federation Partner)
Researches/Stores:
• Authenticate applicant
• Privileges
• Audit
Denies a passport: unable to authenticate
Issues a passport based on authentication
Traveler enters Customs
Customs Officer (Federation Partner)
Customs Officer:
• Checks trusted credentials
• Applies country's rules for entry
Denies entry
Enters Country

Figure 1. Passport authentication process.

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 that 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.

Understanding Claims

GFIPM Components

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)** – (Authorization service)
- **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."[5] For the CISS project, the Identity Provider will be a service that will authorize claims that are stored in a database for each 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.[6] 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."[7] Within the metadata are the claims.

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

[5] 5, *Global Federated Identity & Privilege Management*. Justice Information Sharing, US Department of Justice, Office of Justice Programs, National Initiatives. http://it.ojp.gov/gfipm.

[6] 6 *Global Federated Identity & Privilege Management*. Justice Information Sharing, US Department of Justice, Office of Justice Programs, National Initiatives. http://it.ojp.gov/gfipm.

[7] 7 *Metadata*. Taken from Whatis. http://whatis.techtarget.com/definition/metadata.

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.

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 (Figure 2). 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.

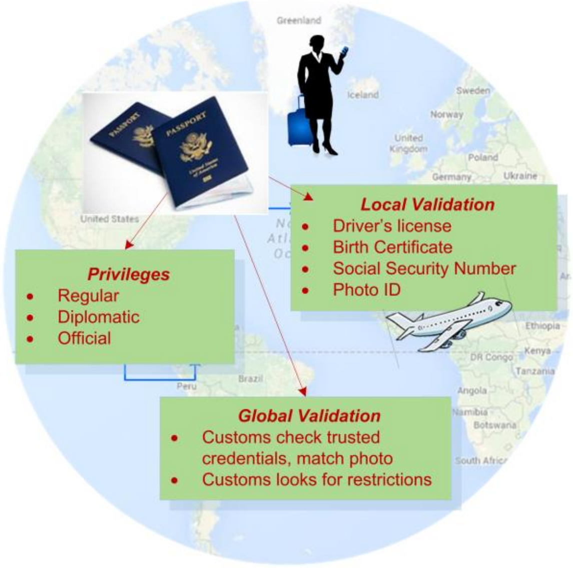

Figure 2. Claims and passport security.

Roles versus Claims

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

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.

Claims Authentication

Just as federated claims in the passport process provide security and claims authorization on travelers systematically, they also provide security and claims authorizations when a user attempts to access CISS.

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

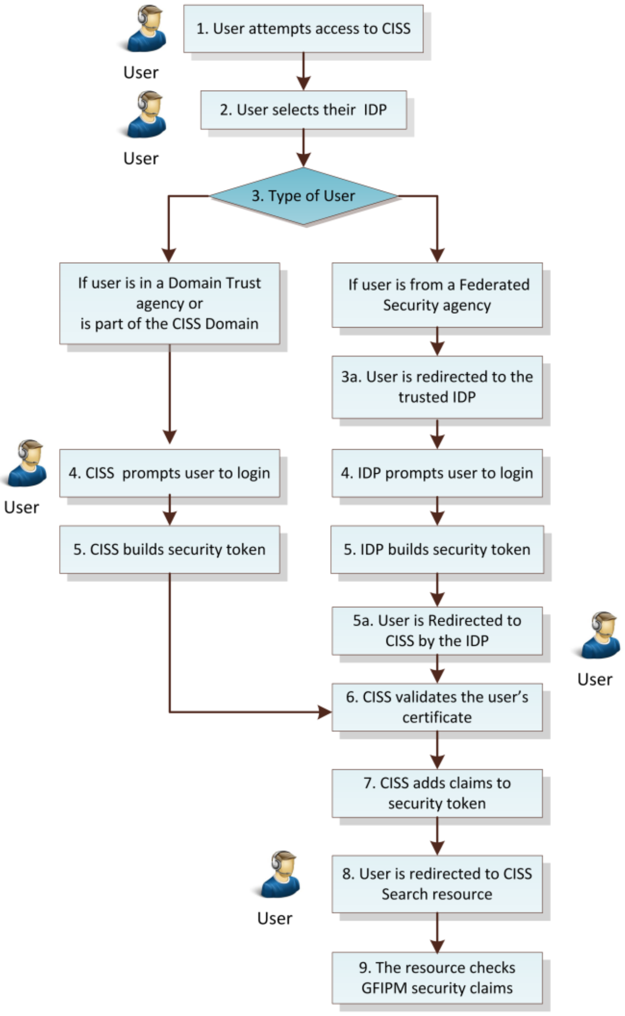
User
1. User attempts access to CISS
User
2. User selects their IDP
3. Type of User
If user is in a Domain Trust agency or is part of the CISS Domain
If user is from a Federated Security agency
3a. User is redirected to the trusted IDP
User
4. CISS prompts user to login
4. IDP prompts user to login
5. CISS builds security token
5. IDP builds security token
5a. User is Redirected to CISS by the IDP
User
6. CISS validates the user's certificate
7. CISS adds claims to security token
User
8. User is redirected to CISS Search resource
9. The resource checks GFIPM security claims

Figure 3. Authentication process.

Figure 3 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**).

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 structured repository of information on people and resources within an organization) that is hosted in CISS and authenticated by a CISS security service. If 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** agency, 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**).

Assigning Claims to Users

Users are assigned claims by their agency authorized administer(s). The claims consist of credentials and privileges that will make up their user profile. These claims provide authorization to search data sources and receive information from participating criminal justice agencies and organizations using a single login process.

The User Assignment Process

Within each agency, there will be authorized administrator(s) who will assign one or more of the GFIPM claims to their agency users' profiles, depending on their credentials and privileges. Users may have more than one claim attached to their user profile. The profiles 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.

The four GFIPM claims currently being assigned to users 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. 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. This would include users from any agency or branch that is represented in the CJIS Governing Board. The other three claims are more restrictive based on privileges and security clearance.

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.

As the CISS project progresses, more GFIPM claims will be added and assigned to users.

Mapping Data Elements to Claims Classifications

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

All data is being assigned to GFIPM claims classifications by agencies who own the data, based on their interpretation of the sensitivity of the data that will be accessed by the CJIS community (Figure 4). 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 fields) in the records to specific GFIPM 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

Public Data

Public Data is any information that is permitted to be released to the public and not subject to controlled unclassified information (CUI) access restrictions.

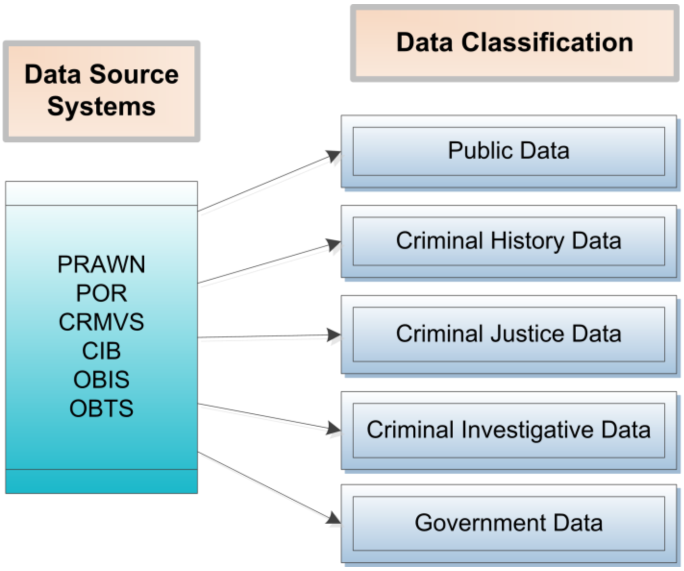

Figure 4. Classifying data from source systems.

Government Data

Government Data is any data obtained by a government agency pursuant to an administrative, legal, or investigative function in furtherance of the official duties or functions of the agency.

Criminal Justice Data

Criminal Justice Data is data from law enforcement agencies, administrative agencies, courts, and correction agencies regarding arrest, 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.

Criminal History Data

Criminal History Data is any information collected by criminal justice agencies on individuals that consists of identifiable descriptions and notations of arrests, detentions, indictments, informational notes, or other formal criminal charges, and any disposition arising from them, including sentencing, correctional supervision, and/or release. The term does not include identification information, such as fingerprint records, to the extent that such information does not indicate involvement of the individual in the criminal justice system.

Criminal Investigative Data

Criminal Investigative Data is information obtained from a variety of sources (public, governmental, confidential, etc.). The information may be utilized to further an investigation or could be derived from an investigation.

Classifying Data

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.❖