



Criminal Justice Policy Dashboard

Requirements & Design

Prepared by



BRT, Inc.

A Minnesota Company
(DBA Beam Reach Technologies)



Intentionally Blank





Introduction

The purpose of this document is to define the requirements and design of the BRT, Inc. Criminal Justice Policy Dashboard (CJPD) product. CJPD is intended to allow Criminal Justice organizations to share information easily while maintaining and monitoring compliance with Service Level Agreements and Policy Definition requirements. The intended audience for this document consists of:

- Criminal Justice Information Architects. Criminal Justice Information Systems architects will review and edit the requirements and design to insure that resulting BRT, Inc. product offering targets realistic and recognized needs within the Criminal Justice Information Technology (CJIT) community.
- Developers. Software developers will review and edit the requirements and design to insure that the resulting BRT, Inc. product can be implemented in the required schedule and resource windows.
- Criminal Justice Information Buyers. Purchasing authority and purchasing influencers in Criminal Justice will be asked to review polished drafts of the document to determine the market urgency of the product.





Requirements

The definition of requirements for the CJPD is divided into three main areas. First are the requirements that relate to the ability to analyze, define, specify, and configure policy and service level agreements for a particular data source. The second contains the requirements that relate to translating defined policy into a data sharing implementation. The third area contains requirements of a general marketing nature.

General Overview

The CJPD product is designed to support a Criminal Justice organizations need to share information with others. This results in an “Organizational Namespace” view of requirements. This means in general that an organization may have multiple heterogeneous information systems from which data is being requested by multiple heterogeneous agencies. Consequently, the CJPD information sharing “Name Space” is a logical many-to-many policy mapping, from information systems of one particular justice organization, to requesting agencies. CJPD assumes this mapping is to be created, monitored and maintained by the organization that is providing the data. This “**Provider**” organization defines the policy and data sharing name space. Further it is assumed that the “**Requester**” organization must agree to comply with the policy for any data the Provider shares.

Significant work has already been completed in the development of a data dictionary and schema modeling of criminal justice data. Such standards as Justice XML (GJXDD) and NIBRS/NDEx data dictionaries and schemas are already defined and in use. More recently, a joint effort thru both The US DOJ and DHS had sought to leverage this effort with the more holistic model, NIEM (National Information Exchange Model).

Reference documents exist in “defacto” form used by various cooperating agencies. Standards based Reference documents are just being addressed. These include documents describing typical information exchange groupings for criminal justice organizations, e.g. Arrest Record, Jail Roster, Vehicle Inquiry, etc.

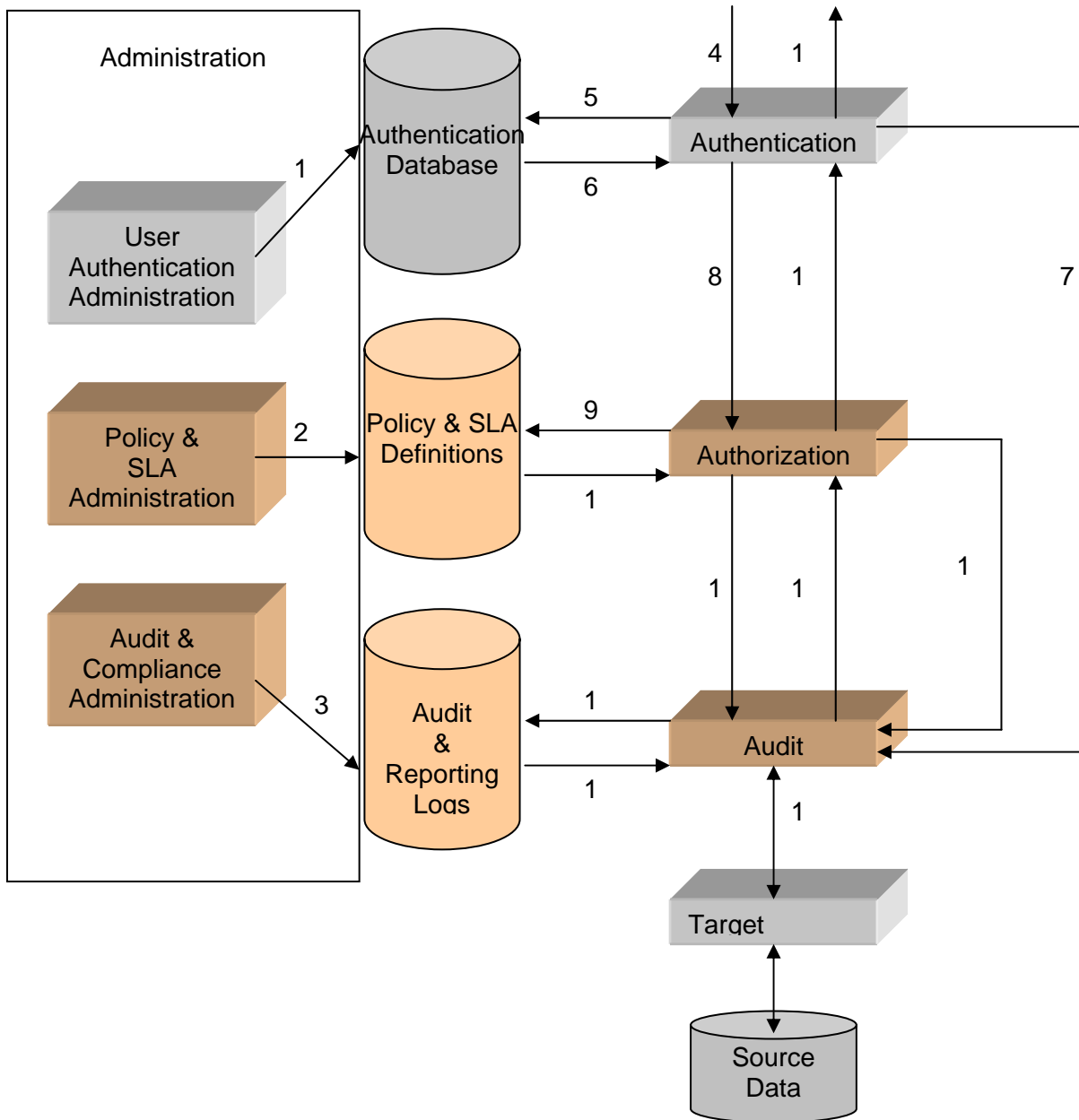
The Query/Response envelope is the layer where implementation meets definition. As of the writing of this document, little standards based implementation effort has been completed to map the criminal justice information systems into transport and exchange protocol. In general, this is due to the complexity of managing Service Level Agreements and Policy Definitions at the transport and exchange levels. Providing data to requesting organizations in a secure manner with verifiable compliance to Service Level Agreements and Policy Definitions is the focus of the requirements and design of the Criminal Justice Policy Dashboard.





Logical Exchange Architecture

The following diagram shows the flow of an information request.





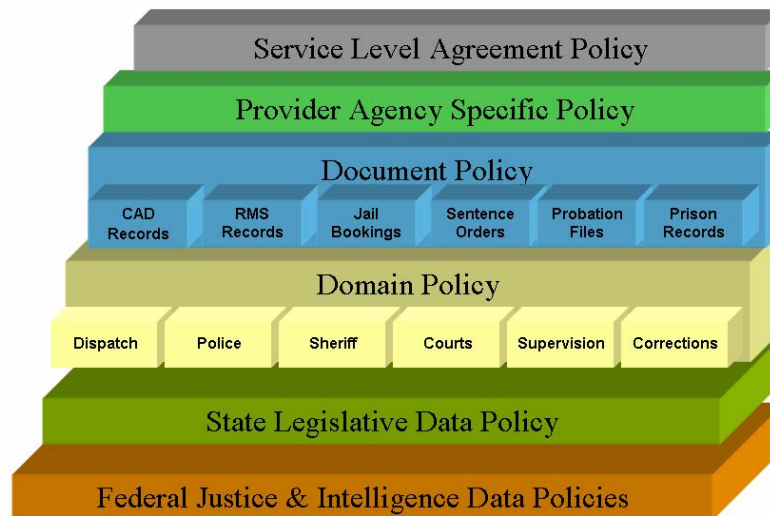
Design

Definitions

Before detailed design can be discussed, it is important to level set with common terms and definitions that will be used thru out the design specification.

Policy

Policies in the CJPD context are definitions of data sharing practices at some organizational level. Consider the following “policy stack” diagram.



The CJPD policy stack default is shown in the above policy stack diagram. Policy is defined in the same format at each layer, but each layer has different organizational emphasis. In general, each layer is allowed to be more restrictive, or at least as restrictive, in the sharing of information. No layer may be less restrictive than any lower level. For example, the Law Enforcement Domain Policy may not permit sharing information that is restricted by Legislative Policy.





Legislative Policy is primarily concerned with State and Federally mandated data practices legislation. For example, policies such as “all data stored about an individual must be made available to that individual once they have established identity” and “Crime victim information stored in any State or Federal criminal justice system may not be shared outside the law enforcement community.”

Domain Policy is usually policy that is an extension or refinement of Legislative Policy. It includes such policy statements such as “Gun Permit information is classified as public, but gun permit violation information is classified as confidential” and “Court documents are not viewable by the public, until a formal charge has been filed”.

Reference Document Policy is a data provider’s policy towards useful groupings of data elements. These groupings include such items as arrest document, DMV inquiry, probation record, prison roster, etc. These include such policy statements as “This agency provides charge records and booking records to Law Enforcement domain roles” and “This agency provides court documents only to court domain roles.”

Agency Policy is a data provider agencies policy that is specific to their internal policy. For example, “This agency provides data only in read only format” and “all data provided by this agency is considered “confidential” under Chapter 13 and 28CFR”.

Service Level Agreement is a data providers specific policy that specifies how data is to be provided and under what circumstances. For example, an SLA may be “Data from this agency is provided under a WSDL service defined on port 443 for PKI users only” and “Data will be available in less than 15 seconds from query submission for 99.9% of all queries.

Business Logic

A central key goal for CJPD is the separation of the any justice sharing application business logic components, from the authentication, authorization and audit components. Consequently for the CJPD, business logic is defined as any processing logic that is not oriented towards policy definition, policy enforcement, policy audit definition, and policy auditing and reporting. This includes all data processing logic not directly related to the CJPD. Examples of business logic in this context are searching, sorting, filtering, collating, analysis, messaging, and others.





Data Dictionary

Criminal Justice has several data dictionaries that have been defined. These include defacto, dejure, and emerging standards. For example NIBRS/NDEx, GJXDM, NIEM and others. CJPD includes one or more Data Dictionaries that can be selected during installation.

Schemas and Reference Documents

Schemas are used in conjunction with data dictionaries to give contextual meaning to collections of data definition elements. For example, an Arrest Record schema is a definition of context for a collection of information such as Last Name, First Name, Charge, Arrest Date, Bail Amount, . . .etc. In the context of CJPD, schemas are synonymous with Reference Documents or IEP's

Roles and Domains

Roles are work and job functions that are assigned to individual criminal justice workers. Examples of roles are "County Prosecutor", "Sheriff", "Probation Officer" and "Court Clerk". Roles are one of the primary components of data sharing policy. Every person that makes a request via the CJPD will be required to have one or more roles assigned.

Domains in the context of criminal justice, CJPD and policies, are groups of logically associated roles. The "Law Enforcement" domain for example is composed of Highway Patrol, Police, Sheriff, Police Dispatcher, etc. Criminal Justice data sharing policy is often based upon the domains of the requestor and the provider. Every person that makes a request via the CJPD will be required to have one or more domains assigned.

Domains and Roles can be added, deleted and modified in the CJPD. . From the roles, domains can be determined. After initial installation, some typical domains that are defined as default in the CJPD are:

Corrections and Probation

The correction and probation domain includes such individual roles as:





- CP Administrative Staff
- CP Administrator
- CP Case Manager
- CP Intake-Records Personnel
- CP Investigator
- CP Line Supervisor
- CP Non Supervisory Support Staff
- Probation Officer (Adult & Juvenile)

Courts

The courts domain includes such individual roles as:

- Court Clerks (level 1-3)
- Court Supervisors
- Judges (Courts)

Administrative

The Administrative domain includes such individual roles as:

- Test Profile for Testing
- Help Desk
- Administrator
- Test Profile No Juvenile Access

Law Enforcement

The Law Enforcement domain includes such individual roles as:

- L.E. Administrative (Civilian)
- L.E. Administrative (Sworn)
- L.E. Administrative Staff
- L.E. Civilian Dispatch
- L.E. Civilian Support Staff
- L.E. Investigator
- L.E. Jail-Bailiff
- L.E. Patrol Function
- L.E. Warrants-Records
- Specialty L.E. Unit Civilians





Prosecutors

The Prosecutors domain includes such individual roles as:

Administrative Staff & Paralegals (Prosecutors)
Investigators (Prosecutors)
Prosecuting Attorneys
Victim/Witness Staff (Prosecutors)

Public Defenders

The Public Defenders domain includes such individual roles as:

Public Defender Administrative Staff & Law Clerks
Public Defender Conflict Lawyers
Public Defenders

Use Cases (High Level)

Use cases for the CJPD fall into two broad categories. These are the deployment and administration of the Policy and Audit Decision Points, and the deployment and administration of the Policy and Audit Enforcement Points. The primary high-level use cases are described below. The general use of the CJPD would be:

1. Select and configure the policies that are to be the controlling policies for data sharing.
2. Select and configure the auditing methods to be used to document the use and compliance with the controlling policies selected.
3. Install and configure the “enforcement point” system.
4. Activate the enforcement system.
5. Monitor the policy and access logs generated.

Policy Deployment and Administration (Quick Start)

The CJPD product comes complete with pre-defined common policies for the Criminal Justice Data Exchange Policy Stack. If the default provided stack includes sufficient policy definition, the policy administrator can use the defaults when running the CJPD policy administrator tool.





1. Select the data dictionary to be supported (GJXDD, NIBRS, etc.)
2. Select the Legislative Polices to be supported (28CFR, Chapter 13, etc.)
3. Select the Domain group for which data will be provided (Law Enforcement, Courts, etc.)
4. Select the actual data to be provided in reference documents (Arrest records, prison roster, etc.)
5. Enter information regarding the service level agreements that will be supported.

Policy Deployment and Administration (Advanced)

If the out of the box default Criminal Justice Data Exchange Policy Stack must be modified or enhanced, the use case proceeds in the following fashion.

1. Select the data dictionary to be supported (GJXDD, NIBRS, etc.)
2. Select the Legislative Polices to be supported (28CFR, Chapter 13, etc.), or modify and create a new Legislative Policy to be supported.
3. Select the Domain group for which data will be provided (Law Enforcement, Courts, etc.), or modify and create a new Domain Group to be supported.
4. Select the actual data to be provided in reference documents (Arrest records, prison roster, etc.), or modify and create new reference documents to be provided.
5. Create, if needed, any agency specific policy not related or contained within the previous Legislative, Domain, or Reference Document policies.
6. Enter information regarding the service level agreements that will be supported.





In addition, the Policy Administrator can select a slide setting of Low, Medium, or High for policy enforcement. These settings have the following definitions:

1. **Low.** This setting does not enforce policy, but causes auditing to take place. This setting is primarily useful in setting up and understanding Policy, or for using internally for an authorized and segregated private network.
2. **Medium.** This is the default setting. All defined policy of the policy stack is enforced. Any requests that are denied under the policy return information to the requestor about the denial and the reason.
3. **High.** All defined policy of the policy stack is enforced. Any request that is denied under the policy returns no information about the denial.

Audit Deployment and Administration

The CJPD product comes complete with pre-configured audit scenarios. The administrator may select various parameters regarding logging that will be used by the enforcement server.

1. Select the audit information level desired from Brief, Normal, or Verbose. Brief includes all information required to fulfill requirements of the selected Policy stack.
2. Select logging archive save dates. Retention dates will be selected based on requirements of the various policy stack supported.
3. Determine the log file sizes, frequencies and cycles (administrative functions useful to system administrators for managing log files).
4. Configure the log file location directories.

Enforcement Deployment and Administration

The system administrator installs and configures the Policy Enforcement component of the CJPD on some system that will control access to criminal justice information to be shared. This process can be described as:





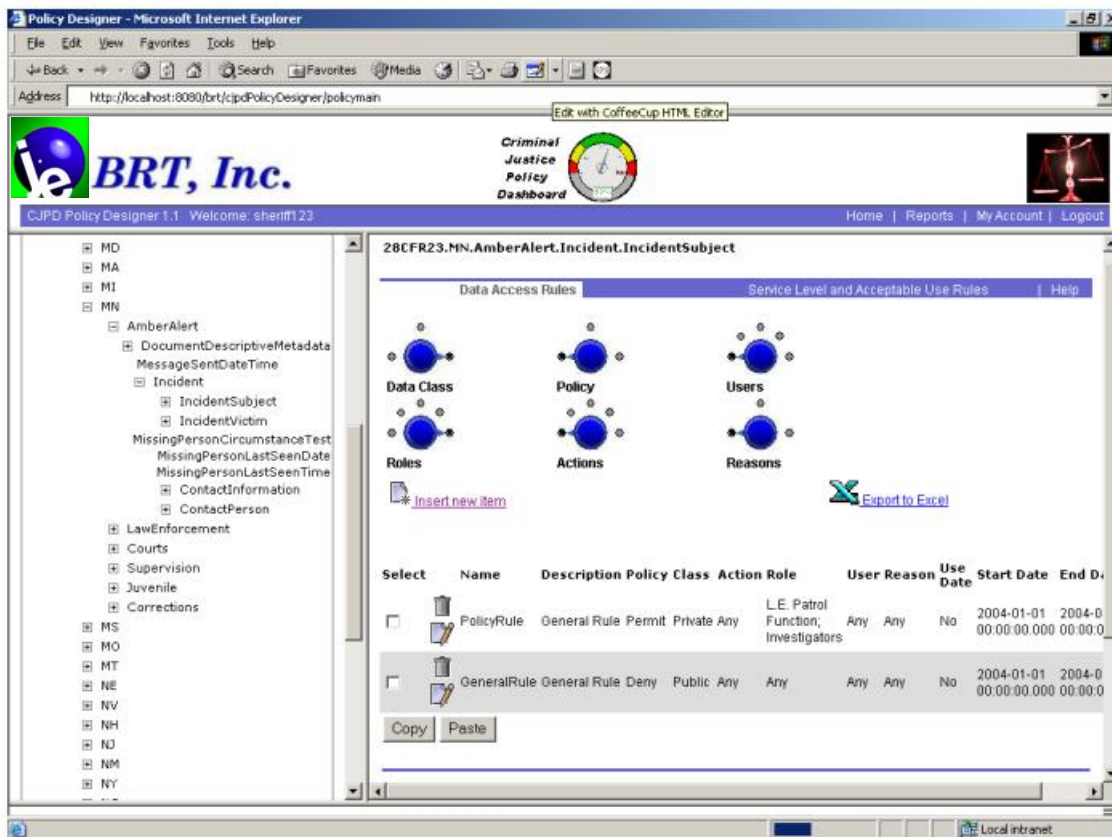
1. Install the Policy Enforcement Server
2. Provide the Policy Enforcement Server with policy definition files generated in previous steps.
3. Configure the Policy Enforcement Server to map the Data Dictionary selected in the Policy Definition documents to the targeted data systems.
4. Provide the Policy Enforcement Server with the Audit definition files generated in previous steps.
5. Activate the Policy Enforcement Server, and monitor access.





Runtime User Interface

The following are example screenshots of the users control of creating or inheriting privacy policies and applying them against specific web services within a justice information sharing environment, but yielding their use and auditing within the constructs of the available security architecture.



This frame shows the hierarchal control tree (left) for managing policies from Federal down to specific State and Local configurations. In the right frame, the user can choose to inherit or edit policies for specific justice data exchanges.

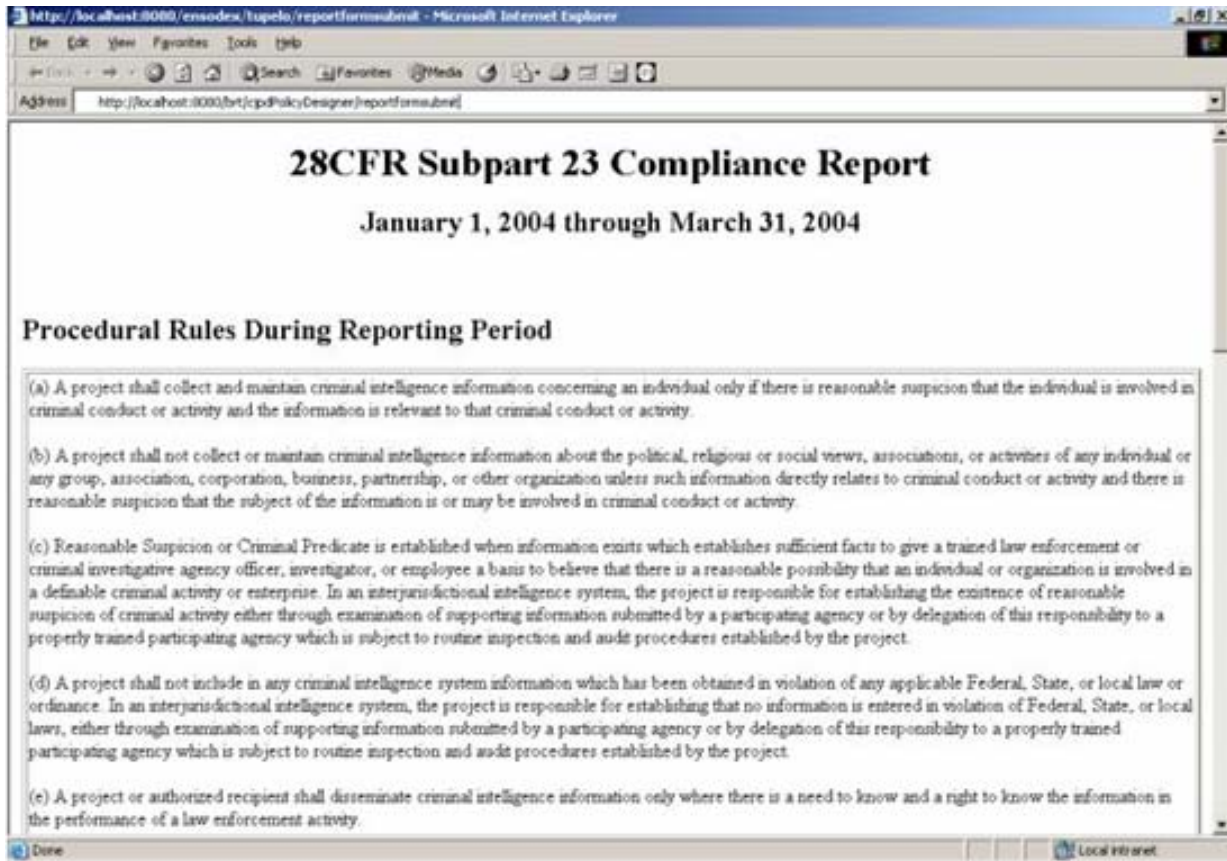




Flexible Development Environment Process

In this view, a specific web service for Amber Alert has been selected and the user is editing the policy by limiting role-based access to fine-grained data elements within the document - - in this example, for the IncidentSubjectName>PersonName. In creating this “fine-grained” rule, the web service data publisher determines what “justice roles” can have access to this data element in any Amber Alert notice that it publishes, and the conditions for auditing or special conditions for “need to know”.





Ultimately, the Policy Designer and Justice Policy Dashboard can generate Compliance Reports, indicating the specific rules for access and auditing reports for any period of time against any system or data source.

