Connecticut Information Sharing System

Security 301

June 25, 2014

Agenda

- Review of GFIPM claims currently identified for use in CISS
- Explain the process for determining data security rules
- Discuss methods for identifying and assigning user security claims
- Show a preliminary user management interface
- Answer any remaining questions

GFIPM Claims in CISS So Far

Currently in use (POC):

- Criminal Justice Data Privilege
- Public Data Privilege
- Youthful Offender Data Privilege (non-standard)
- Employer Name

Anticipated for future use:

- Criminal History Data Privilege
- Government Data Privilege
- Sworn Law Enforcement Officer Indicator

More GFIPM Claims for CISS?

Other claims may be introduced as-needed to satisfy specific requirements

- If a specific type of data requires a specific claim, we will use that claim to secure that data

The data security rules dictate which claims are used, and the claims do not suggest which users may or may not use CISS

- Example: Can law enforcement use CISS if we don't use the SLEO claim?

  Sure – especially if there's no data that requires the SLEO claim.

Identifying Data Security Rules

Start by placing “labels” on the data (at the record level and, if appropriate, the data level), as in:

- “Criminal Justice Data,” “Government Data,” “Public Data,” etc.
- Definitions for these labels provided as part of the GFIPM specification

In some cases it may be appropriate to use multiple labels for a single piece of data, for example:

- The data is both criminal justice and pertains to a youthful offender

Identifying Data Security Rules

Identify any business rules that may affect which labels are applied

Examples:

- A record may be labeled as “criminal justice data,” but if the case resulted in a conviction it may later be labeled as “public data.”
- A record may be labeled as “criminal history data,” but if the subject’s age is less than 18 it may be labeled as both “criminal justice data” and “youthful offender data.”

Identifying Data Security Rules

Rules may be very simple:

- “A user may view this record if they have the criminal justice data claim.”

Rules may also be arbitrarily complex:

- “A user may view this record if they have the criminal justice claim, but they may also view this record if they work for DPDS and the case is assigned to the public defenders office, unless the subject is a youthful offender in which case the user must also have the youthful offender data claim.”

Remember that it won’t always be as simple as, “a user with claim X is allowed to see data Y”.

Identifying Data Security Rules

Once these rules have been identified, evaluate them to determine if they produce the desired effect:

This data is labeled as “criminal justice data.”

- Does it make sense that any user who is authorized to see criminal justice data at their agency can see this information?
- Alternatively, are there any users who are authorized to see criminal justice data that shouldn’t be allowed to see this data?

This exercise verifies that the rules are correct and identifies any exceptions that need to be considered

Identifying User Security Claims

You will recall that security claims make assertions about users, as in:

- A user with the “criminal justice data” claim has permission to search for criminal justice data

These assertions are formally defined by the GFIPM specification

The data privilege claims indicate that a user has permission to view a specific type of data at their agency

Identifying User Security Claims

Since claims are assertions about a user, the simplest way to assign claims is to decide if the user meets the requirements that the claim asserts.

Example: Criminal Justice Data Self Search Privilege Indicator

- *"True if the user has permission to search…for criminal justice data and documents within the user's home system, network, or agency. False otherwise."*

Therefore . . .

- If this user is allowed to search for criminal justice data at their agency, they should have this claim.

Identifying User Security Claims

For some claims this is fairly straightforward, for example:

- Sworn Law Enforcement Officer

For others not so much, as in:

- Criminal Justice Data Self Search Home Privilege Indicator

If in doubt, consult the formal definitions contained in the GFIPM specification

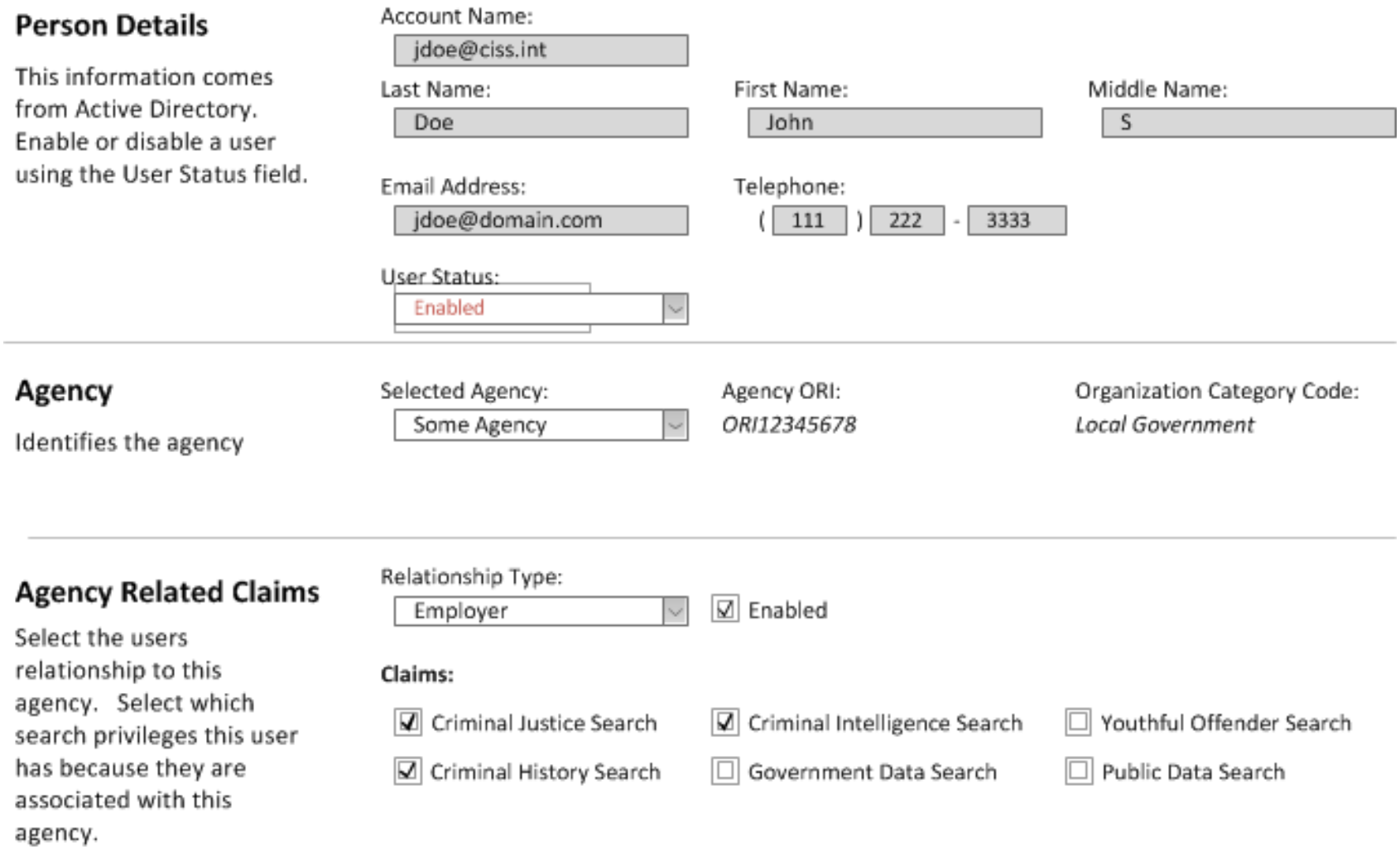
Assigning User Claims

Work on detailed requirements for user provisioning and claims management is currently in-progress

Agency administrators will be responsible for assigning claims to users within their agency

The CISS User interface is intended to allow administrators to assign claims to individual users or multiple users at once

Sample User Management Page



Connecticut Information Sharing System

Security 301

June 25, 2014