Connecticut Information Sharing System

Security 101

April 23, 2014

Agenda

- No one leaves here today without understanding how your agency data is secured within CISS
- Brief CISS Overview
- How Data is shared and secured
- So what is GFIPM really?
- CISS Security Implementation

What is CISS (in a nutshell)?

Search Tool

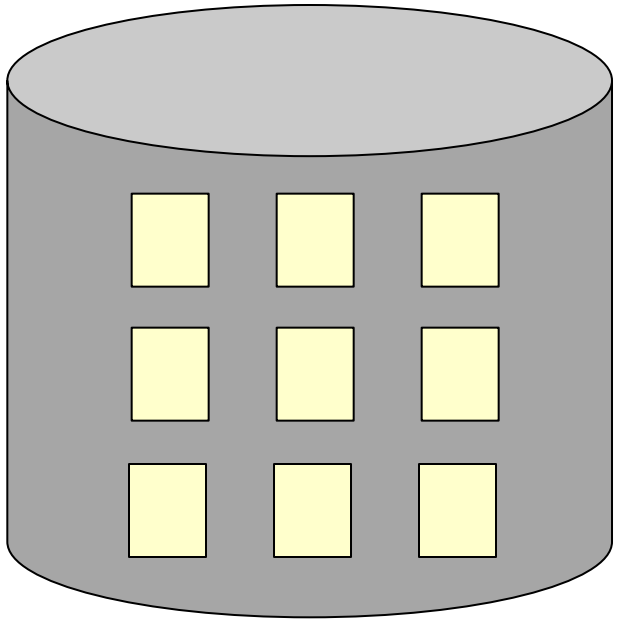
- Search and view data made available by participating agencies
- “Provides a secure Window into shared agency data”

Post Office

- Replaces Paper delivery with electronic delivery
- Send electronic paper to CISS, and CISS will distribute to destination agencies

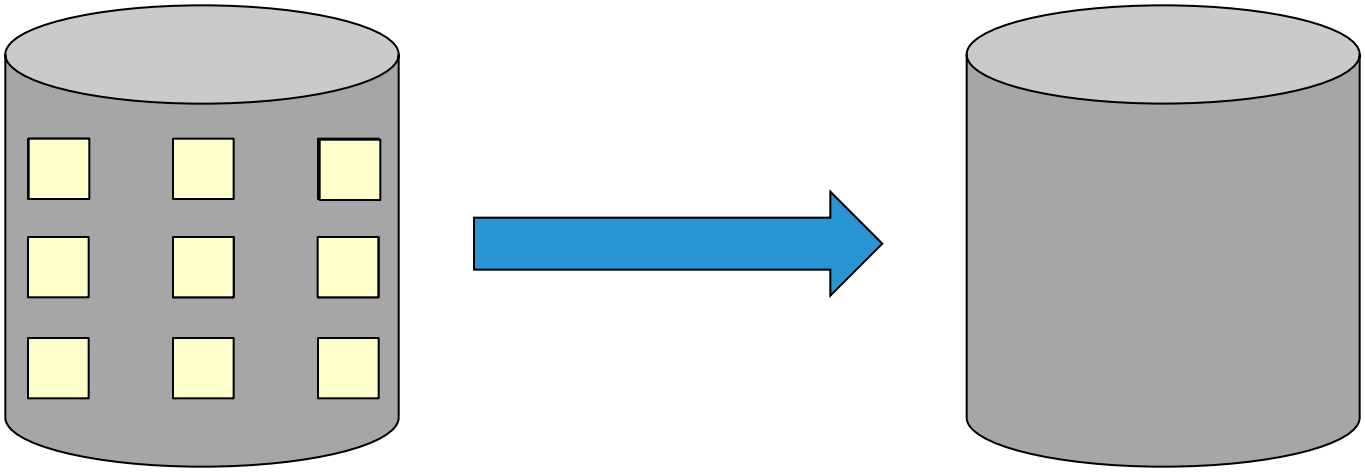
What Data Do I Have?

- Incidents
- Arrests
- Incarcerations
- Bookings
- Paroles
- Probations
- Etc.



What Data Do I want to Make Available through CISS?

Data owner (agency) controls what data is being shared.



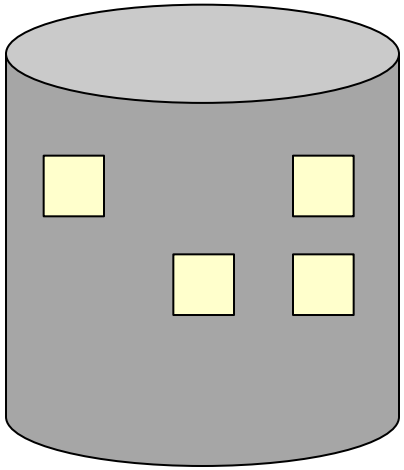
Agency Data **Shared with CISS**

Update the source…. Replica gets updated…. CISS gets updated

What type of data am I sharing?

- Public Data
- Government Data
- Criminal Justice Data
- Criminal Intelligence Data
- Criminal Investigative Data
- Criminal History Data
- Counter Terrorism Data
- Youthful Offender Data
- Agency Only Data

Identify what types of data you will be sharing



Shared with CISS

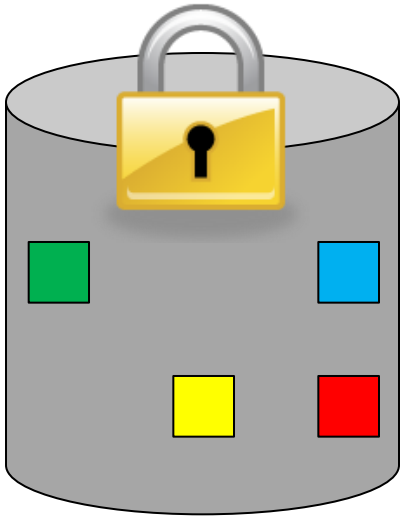
YOU identify Security Policies for YOUR Data

Policies, such as:

- Can be seen by everyone
- Can be seen only by those who are allowed to see Criminal History data.
- Can be seen only by Law Enforcement
- Can be seen only by persons with a certain clearance level
- Can be seen only by specific agencies
- Can be seen only by my agency
- Can be seen only by a specific person

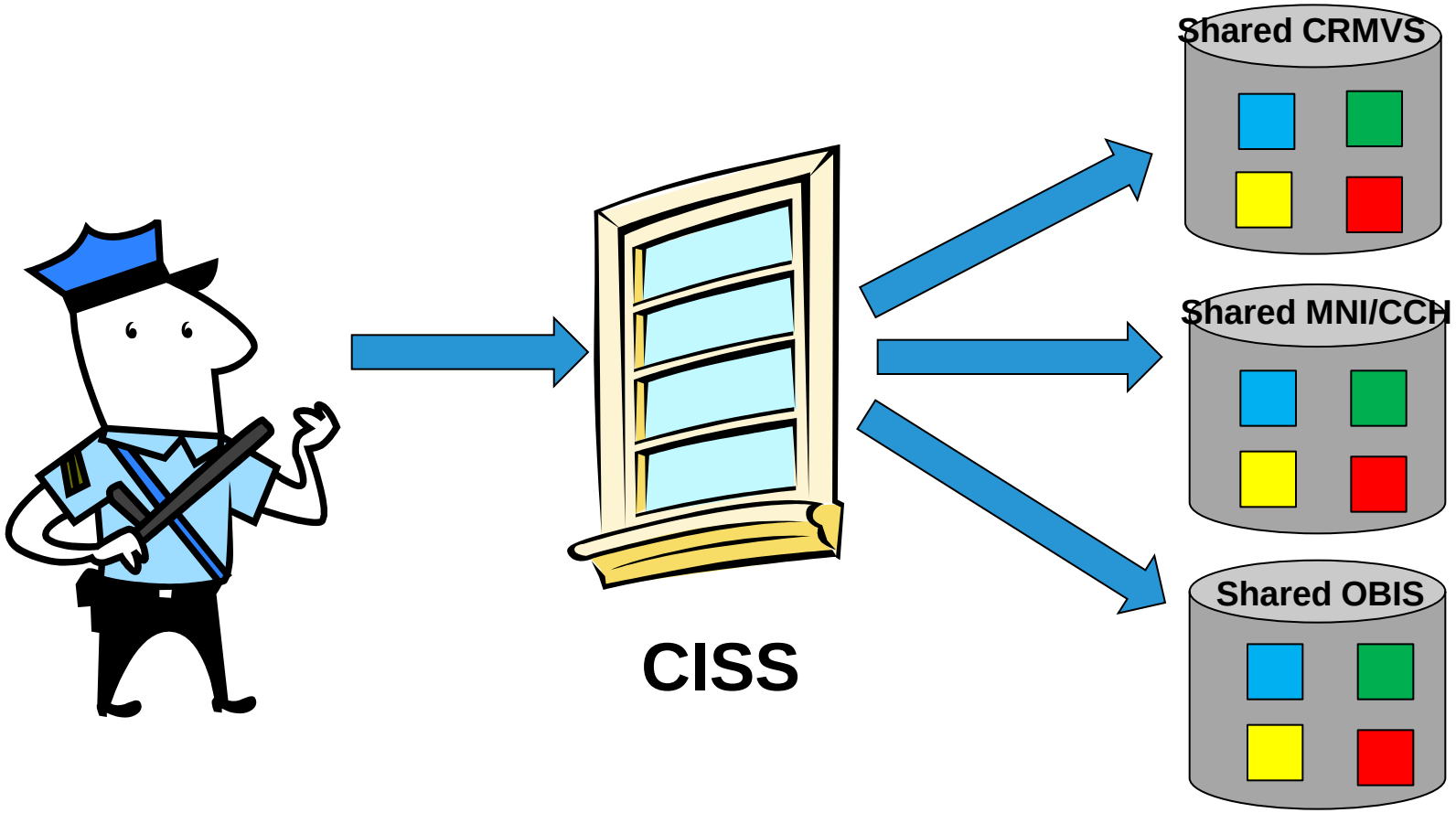
You Identify your policies,

CISS enforces your policies



Shared with CISS

What data will users be able to see when using CISS ???



Depends on the “Rights” given to you

An administrator from **YOUR** agency will provide information about **you**.

- Works for this agency
- Is a sworn officer
- Has a security clearance code of “top secret”
- Has NCIC Hot File privileges
- Has FBI III privileges

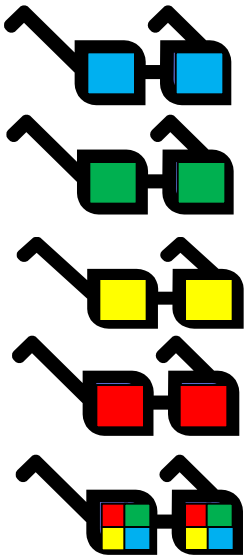
Plus, the type of information you are allowed to see “**at your agency**”:

- Public Data
- Government Data
- Criminal Justice Data
- Criminal Intelligence Data
- Criminal Investigative Data
- Criminal History Data
- Counter Terrorism Data
- Youthful Offender Data

Rights are calculated when you log in

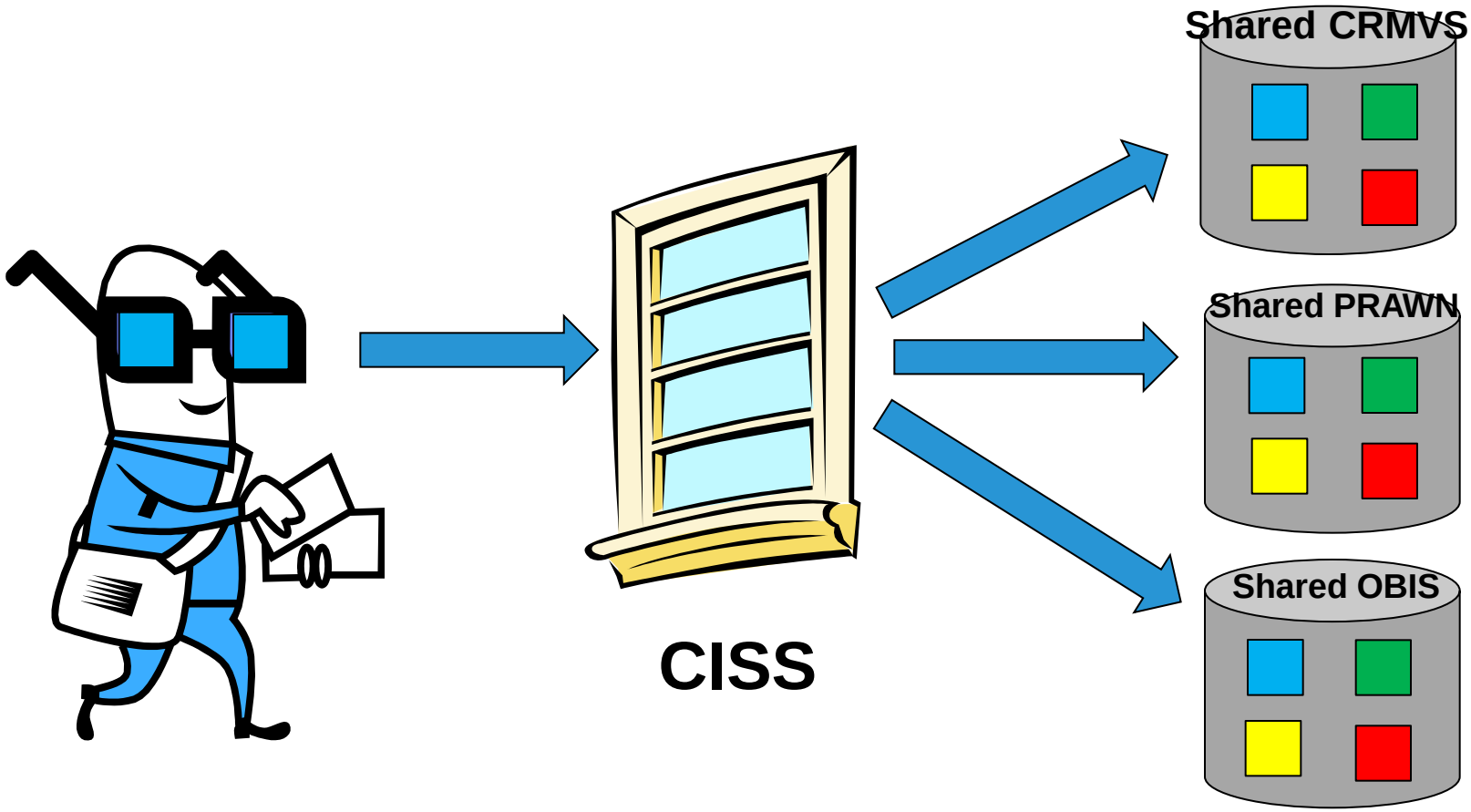
- Must have a user account
  - At CJIS, or
  - At your own agency if your agency is “trusted” by CISS
- Must have another form of Identification
  - Security Questions (CJIS)
  - User Certificate, RSA token, Etc. (Other agencies)

Your “Rights” are associated with your Identity, and control what you are allowed to “See”.



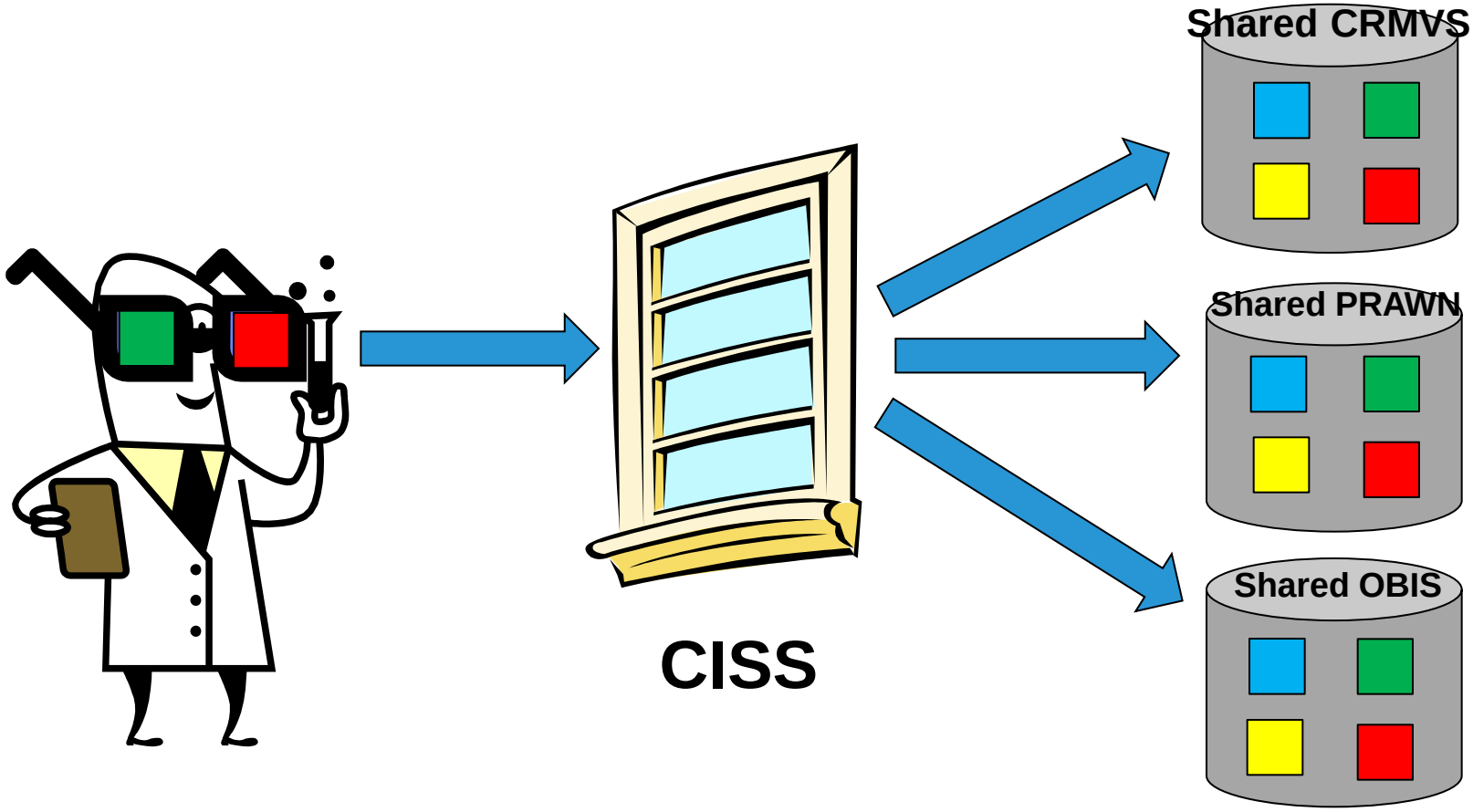
- Government Data
- Criminal Justice Data
- Criminal History Data
- Agency Restricted Data
- Sworn Law Enforcement related data

What John Q Public Sees



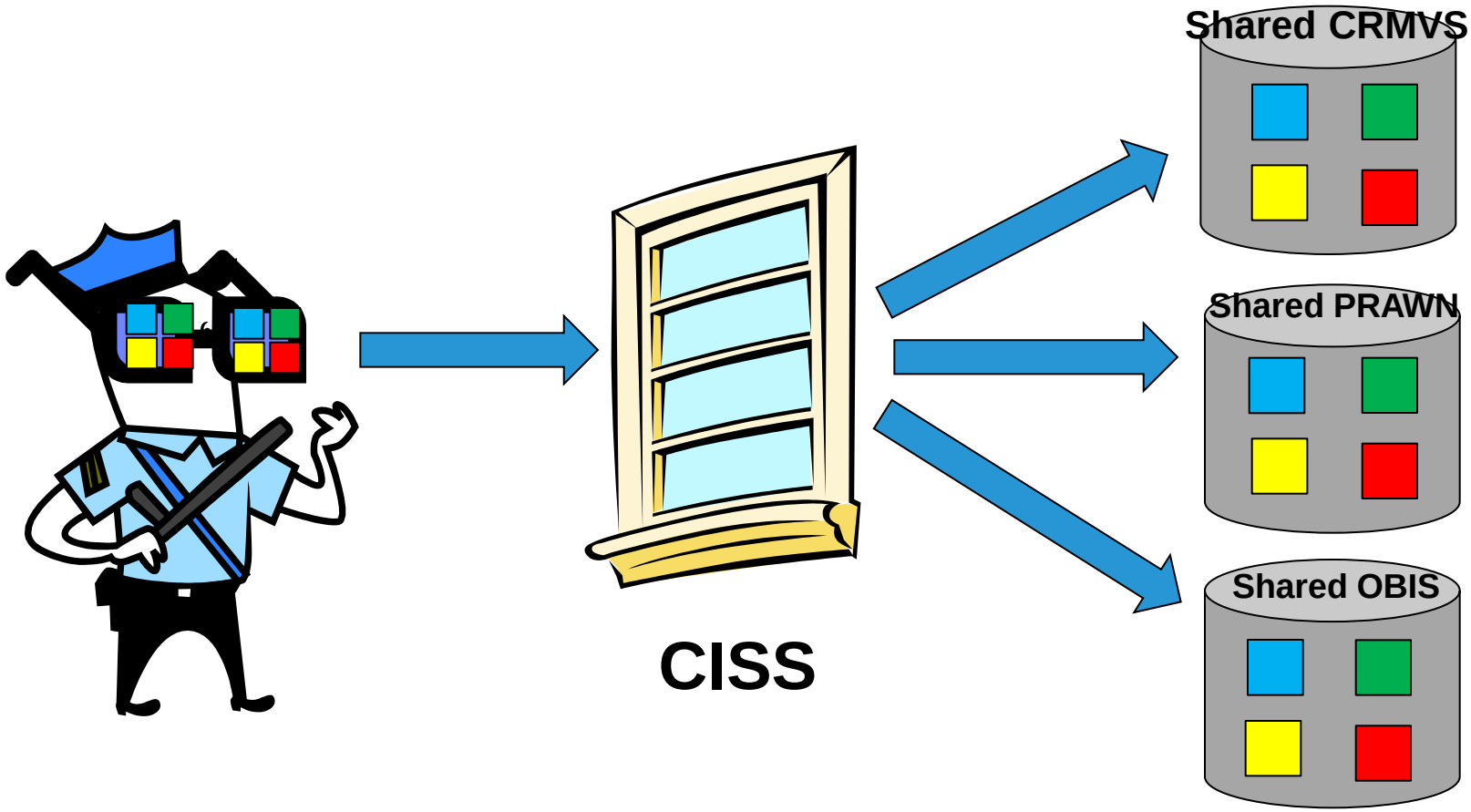
Just Public Data !

What a user at Judicial sees



What their rights allow!

What Officer Friendly sees



What their rights allow!

How is All of this Done???

CISS utilizes a federal standard for information sharing, known as:

GFIPM

GFIPM (Definition)

Global Federated Identity & Privilege Management:

A federal specification for implementing federated security for law enforcement and criminal justice organizations.

- **Global**: The federal standards body that created this specification. Global Justice Information Sharing Initiative (Global) is a federal advisory committee (FAC) of the U.S. DOJ that advises the U.S. Attorney General on justice sharing and integration initiatives.
- **Federated Identity**: A Unique Identity that represents a user across multiple trusted partners and boundaries
- **Privilege Management**: The management of the Rights a person has to See Information Based on their Work and Job Responsibilities

GFIPM Terms

Here are some terms you may have heard, or may hear, that need to be defined.

Claims – Statements of fact about a user. Used for authorizing access.

Security Token – Mechanism for distributing Claims.

Identity Provider – Logs you in and builds your security token.

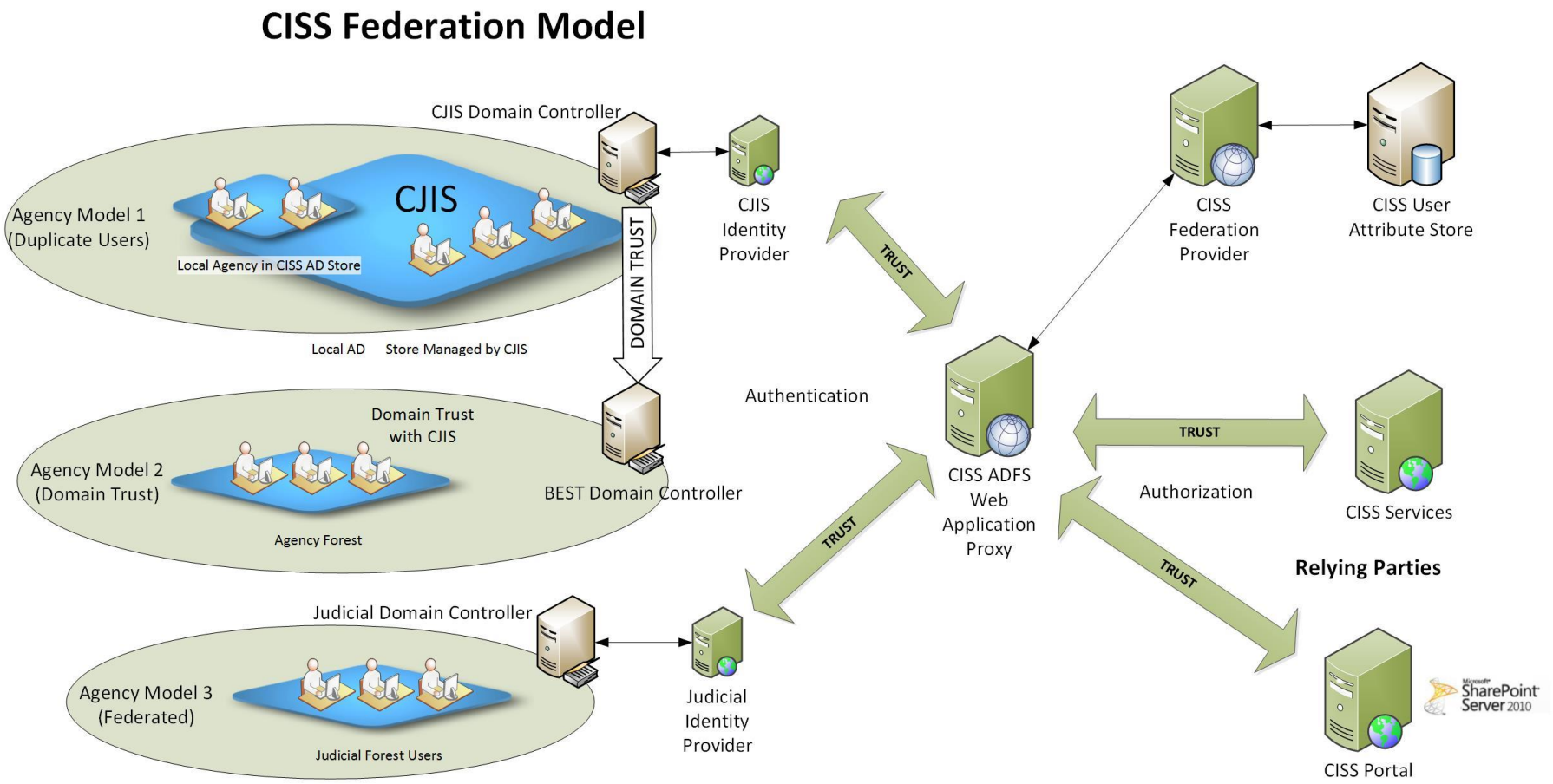
Federation Provider – Translates Identity Provider tokens into a federation token. Grants access to a Resource (a.k.a. Resource Provider)

Service Provider – (CISS) Provides a service and relies on Identity Provider to perform authentication. Makes access decisions based on claims in the federation security token

GFIPM Metadata – An XML vocabulary that defines the claim names

Federation – A collection of Identity Providers and Service Providers that trust each other.

Obligatory Technical Slide



Why is All of this Done?

1. To provide standards-based means of securely accessing data.

   - Following standards allows CISS to communicate with other organizations outside of the state if/when necessary.

2. To comply with the FBI CJIS Security Policy.

3. The CT CISS RFP requested these standards.

Multiple Choice Quiz

1) Who owns the data made available through CISS?
   A. Source Agency
   B. CISS
   C. CJIS
   D. FBI

Multiple Choice Quiz

2) Who decides what data is shared by an Agency?

A. Source Agency
B. CISS
C. CJIS
D. FBI

Multiple Choice Quiz

3) Who defines the rules to control what data is viewable in CISS?

A. Source Agency
B. CISS
C. CJIS
D. FBI

CISS enforces (applies) security policies provided by source agency

Multiple Choice Quiz

4) Who is to blame if an agency provides data to CISS that shouldn't be?

A. Source Agency
B. CISS
C. CJIS
D. FBI

CISS doesn't "have data", it provides a window on to Agency data.
PROTECT IT PROPERLY

Multiple Choice Quiz

5) What federated security standard is being used to secure CISS?

A. GFIPM
B. FICAM
C. SICAM
D. XACML

Multiple Choice Quiz

6) Information/Facts about a user are represented in?

A. Claims
B. Roles
C. Dictionary
D. Envelope

QUESTIONS?

Connecticut Information Sharing System

Security 201

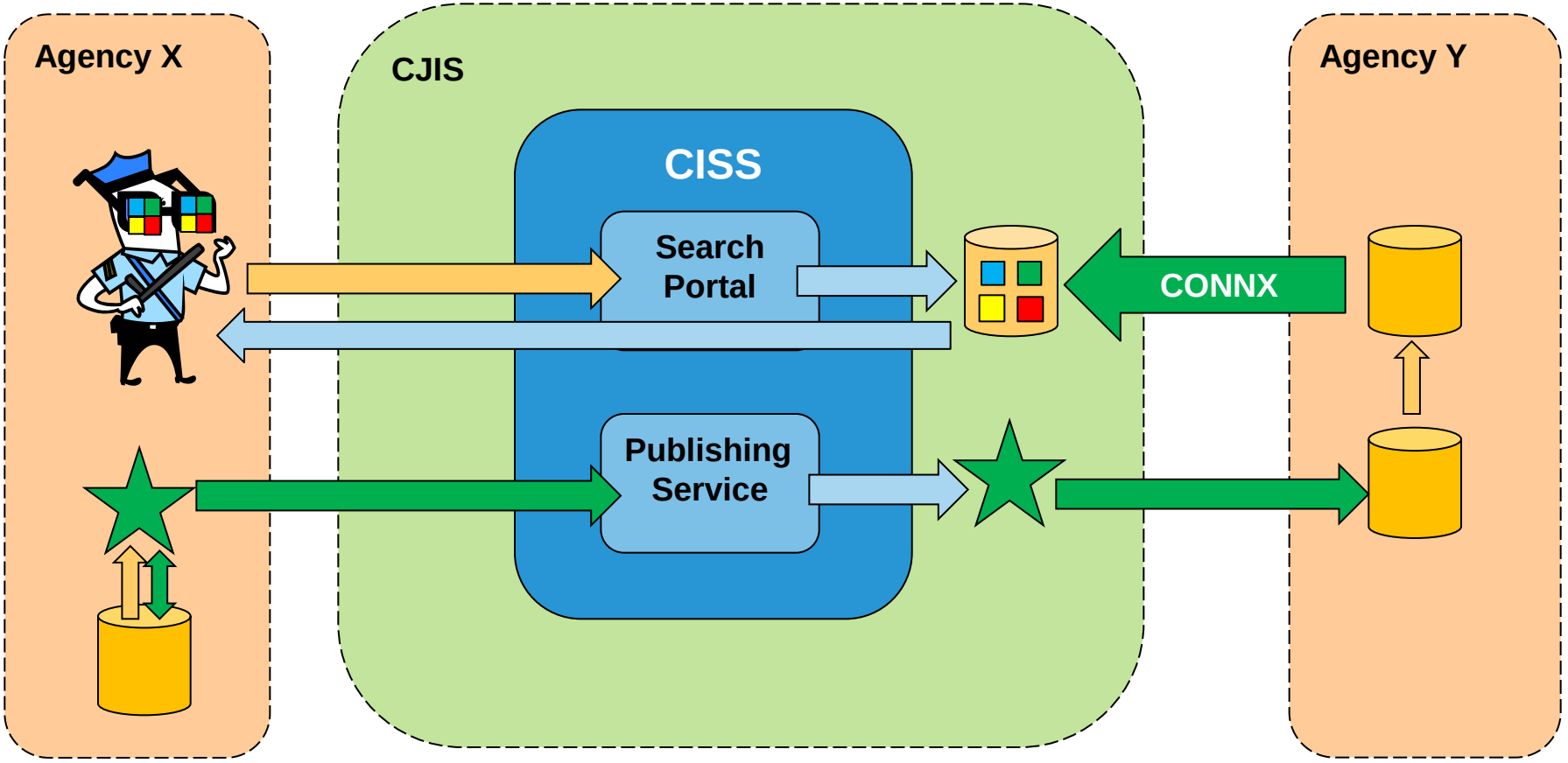
May 28, 2014

Topics

1. Quick Review from last meeting
2. Data Ownership (Agencies, CJIS, CISS)
3. How to Identify the data to share in your replica
4. How to classify your data in GFIPM
5. How to define your security policies in GFIPM
    a) Erasure example
    b) FBI data example
6. How to replicate data to your replica
7. How users Authenticate to CISS
8. How to Trust your sister agencies

xerox

CISS, CJIS, Agencies… Who is doing what?



How to Identify Data to be Shared in Your Replica?

- Recall that data you want to share with CISS is replicated to a database located at CJIS.

- CJIS will provide you with a NIEM mapping worksheet that has been augmented to capture GFIPM security information

- Identify the CLASSES you want to share
  - (e.g. Warrant, Subject, Arrest)
  - (Think Tables, Records, Objects)
- Identify the ELEMENTS of each Class you want to share
  - (e.g. Subject has First Name, Last Name, Date of Birth)
  - (Think Columns, Attributes)

- CJIS analysts will assist with populating the data mapping worksheet.

PRAWN Data Elements

Class	Element	Definition	Classification	Claims
Warrant				
	Docket Number			
	Description			
	WarrantType			
	WarrantStatus			
	YouthfulOffender			
Subject				
	First Name			
	Last Name			
Warrant Notes				
	Note Type			
	Note Text			

How to classify your data in GFIPM?

- Finish populating data into the mapping worksheet.
- Understand the GFIPM resource definitions
- Add the classification for each Class/element to the mapping spreadsheet.

GFIPM Resource Definitions

Attribute	Type of data	Qualifications
Counter Terrorism	Any Data	investigation, prevention, or prosecution of politically motivated, violent or life-threatening acts perpetrated against noncombatant targets by sub-nationals or clandestine agents
Criminal History	Arrests, Detentions, Indictments, Charges, Dispositions	Convicted. The person has a record.
Criminal Investigative	Any Data	Used for investigation purposes. Building a case. Privacy Issues.
Criminal Intelligence	Any Data	Info about person/organization suspected of criminal activity. Meets Criminal Intel submission definition.
Criminal Justice	Everything about the criminal, not just Criminal History	Whether or not the person is convicted. Incidents, arrests, etc.
Government	Any Data	used for the administrative, legal, or investigative function in furtherance of the official duties or functions of the agency
Public	data that is permitted to be released to the public	Not subject to controlled unclassified information (CUI) restrictions

PRAWN Classification Example

Class	Element	Defn	Classification	Claims
Warrant				
	Docket Number		Public	
	Description		Criminal Justice	
	WarrantType		Public	
	WarrantStatus		Criminal Justice	
	YouthfulOffender		Criminal Justice	
Subject				
	First Name		Public	
	Last Name		Public	
Warrant Notes				
	Note Type		Criminal Justice	
	Note Text		Criminal Justice	

How To Define Your Security Policies in GFIPM?

1) Work with CJIS business team capture the security rules surrounding your data
2) CJIS Team will document the rules into a “Rules” document for your data source
    a) This is a plain English document
    b) Uses your language for describing how the data should be handled and who is allowed to see it.
    c) Does not define the exact “GFIPM language” for a security policy
    d) Can identify which GFIPM claims represent your rules
    e) (E.g. “Only officers should be allowed to see this if the status is….”)
3) CJIS and Xerox will create the actual “GFIPM Language” of the security policies.
    3) Agencies don’t “Need to”, but are welcome to work on policies at this level.

Sample Rules Document (excerpt)

PRAWN Data Security Business Rules

In general, PRAWN warrant information should be available to users with the "Criminal Justice Data Agency Search Home Privilege Indicator" claim. That is, users who are authorized to see "criminal justice information" are generally permitted to view PRAWN warrant information.

The following records will *not* be available to any users through CISS, regardless of a user's security claims:

- Warrants that have been served (based on the WARRANT.WARRANT_STATUS field).
- Warrants that have been vacated (based on the WARRANT.WARRANT_STATUS field).

The following records will only be available to users with the "Youthful Offender Data Agency Search Home Privilege Indicator" claim in addition to the "Criminal Justice Data Agency Search Home Privilege Indicator" claim:

- Warrants for youthful offenders (based on the WARRANT.YOUTHFUL_OFFENDER field).

CRMVS Erasure Sample

Class	Element	Defn	Classification	Claims
Arrest			Criminal Justice	
	Arrest Date			
	Case Number			
	UAR Number			
Arrest Charge			Criminal Justice	
	Case Status			SEE RULES DOC
	Statute Code			

Case Status = ‘Post Conviction’ OR ‘Pre-Finding’

ALLOW IF PublicDataSelfSearchHomePrivilegeIndicator = True

Case Status = ‘Pre AE/DE/SV Sealed’

ALLOW IF CriminalJusticeDataSelfSearchHomePrivilegeIndicator = True

Case Status = ‘Erased’ OR ‘Pardoned’

DISALLOW

RMS FBI Data Example

Class	Element	Defn	Classification	Claims
Arrest Report			Criminal Justice	SwornLawEnforcement OfficerIndictor
	From FBI			NCICCriminalHistoryPrivilegeIndicator
Arrest			Criminal Justice	
	UAR Number			
	Arrest Date			
Subject			Criminal Justice	
	Name			

IF ‘From FBI’ = True

ALLOW IF

CriminalHistoryDataAgencySearchHomePrivilegeIndicator = true

AND SwornLawEnforcementOfficerIndicator = true

AND NCICCriminalHistoryPrivilegeIndicator = true

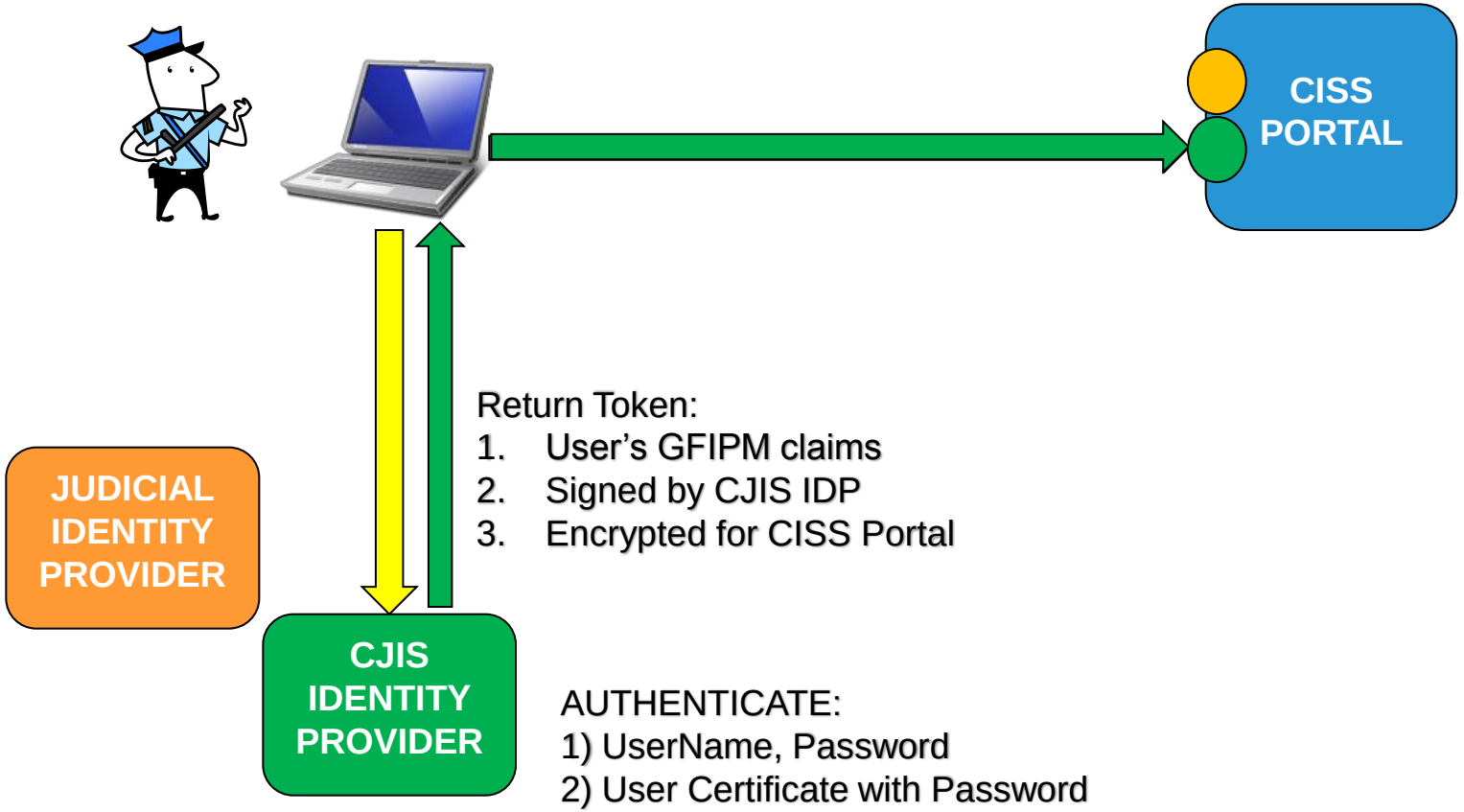
How to Replicate Data to Your Replica?

1) Agency Builds T-SQL View to query your data
   a) Or whatever is appropriate for your data source type.

2) CJIS uses CONNX to replicate Agency Data to Replica at CJIS
   a) CONNX Extracts, Transforms, Loads (ETL) data to the replica
   b) CONNX queries the ‘View’ that provides your established data.
   c) CONNX can transform data. (e.g. 5 fields into PRAWN Docket Number)
   d) CONNX loads the data into the Agency Replica

3) CONNX synchronizes what is available in your view with what is stored in the Replica at CJIS

How Users Authenticate to CISS?



How To Trust your Sister Agencies?

Concern:

"*How do I know that other agencies are properly assigning GFIPM claims to their users, and not just giving them every permission possible*?"

Mitigation:

1. Use the CJIS Security Policy!
   a) Each agency is supposed to have a Local Agency Security Officer (LASO) that reports to the CJIS Systems Officer (CSO)

2. Put the LASO at each agency in charge of assigning security claims
   a) LASO vets registered users for their agency, and adds GFIPM claims

3. Review
   a) CSO can have reviews with the LASOs
   b) CSO can review CISS Audit logs

QUESTIONS?

Connecticut Information Sharing System

Security 201

May 28, 2014