CJIS-CT CLAIMS SECURITY MODEL

Global Federated Identity and Privilege Management Implementation in the Connecticut Information Sharing System

Anatolie Criucov, Solutions Architect, MPA
anatolie.criucov@ct.gov

This page intentionally left blank

Contents

REVISION HISTORY:

Date	Version	Description	Author
10/16/2024	1.0	Initial draft	Anatolie Criucov
10/16/2024	1.1	Added updated data classification, SLEO definition	Tammi Harris
10/16/2024	1.2	Enhanced Agency Security	Sean Bucher/Tammi Harris/Anatolie Criucov

ABSTRACT

The Connecticut Information Sharing System (CISS) has revolutionized how criminal justice agencies securely share data across the state. By using the Global Federated Identity and Privilege Management (GFIPM) model, CISS enables authorized users to access critical information seamlessly, while maintaining tight control over sensitive data. Through claims-based authentication, users no longer need to manage multiple logins - just one set of credentials grants access to the information they need, tailored precisely to their role. This document explores how GFIPM enhances security, streamlines data sharing, and improves overall efficiency. It also looks at how dynamic claims-based access provides a more secure and flexible framework than traditional role-based systems. With growing demands for better data protection and sharing, this model is poised to continue strengthening Connecticut's justice system, with future enhancements on the horizon to further improve its security, functionality, and integration with national systems.

1. INTRODUCTION

The Connecticut criminal justice ecosystem has experienced significant advancements in recent years. Prior to these transformations, the system was fragmented due to the lack of standardized technology and protocols across state and local agencies. These agencies independently acquired software and hardware, resulting in systems that could not communicate seamlessly. Consequently, sharing critical criminal justice data was difficult, and managing identity and access controls across these disparate systems was inefficient.

With an increased focus on cybersecurity and the need for better interoperability, the **Connecticut Information Sharing System (CISS)** implemented the **Global Federated Identity and Privilege Management (GFIPM)** model. GFIPM facilitates secure, scalable, and cost-effective data sharing across multiple agencies by enabling a federated trust model. This allows agencies to maintain their independent systems while participating in a unified framework that provides seamless access to resources.

With **claims-based authentication**, CISS ensures that authorized users can access sensitive information from other agencies without having to manage multiple logins. Claims represent specific permissions tied to a user's role and access rights, providing a secure way to control data access at a granular level.

2. GFIPM OVERVIEW

What is GFIPM? The **Global Federated Identity and Privilege Management (GFIPM)** model was developed to improve the interoperability and security of criminal justice information systems across the United States. It provides a standardized framework for identity management that is federated across multiple agencies. This federated approach ensures that users can authenticate once and access the data and systems they need, without requiring multiple credentials.

By implementing **GFIPM**, Connecticut can connect various agencies such as the Department of Emergency Services and Public Protection (DESPP), Department of Motor Vehicles (DMV), Division of Criminal Justice, Judicial Branch, and others, enabling secure data sharing without duplicating identity information.

3. BENEFITS OF GFIPM IN CISS

The GFIPM model offers several significant benefits to CISS and the criminal justice agencies participating in the system:

3.1. ENHANCED SECURITY

GFIPM’s claims-based approach allows for precise access control. Instead of broad user roles, claims specify the exact data and resources a user can access. This ensures that sensitive information is only available to authorized personnel.

3.2. STREAMLINED AUTHENTICATION

Through **federated identity management**, users no longer need to manage multiple credentials. A single sign-on process ensures that users authenticated by their home agency can access resources in other agencies. For instance, a law enforcement officer authenticated by DESPP can access DMV records without additional logins.

3.3. IMPROVED INFORMATION SHARING

GFIPM facilitates the secure sharing of information between agencies, without exposing personal identity information unnecessarily. This is crucial for ensuring that sensitive data such as criminal history or investigative reports remain protected.

3.4. DYNAMIC USER PROVISIONING

GFIPM allows for dynamic provisioning and de-provisioning of user accounts. As user roles change or as new staff are hired, the claims associated with their identity are updated automatically to reflect their access rights. This reduces the administrative burden and ensures that user access is always up to date.

3.5. AUDIT AND COMPLIANCE

GFIPM supports comprehensive auditing and logging, providing a detailed record of who accessed which data and when. This is important for ensuring compliance with legal requirements and for maintaining accountability across the system.

4. THE FEDERATED IDENTITY SYSTEM

What is a Federation? A **Federation** refers to a trusted group of agencies that agree to share data securely. These agencies, known as **Identity Providers (IDPs)** and **Service Providers (SPs)**, establish business and technical agreements that govern how data is accessed and shared. In Connecticut, agencies participating in CISS form part of this federation.

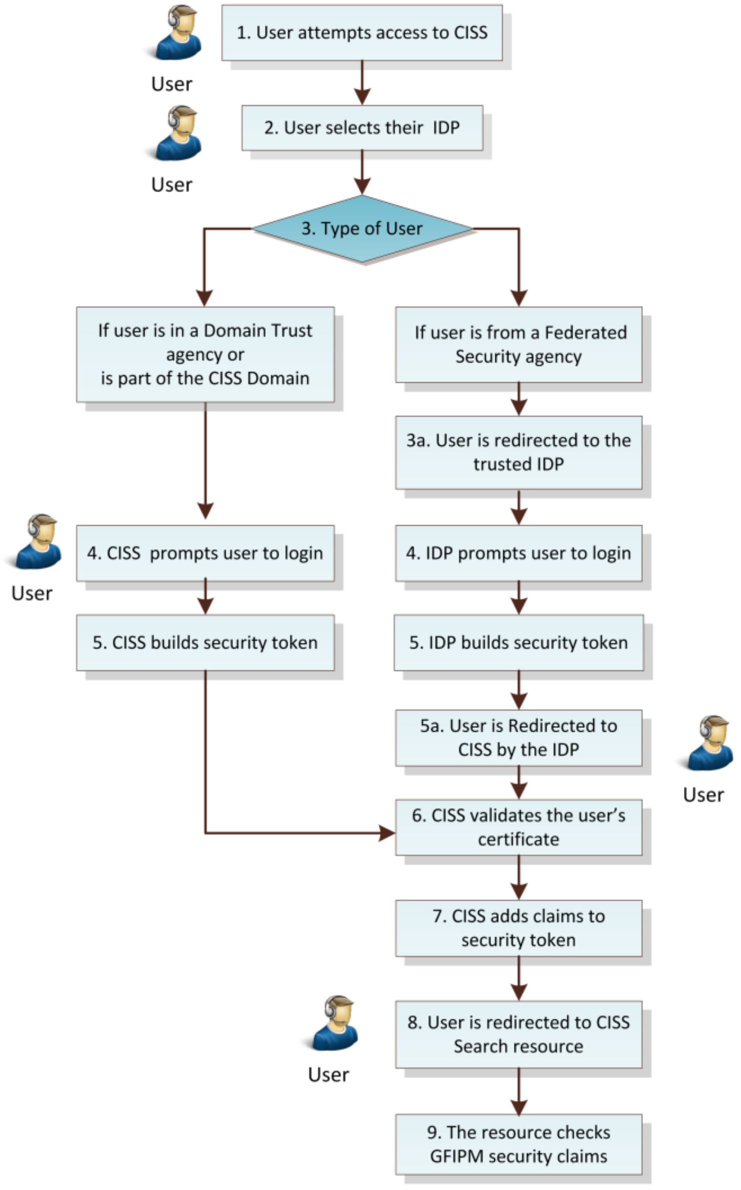
Federation Components:

- **Identity Providers (IDPs)**: These entities are responsible for authenticating users and issuing claims that define what data the user can access.
- **Service Providers (SPs)**: CISS acts as a service provider that consumes the claims issued by the IDPs. Based on these claims, CISS determines which data the user can access.

4.1. HOW THE FEDERATION MODEL WORKS

In the federated model:

1. **Agency A's Identity Provider** authenticates the user and issues claims about their identity and access rights.
2. The user then accesses CISS, which serves as a **Service Provider**.
3. **CISS** evaluates the claims to determine what data can be shared with the user, based on their role and clearance.
4. The user is granted access to the requested data if they hold the necessary claims.


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

Picture 1. Authentication Process

This model ensures that data access is based on a standardized set of claims, reducing the complexity of managing access across multiple systems.

5. GFIPM CLAIMS MODEL

What Are Claims? Claims are assertions about a user's identity, role, or access rights. In GFIPM, claims are used to control what data a user can access. Each claim represents specific permission and is issued by an Identity Provider.

Example of Claims in CISS:

- **Public Data Claim**: Grants access to public, non-classified data such as warrant information or inmate records.
- **Sworn Law Enforcement Officer Indicator Claim**: designated for full-time employees of recognized law enforcement agencies who are certified by the state (e.g., POST) and possess arrest authority. This claim ensures that only officers who meet these criteria can access sensitive data necessary for law enforcement operations.
- **Criminal Justice Data Claim**: Provides access to sensitive criminal justice data, including arrest records, investigations, and court rulings.
- **Weapons Data Claim**: Allows access to restricted weapons-related data, typically used by law enforcement officers.
- **Wanted File Data Claim**: Grants access to active warrant information.

These claims ensure that users can only access the information relevant to their role, minimizing the risk of unauthorized data exposure.

6. ASSIGNING AND MANAGING CLAIMS

Claims are assigned to users by administrators at their home agencies. Each user's claims are stored in their profile within CISS, and the system dynamically updates these claims as the user's role or privileges change.

6.1. THE PROCESS OF ASSIGNING CLAIMS

1. **User Authentication**: The user logs into the system through their agency's Identity Provider.
2. **Claims Issuance**: The Identity Provider generates a set of claims based on the user's role, security clearance, and access needs.
3. **Claims Evaluation**: CISS evaluates the claims to determine what data the user can access.
4. **Data Access**: If the user holds the necessary claims, they are granted access to the requested data.

This process ensures that access is granted based on precise permissions, reducing the risk of unauthorized data access.

6.2. ENHANCED AGENCY SECURITY

To reduce the risk of unauthorized access to sensitive information, the enhanced security functionality enables CISS System Administrators to define the set of allowable security claims for users. This list of allowable claims is agreed upon by all data owners and consuming agencies to maintain alignment and security standards. If a particular claim is restricted, it cannot be assigned by users with administrative privileges within the system. This approach guarantees that only authorized claims are available for assignment, minimizing the possibility of accidental or deliberate misconfiguration.

A full list of allowable claims per each agency can found in APPENDEX A.

As an example, DMV allowable and agreed upon list of claim is:

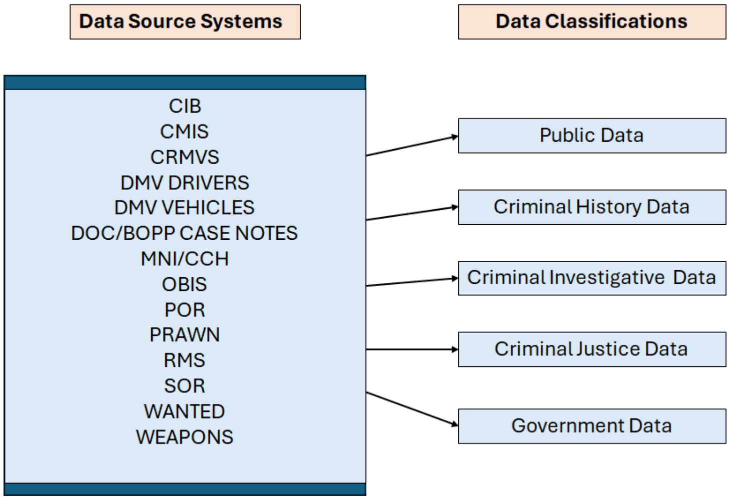
- Public Data Claim
- Government Data Claim
- Criminal Justice Data Claim
- Criminal History Data Claim

7. SECURITY IMPLICATIONS OF GFIPM

The implementation of GFIPM within CISS brings several security advantages:

7.1. ROLE-BASED VS. CLAIMS-BASED SECURITY

Traditional systems often use **role-based access control (RBAC)**, where users are assigned broad roles such as "Analyst" or "Officer." However, this approach is limited because roles are often too general, allowing users to access more data than necessary. GFIPM, in contrast, uses **claims-based access control**, where each claim specifies exactly what data a user can access. This allows for more granular control over data access.



Picture 2. Classifying Data from Source Systems

7.2. DATA CLASSIFICATION

In CISS, all data elements are classified according to their sensitivity. For instance:

- **Public Data** is any information that can be accessed by the public, such as non-sensitive court records.
- **Criminal Justice Data** includes arrest records, court rulings, and sentencing information, accessible only to authorized personnel.
- **Criminal Investigative Data** pertains to ongoing investigations and is highly restricted. By mapping data elements to specific claims, CISS ensures that users can only access the data they are authorized to view.

7.3. AUDIT LOGS AND MONITORING

Every time a user accesses data through CISS, their actions are logged. These audit logs provide a detailed record of who accessed what data and when, ensuring that agencies can monitor and review access patterns to detect any suspicious activity.

8. PRACTICAL USE CASES FOR GFIPM CLAIMS IN CISS

To illustrate how GFIPM works in practice, consider the following examples:

8.1. LAW ENFORCEMENT OFFICER ACCESSING ARREST RECORDS

An officer from DESPP needs to access arrest records held by the Judicial Branch. Upon logging into CISS, the officer's Identity Provider (DESPP) issues a **Criminal Justice Data Claim**. CISS evaluates this claim and grants the officer access to the arrest records, allowing them to view only the data they are authorized to access.

8.2. DMV ADMINISTRATOR ACCESSING VEHICLE DATA

A DMV administrator requires access to vehicle registration data. Upon login, the administrator's Identity Provider issues a **Government Data Claim**. CISS evaluates this claim and grants the administrator access to the DMV's vehicle registration data, but not to any criminal justice data.

8.3. COURT CLERK ACCESSING PUBLIC DATA

A court clerk needs to view publicly available case information. Their Identity Provider issues a **Public Data Claim**, which CISS uses to determine that the clerk can access non-classified court records, but not sensitive criminal justice or investigative data.

9. MAPPING DATA ELEMENTS TO CLAIMS

Each data element within CISS is assigned a security classification based on its sensitivity and relevance to specific claims. This ensures that users only receive access to the data they are authorized to view. The process of mapping data elements to claims is done by the CJIS Business team in collaboration with the agencies that own the data. Each data source is evaluated, and business rules are applied to determine the appropriate claim classification.

9.1. DATA CLASSIFICATIONS IN CISS

- **Public Data**: Data that can be freely accessed without restrictions, such as court rulings or public inmate information. Users with the **Public Data Claim** can access this information.
  - *Examples*: PRAWN Active Warrants, OBIS Inmate Records, CRMVS.
- **Government Data**: Data collected by a government agency during its administrative or legal functions. Only users with the **Government Data Claim** can access this information.
  - *Examples*: DMV Vehicle/Boat Registration Data, Driver's License Data.
- **Criminal Justice Data**: Sensitive data related to arrests, investigations, convictions, and sentencing. This data is typically restricted to law enforcement officers and other authorized users.
  - *Examples*: DOC/BOPP Case Notes, DESPP Sex Offender Registry, Local Law Enforcement RMS.
- **Criminal History Data**: Information about an individual's formal criminal charges, detention, sentencing, and correctional supervision. Only users with the **Criminal History Data Claim** can view this information.
  - *Examples*: MNI-CCH, POR.
- **Criminal Investigative Data**: Data obtained during or derived from an ongoing criminal investigation. This data is highly restricted and can only be accessed by users with the **Criminal Investigative Data Claim**.
  - *Examples*: Criminal Law Enforcement RMS Data.
- **Criminal Intelligence Data**: Information related to criminal activity that has been evaluated and meets the criteria for inclusion in a criminal intelligence system. Access is limited to those with the **Criminal Intelligence Data Claim**.
  - *Examples*: Regional Information Sharing Systems, Joint Regional Information Exchange System.
- **Youthful Offender Data**: This custom claim is specific to CISS and pertains to individuals with youthful offender status. Only users with both the **Youthful Offender Data Claim** and another relevant claim (such as Criminal Justice Data) can access this information.
  - *Examples*: OBIS Inmate Records, CRMVS Limited Information.
- **Sworn Law Enforcement Officer indicator: (SLEO)** claim is designated for full-time employees of recognized law enforcement agencies who are certified by the state (e.g., POST) and possess arrest authority. This claim ensures that only officers who meet these criteria can access sensitive data necessary for law enforcement operations.
  - Examples: MNI-CCH (Master Name Index-Computerized Criminal History), PRAWN, Weapons, DOC/BOPP Case Notes, CMIS Probation Data, DMV Driver Photos, OBIS (Inmate Records).

10. CUSTOM CLAIMS IN CISS

CISS has also implemented several custom claims to meet the unique needs of Connecticut's criminal justice community. These custom claims include:

- **Weapons Data Claim**: This claim allows access to weapons-related data, including records from the NCIC Weapons Database. Access to this claim is restricted to law enforcement officers, dispatchers, and authorized personnel involved in criminal investigations.
  - *Data Sources*: NCIC Weapons Database, DESPP Weapons Database.
- **Wanted File Data Claim**: This claim grants access to data on individuals with active warrants. Like Weapons Data Claim, access is restricted to law enforcement officers and investigators with appropriate clearance.
  - *Data Sources*: CT WANTED, DESPP.
- **Criminal Justice Data Agency Edit Privilege Claim**: This claim is granted to users who have the authority to edit criminal justice data on behalf of their agency. These users can annotate, redact, or update documents within CISS, ensuring the accuracy and security of shared information.

Data Sources: CISS Electronic Content Management System (Document Repository).

11.CASE STUDY: HOW GFIPM ENHANCES SECURITY AND EFFICIENCY

To better understand how GFIPM claims improve security and efficiency, let's explore a real-world scenario within CISS.

11.1. SCENARIO: LAW ENFORCEMENT INVESTIGATION

An officer from DESPP is investigating a suspect with an active arrest warrant. The officer logs into CISS, and their Identity Provider (DESPP) authenticates them. Based on the officer's role and clearance level, the Identity Provider issues the following claims:

- **Criminal Justice Data Claim**
- **Wanted File Data Claim**
- **Weapons Data Claim**

CISS evaluates these claims and grants the officer access to the relevant data sources, such as the active warrant information from the PRAWN system and weapons data from the NCIC database. This seamless access ensures that the officer can gather all necessary information without needing to request access from multiple systems or agencies.

11.2. SCENARIO: COURT CLERK ACCESSING PUBLIC RECORDS

A court clerk needs to review public case information for administrative purposes. Upon logging into CISS, their Identity Provider issues a **Public Data Claim**. CISS evaluates this claim and grants the clerk access to public records, such as court rulings and non-sensitive inmate information. However, the clerk is restricted from accessing criminal investigative or criminal justice data, as their role does not authorize them to view this information.

12.FEDERATED IDENTITY FLOW IN CISS

To better illustrate how claims and federated identity work within CISS, here's a step-by-step flow of the process:

12.1. FEDERATED IDENTITY FLOW

[User from Agency **A**]→ [Agency **A**'s IDP] → [Authentication & Claims Issuance] → [CISS (SP)] → [CISS Verifies Claims] → [**Access Data in Agency B**]

12.2. CLAIMS AUTHENTICATION PROCESS

[User Logs In] → [Identity Provider] → [Claims Issuance] → [Security Token Created] → [CISS Verifies Claims] →[**Access Granted**]

This visual representation shows how a user's claims are issued by their home agency (Identity Provider), evaluated by CISS (Service Provider), and used to grant access to data held by other agencies.

13.SECURITY CONSIDERATIONS FOR FEDERATED IDENTITY AND CLAIMS

13.1. CLAIMS-BASED ACCESS CONTROL VS. ROLE-BASED ACCESS CONTROL

The use of claims-based access control (CBAC) in CISS provides several advantages over traditional role-based access control (RBAC). In RBAC, users are assigned broad roles, such as "analyst" or "officer," which often grant more access than necessary. In contrast, CBAC allows for more precise control over what specific data a user can access based on their claims. This reduces the risk of unauthorized access to sensitive information.

13.2. REAL-TIME CLAIM EVALUATION

One of the key benefits of GFIPM in CISS is the ability to evaluate claims in real-time. As soon as a user logs into the system, their claims are issued and evaluated based on their current role and clearance. This ensures that users can only access the data they are authorized to view, even if their role or clearance changes over time.

13.3. DATA PROTECTION AT THE RECORD LEVEL

By mapping each data element to specific claims, CISS ensures that data protection is enforced at the record level. For example, a user with access to criminal justice data may only see certain parts of a record, while more sensitive information, such as criminal investigative data, remains hidden unless the user holds the appropriate claims.

14.FUTURE ENHANCEMENTS TO GFIPM IN CISS

As CISS continues to evolve, there are several potential enhancements to the GFIPM model that could further improve security and efficiency:

14.1. EXPANDED USE OF CUSTOM CLAIMS

In addition to the existing custom claims (e.g., Weapons Data, Wanted File Data), CISS could introduce new claims for other sensitive data types, such as mental health records or juvenile records. These custom claims would provide even more granular control over who can access specific types of sensitive information.

14.2. INTEGRATION WITH NATIONAL SYSTEMS

CISS could also explore opportunities to integrate GFIPM with national criminal justice systems, such as the **National Crime Information Center (NCIC)** and the **National Data Exchange (N-DEx)**. This would enable Connecticut agencies to securely share data with federal partners while maintaining strict control over who can access the information.

14.3. ENHANCED AUDIT AND REPORTING CAPABILITIES

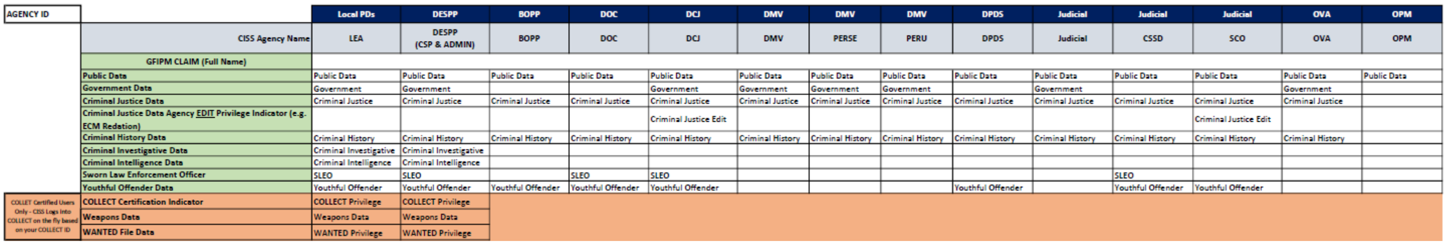
Future updates to CISS could include more advanced auditing and reporting features, allowing agencies to monitor access patterns and detect potential security risks in real time. These enhanced features would provide even greater transparency and accountability within the system.

15.CONCLUSION

The implementation of **GFIPM** in the **Connecticut Information Sharing System (CISS)** has revolutionized the way criminal justice information is shared across agencies. By using a **claims-based access control model**, CISS ensures that sensitive data is only accessible to authorized personnel, while facilitating seamless data sharing between agencies. The addition of custom claims for sensitive data types, such as **Weapons Data** and **Wanted File Data**, further enhances the security of the system.

As CISS continues to grow and evolve, the GFIPM model will remain a critical component in ensuring the security and efficiency of Connecticut's criminal justice information sharing system. By adopting a federated identity approach, CISS can continue to provide users with the access they need, while protecting sensitive information from unauthorized access.

APPENDIX A



AGENCY ID		Local PDs	DESPP	BOPP	DOC	DCJ	DMV	DMV	DMV	DPDS	Judicial	Judicial	Judicial	OVA	OPM
	CISS Agency Name	LEA	DESPP (CSP & ADMIN)	BOPP	DOC	DCJ	DMV	PERSE	PERU	DPDS	Judicial	CSSD	SCO	OVA	OPM
	GFIPM CLAIM (Full Name)														
	Public Data	Public Data	Public Data	Public Data	Public Data	Public Data	Public Data	Public Data	Public Data	Public Data	Public Data	Public Data	Public Data	Public Data	Public Data
	Government Data	Government	Government			Government	Government	Government	Government		Government			Government	
	Criminal Justice Data	Criminal Justice	Criminal Justice	Criminal Justice	Criminal Justice	Criminal Justice	Criminal Justice	Criminal Justice	Criminal Justice	Criminal Justice	Criminal Justice	Criminal Justice	Criminal Justice	Criminal Justice	
	Criminal Justice Data Agency EDIT Privilege Indicator (e.g. ECM Redation)					Criminal Justice Edit							Criminal Justice Edit		
	Criminal History Data	Criminal History	Criminal History	Criminal History	Criminal History	Criminal History	Criminal History	Criminal History	Criminal History	Criminal History	Criminal History	Criminal History	Criminal History	Criminal History	
	Criminal Investigative Data	Criminal Investigative	Criminal Investigative												
	Criminal Intelligence Data	Criminal Intelligence	Criminal Intelligence												
	Sworn Law Enforcement Officer	SLEO	SLEO		SLEO	SLEO						SLEO			
	Youthful Offender Data	Youthful Offender	Youthful Offender	Youthful Offender	Youthful Offender	Youthful Offender				Youthful Offender		Youthful Offender	Youthful Offender		
COLLET Certified Users Only - CISS Logs Into COLLECT on the fly based on your COLLECT ID	COLLECT Certification Indicator	COLLECT Privilege	COLLECT Privilege												
	Weapons Data	Weapons Data	Weapons Data												
	WANTED File Data	WANTED Privilege	WANTED Privilege												

APPENDIX B

For further details on GFIPM claims and their classifications, see the full “CISS GFIPM Claim Definitions_Approved_Final.docx”.

For additional reference materials, visit the GFIPM Overview from the U.S. Department of Justice: **https://it.ojp.gov/gfipm**.

Global Federated Identity and Privilege Management (gfipm.net)