Conceptual Design Document - Disposition Reporting Management

Prepared for the

Arizona Criminal Justice Commission

November 2004

spherion SM

NORTHROP GRUMMAN
Information Technology

eCorridor

TABLE OF CONTENTS

1 INTRODUCTION 1-1

1.1 PURPOSE 1-2
1.2 EXECUTIVE SUMMARY 1-3
1.3 DEFINITION OF TERMS 1-4
1.4 PROJECT APPROACH AND REQUIREMENTS IDENTIFICATION 1-7
1.4.1 Joint Application Design and Other Project Meetings 1-7
1.4.2 Requirements Recommendations 1-9
1.5 PROJECT REFERENCES 1-19

2 DISPOSITION REPORTING INTEGRATION CONCEPTS 2-1

2.1 INTEGRATION REQUIREMENTS 2-1
2.2 RECOMMENDED SOLUTIONS 2-2
2.2.1 Criminal Cycle Identifier 2-3
2.2.2 Charge Tracking 2-4
2.2.3 Interagency Indexing 2-5

3 BUSINESS PROCESS DEFINITIONS 3-1

3.1 OVERVIEW 3-1
3.1.1 Identification of Business Processes Supported by the DRM 3-1
3.1.2 Interaction Between the DRM, ACCH, and AZAFIS 3-2
3.1.3 Statutory and Rule Requirements 3-3
3.1.4 Common Documents and Data Sets 3-4
3.2 DESCRIPTION OF BUSINESS PROCESSES 3-6
3.2.1 Physical Arrest and Booking 3-6
3.2.1.1 High-Level Process Flow 3-6
3.2.1.2 Physical Arrest Event 3-6
3.2.1.3 In-Custody Arrests 3-7
3.2.1.4 Citation and Fingerprinting 3-7
3.2.1.5 Processing After Fingerprinting: Physical Arrest 3-7
3.2.1.6 Data Exchanged 3-9
3.2.1.7 Notifications 3-10
3.2.1.8 Issues 3-10
3.2.2 Cite and Release 3-11
3.2.2.1 High-Level Process Flow 3-11
3.2.2.2 Data Exchanged 3-13
3.2.2.3 Notifications 3-14
3.2.2.4 Issues 3-14
3.2.3 Law Enforcement Reports Submitted for Prosecution Review 3-14
3.2.3.1 High-Level Process Flow 3-14
3.2.3.2 Data Exchanged 3-17
3.2.3.3 Notifications 3-18
3.2.3.4 Issues 3-18
3.2.4 Grand Jury Indictment 3-18
3.2.4.1 High-Level Process Flow 3-18
3.2.4.2 Data Exchanged 3-22
3.2.4.3 Notifications 3-22

3.2.4.4 Issues 3-23
3.2.5 Information Filed Directly in Superior Court 3-23
3.2.5.1 High-Level Process Flow 3-23
3.2.5.2 Data Exchanged 3-25
3.2.5.3 Notifications 3-25
3.2.5.4 Issues 3-25
3.2.6 Court-Initiated Charges 3-26
3.2.6.1 High-Level Process Flow 3-26
3.2.6.2 Data Exchanged 3-28
3.2.6.3 Notifications 3-28
3.2.6.4 Issues 3-28
3.2.7 Court Transfers 3-28
3.2.7.1 High-Level Process Flow 3-28
3.2.7.2 Data Exchanged 3-30
3.2.7.3 Notifications 3-30
3.2.7.4 Issues 3-30
3.2.8 DOC Custody and Supervision Status 3-30
3.2.8.1 High-Level Process Flow 3-30
3.2.8.2 Data Exchanged 3-32
3.2.8.3 Notifications 3-32
3.2.8.4 Issues 3-32
3.2.9 DNA Sample Data 3-33
3.2.9.1 High-Level Process Flow 3-33
3.2.9.2 Data Exchanged 3-36
3.2.9.3 Notifications 3-36
3.2.9.4 Issues 3-36

4 DRM SYSTEM REQUIREMENTS 4-1

4.1 FUNCTIONAL HIERARCHY DIAGRAM 4-1
4.2 DRM DISPOSITION INFORMATION COLLECTION AND MANAGEMENT 4-3
4.2.1 Law Enforcement Segment 4-3
4.2.1.1 Overview 4-3
4.2.1.2 Functional Requirements 4-3
4.2.1.2.1 Accept and Store Non-Fingerprint Supported Demographics and Charges 4-3
4.2.1.2.2 Send CCID Assignment Response 4-3
4.2.1.2.3 Send Pre-Fingerprinting Data to Live Scan Device 4-3
4.2.1.2.4 Record OCA in Interagency Index 4-4
4.2.1.2.5 Create and Track Notification of Fingerprints Needed 4-4
4.2.1.2.6 Record No Referrals 4-4
4.2.1.2.7 Return Charges to Prosecutor After Further Investigation 4-4
4.2.1.3 Transaction Profile 4-5
4.2.2 Booking Segment 4-7
4.2.2.1 Overview 4-7
4.2.2.2 Functional Requirements 4-8
4.2.2.2.1 Create/Update Record in DRM 4-8
4.2.2.2.2 Associate SID to Cycle 4-8
4.2.2.2.3 Associate FBI Number to Cycle 4-9
4.2.2.2.4 Notify Operator of Assigned CCID/CTN 4-9
4.2.2.2.5 Update ACCH 4-9
4.2.2.2.6 Print Disposition Information Sheet 4-9
4.2.2.2.7 Send Notification of Charges to Prosecuting Agency 4-9
4.2.2.2.8 Cease Notification 4-10
4.2.2.3 Transaction Profile 4-10
4.2.3 Prosecutor Segment 4-12
4.2.3.1 Overview 4-12

4.2.3.2 Functional Requirements 4-12
4.2.3.2.1 Process Prosecutor-Initiated Charges 4-12
4.2.3.2.2 Send CCID/CTN Assignment Response 4-13
4.2.3.2.3 Record Prosecutor Case Number in Interagency Index 4-13
4.2.3.2.4 Process Disposition 4-13
4.2.3.2.5 Process Amended Charge 4-13
4.2.3.2.6 Decline Charges for Further Investigation 4-13
4.2.3.2.7 Create Notification for Court Segment 4-13
4.2.3.2.8 Update ACCH 4-14
4.2.3.3 Transaction Profile 4-14
4.2.4 Court Segment 4-16
4.2.4.1 Overview 4-16
4.2.4.2 Functional Requirements 4-16
4.2.4.2.1 Refer Case to Different Court 4-16
4.2.4.2.2 Add or Amend Charges 4-17
4.2.4.2.3 Initiate Cycle in DRM 4-17
4.2.4.2.4 Send CCID/CTN Assignment Response 4-17
4.2.4.2.5 Record Court Case Number in Interagency Index 4-17
4.2.4.2.6 File Disposition 4-18
4.2.4.2.7 Update ACCH 4-18
4.2.4.2.8 Process Post-Disposition Changes 4-18
4.2.4.3 Transaction Profile 4-18
4.2.5 Custody and Supervision Segment 4-21
4.2.5.1 Overview 4-21
4.2.5.2 Functional Requirements 4-21
4.2.5.2.1 Notify Custodial or Supervisory Agency of Final Disposition 4-21
4.2.5.2.2 Process Custodial Intake Information 4-22
4.2.5.2.3 Make DNA Needed Determination 4-22
4.2.5.2.4 Process DNA Sample Taken Information 4-22
4.2.5.2.5 Process Inmate/Parolee Status Change 4-23
4.2.5.2.6 Process Incarceration or Parole Termination 4-23
4.2.5.2.7 Update ACCH 4-23
4.2.5.3 Transaction Profile 4-23
4.2.6 JAD Recommendations Related to Disposition Collection and Management 4-26
4.3 DRM DISPOSITION INFORMATION REPORTING 4-28
4.3.1 DRM Criminal History Cycle Management 4-28
4.3.1.1 Overview 4-28
4.3.1.2 Functional Requirements 4-29
4.3.1.3 Recommendations 4-29
4.3.2 Transaction Log Reporting 4-30
4.3.2.1 Overview 4-30
4.3.2.2 DRM Functionality 4-30
4.3.2.3 Functional Requirements 4-31
4.3.2.4 Recommendations 4-31
4.3.3 Disposition Scorecard Reporting 4-31
4.3.3.1 Overview 4-31
4.3.3.2 DRM Functionality 4-32
4.3.3.3 Functional Requirements 4-33
4.3.3.4 Recommendations 4-33
4.3.4 Custom Reporting 4-33
4.3.4.1 Overview 4-33
4.3.4.2 DRM Functionality 4-34
4.3.4.3 Functional Requirements 4-34
4.3.4.4 Recommendations 4-34
4.3.5 Reporting to ACCH 4-35
4.3.5.1 Overview 4-35

4.3.5.2 DRM Functionality 4-36
4.3.5.3 Functional Requirements 4-38
4.3.5.4 Recommendations 4-38
4.3.6 Creating and Sending Notifications 4-39
4.3.6.1 Overview 4-39
4.3.6.2 DRM Functionality 4-40
4.3.6.3 Functional Requirements 4-41
4.3.6.4 Recommendations 4-42
4.3.7 Person Search 4-42
4.3.7.1 Overview 4-42
4.3.7.2 Functional Requirements 4-43
4.3.7.3 Recommendations 4-43
4.3.8 JAD Recommendations Related to Disposition Reporting 4-43
4.4 DRM System and Enterprise Administration 4-46
4.4.1 Create and Maintain User Profiles 4-46
4.4.1.1 Overview 4-46
4.4.1.2 Create and Maintain Security Access 4-46
4.4.1.2.1 Security Access Overview 4-46
4.4.1.3 Create and Maintain Notification Preferences 4-46
4.4.1.3.1 Notification Management Overview 4-47
4.4.1.4 Functional Requirements 4-48
4.4.1.5 Recommendations 4-49
4.4.2 Maintain Code Tables 4-50
4.4.2.1 Overview 4-50
4.4.2.2 DRM Functionality 4-51
4.4.2.3 Functional Requirements 4-51
4.4.2.4 Recommendations 4-51
4.4.3 Maintain Translation Values and Interagency Index 4-51
4.4.3.1 Overview 4-51
4.4.3.2 DRM Functionality 4-52
4.4.3.3 Functional Requirements 4-53
4.4.4 Process Record Consolidations and Corrections 4-53
4.4.4.1 Overview 4-54
4.4.4.2 Functional Requirements 4-54
4.4.4.3 Recommendations 4-55
4.4.5 Logging 4-55
4.4.5.1 Overview 4-55
4.4.5.2 Functional Requirements 4-56
4.4.5.3 Recommendations 4-56
4.4.6 Transaction Validation and Management 4-56
4.4.6.1 Overview 4-56
4.4.6.2 Functional Requirements 4-57
4.4.6.3 Recommendations 4-58
4.4.7 JAD Recommendations Related to System Requirements 4-58
4.5 Non-Functional Issues 4-59

5 DATABASE MODEL 5-1

5.1 Overview 5-1
5.2 Proposed DRM Database Model 5-1
5.2.1 Criminal History Cycle 5-2
5.2.2 Interagency Index 5-2
5.2.3 Person Source 5-2

5.2.4 Person Source Types 5-2
5.2.5 Identification 5-2
5.2.6 Identification Type Code 5-2
5.2.7 Name 5-3
5.2.8 Identification Person Source Cross-Reference 5-3
5.2.9 Caution 5-3
5.2.10 Scars Marks Tattoos 5-3
5.2.11 DNA Sample 5-3
5.2.12 Person 5-3
5.2.13 Statute Code 5-4
5.2.14 Charge 5-4
5.2.15 Prosecutor Action Code 5-4
5.2.16 Charge Action Cross-Reference 5-4
5.2.17 Disposition Code 5-4
5.2.18 Disposition 5-4
5.2.19 Court Sentence Type 5-4
5.2.20 Court Sentence 5-5
5.2.21 Court Sentence Condition Code 5-5
5.2.22 Sentence Conditions Cross-Reference 5-5
5.2.23 Agency 5-5
5.2.24 Agency - Agency Cross-Reference 5-5
5.2.25 Address 5-5
5.2.26 Agency Jurisdiction Cross Reference 5-5
5.2.27 Event Type 5-6
5.2.28 Event 5-6
5.2.29 Subscription 5-6
5.2.30 Recipient 5-6
5.2.31 Recipient Type 5-6
5.2.32 Delivery Format 5-6
5.2.33 Notify 5-6
5.2.34 Notification Type Code 5-7
5.2.35 Transaction Log 5-7
5.3 ENTITY RELATIONSHIP DIAGRAM 5-7

6 APPENDIX A: JAD MINUTES 6-1

7 APPENDIX B: DISPOSITION REPORTING INTEGRATION CONCEPTS WHITEPAPER 7-1

8 APPENDIX C: CURRENT DISPOSITION REPORT FORM 8-1

1 INTRODUCTION

This Conceptual Design Document is one of two major deliverables for the Conceptual Design Phase of the Disposition Reporting Management (DRM) project sponsored by the Arizona Criminal Justice Commission (ACJC). The Conceptual Design will create the foundation for the development of the DRM system, supported by the System Architecture Document. Northrop Grumman Information Technology, with participation by eCorridor on the System Architecture, has prepared both documents for the ACJC under a subcontract with Spherion.

The Conceptual Design document contains the following sections:

Section 1 – Introduction: This section provides a general overview of the document, identifies the project approach and collection of system requirements, and includes an executive summary of the project's key findings.

Section 2 – Disposition Reporting Integration Concepts: This section describes the concepts behind criminal justice information integration that are used to support the goals of the DRM system.

Section 3 – Business Process Definitions: This section describes the business processes of collecting, updating and reporting disposition data; these are the processes that will be supported by the DRM system.

Section 4 – DRM System and Enterprise Requirements: This section describes the major system requirements for the new disposition reporting system, including the major functional areas for disposition information collection and management, reporting and notification management, and system administration. These administrative functions can be reused for the integration justice enterprise. The section includes a Functional Hierarchy Diagram depicts the functional activities for the DRM and the administrative functionality to be provided at the enterprise level.

Section 5 – Preliminary Data Model: This section also discusses a preliminary data model and a graphical representation of the logical data storage requirements.

Section 6, Appendix A – JAD Minutes: This appendix contains minutes of the meetings conducted with stakeholders.

Section 7, Appendix B – Disposition Reporting Integration Concepts. This appendix includes a whitepaper on the proposed change to the cycle identifier.

Section 8, Appendix C – Current Disposition Report Form: This appendix includes a copy of the current form used for disposition reporting.

1.1 PURPOSE

The DRM project was originally conceived and recommended in the *Arizona ICJIS Strategic Plan* (March 2002), which identified the need for improved accuracy and completeness of disposition reporting to the Arizona Computerized Criminal History system. The *Strategic Plan* described the DRM system as providing the tracking and workflow support automating the Disposition Report process and targeted the process as the "seed and business driver" for integration of justice information throughout the state. The DRM Conceptual Design effort is the first step in implementing the disposition reporting goals of the *Strategic Plan*.

The major components of the Conceptual Design Document are:

- Compilation of recommended system requirements from the ICJIS Strategic Plan and from Joint Application Design (JAD) meetings and interviews with stakeholders
- Discussion of integration concepts recommended for implementation in conjunction with the DRM system
- Process models and detailed narratives illustrating the proposed automated business process for disposition reporting
- Issues analysis related to user needs, expectations, and requirements
- High-level functional requirements for disposition reporting and a corresponding Functional Hierarchy Diagram (FHD)
- Preliminary view of the proposed data model using an Entity Relationship Diagram (ERD)
- Summaries of Joint Application Design (JAD) meetings

The ACJC, its key stakeholders, and Northrop Grumman worked together throughout this phase to identify requirements and create process, data, and functional models in preparation for the detailed design stage of the project. It was not the intent of this phase to develop all of the detailed data and functional requirements. Instead, the purpose of the Conceptual Design is to provide all participants and stakeholders with a common understanding of the overall system requirements and to create a solid foundation for the detailed development of the system in the future. This document defines specific capabilities and functions of an integrated disposition reporting system, and identifies the business and technology issues, user interface requirements, and

other non-functional issues that will need to be considered when writing specifications for the future reporting system.

1.2 EXECUTIVE SUMMARY

The goal of the recommended conceptual design for the Disposition Reporting Management system is to create an automated Disposition Report that will enable agencies to report their actions related to the processing of criminal charges, either through an electronic interface between local systems and the DRM or through a secure web site. The Disposition Report (sometimes called the "Yellow Sheet," a copy of which is included in Appendix C) contains disposition-related information from law enforcement agencies, prosecutors, and courts that is submitted to the Department of Public Safety as required by state statute (Arizona Revised Statutes 41-1750). By automating the Disposition Report, the DRM will replace the predominately paper-based manual system of reporting to the state. It will also allow agencies to share information on the status of a disposition, including any outstanding data requirements.

To support this project goal, the recommended design of the DRM has been developed to achieve the following objectives:

- Automate the workflow of the Disposition Report as it is processed in each agency and moved between agencies.
- Provide tracking and accountability in the collection and management of disposition data.
- Provide information on the status of disposition information, including notifications of events and required actions, on-line access to disposition status, and pre-formatted and ad-hoc reports of disposition activity.
- Provide concurrent access to this information to authorized users involved in the disposition reporting process throughout the criminal justice community.
- Enable the automated completion of disposition information by building on previous efforts to track arrest and criminal cycle data and updating those efforts to utilize the current standards of criminal history integration.
- Minimize the requirement for local agencies to make significant changes to their systems in order to participate by using open architecture and web-based services.
- Utilize business processing concepts to more easily accommodate future system changes required by changing business rules.

Critical aspects of the role that the DRM will play in the state's criminal justice enterprise include:

- The DRM is the first major project recommended by the ICJIS *Strategic Plan*; as such, it is intended to act as the seed and business driver for further integration of justice information in the state.
- The DRM capabilities supplement the existing functionality of critical statewide systems such as AZAFIS and ACCH. As an example of the distinction between the roles the systems play, the DRM collects disposition information and the ACCH continues to report the information and is the official record.
- The design as proposed is a day-forward system that manages criminal cycle events after implementation, allowing current systems to continue to manage existing cycles and minimizing the need for a significant conversion effort.
- The DRM utilizes proven key integration concepts for the consistent tracking of information, such as utilization of both cycle and charge tracking numbers and the integration of the State Statutes application through use of charge statute sequences.

In summary, the DRM will provide a secure, robust, comprehensive tracking mechanism for the entire criminal justice community to accurately record and manage charges over the lifetime of the criminal cycle. It will ensure that accurate and timely charge disposition information is reported to the ACCH, and it will accomplish this in conformity with the evolution of integrated justice models.

1.3 DEFINITION OF TERMS

The following list of terms and their definitions have been used throughout this document. Because terms are not used consistently throughout the state, this list was created to represent the most common usage on a statewide level. Wherever possible, state agency publications and state law have been used as a source of the definition. In addition, new terms introduced in this document that refer to system capabilities or integration requirements have also been included.

Term	Explanation
ACCH	Arizona Computerized Criminal History; the computerized database containing criminal history record information, maintained by the Department of Public Safety (DPS).
ACJC	Arizona Criminal Justice Commission
Affidavit of Probable Cause	Officer's Affidavit of Probable Cause to support the filing of charges. Also called a Form IV.
AOC	Administrative Office of the Courts

Term	Explanation
AZAFIS	Arizona Automated Fingerprint Identification System; an automated statewide fingerprint identification system used to store all ten-print cards and for searching fingerprint files and transmitting fingerprint images.
AZTEC	Administrative Office of the Courts' case management system.
Booking	For purposes of this Conceptual Design Document, the booking process describes the fingerprinting and reporting steps of booking and does not include the jail and inmate management aspects of booking.
CCID	See Criminal Cycle Identifier
Common Statute Number	Common Statute Number; a common statute number associated with each charge (CTN) in a criminal cycle (CCID) and identifying the specific statute for the charge.
CMS	Case Management System; common name used for court information systems.
Complaint	Formal written charge that a person has committed a criminal offense.
Complete Cycle	A criminal cycle that has all expected segments, including AFIS identification and disposition for each charge, as well as initiation of the corrections segment when required.
Court	Any state, county, and municipal court in the state.
Criminal Cycle	The criminal cycle represents a criminal case as it moves through the criminal justice process, and is composed of arrest, prosecutor, court, corrections and probation information.
Criminal Cycle Identifier	The criminal cycle identifier is proposed as a replacement for the AFIS-generated PCN when used in integrated justice data exchanges. The CCID would serve as the unique identifier for all cycles regardless of how the charges are initiated.
CSN	See Common Statute Number
CTN	Charge Tracking Number; a sequential number assigned to each charge in a criminal cycle (CCID); each charge linked to its appropriate statute through a common statute number (CSN).
Disposition	Information on an action taken by a criminal justice agency regarding a criminal charge; used in the context of completing the Disposition Report. See also Final Disposition.
Disposition Report	A Disposition Report is required from the disposition agency (arrest, prosecutor or court) pursuant to the Arizona Rules of Criminal Procedure (rule 37) for each person fingerprinted for a reportable crime pursuant to ARS Section 41-1750.
DOB	Date of Birth
DOC	Department of Corrections
DPS	Department of Public Safety
DRM	Disposition Reporting Management system
e-dispo	Electronic disposition reporting from the Administrator of the Courts case management system (AZTEC) to the Department of Public Safety Arizona Computerized Criminal History system (ACCH).
Final Disposition	Ultimate termination of the criminal prosecution of a defendant by a trial court, including dismissal, acquittal or imposition of a sentence. See ARS 13-4401 (10).
Fingerprint Data	Fingerprint images and associated data from the fingerprint card.
Form IV	See Affidavit of Probable Cause
Grand Jury	A group of citizens who usually serve a term of not more than 120 days to hear or investigate charges of criminal behavior.

Term	Explanation
Grand Jury Indictment	Formal, written accusation by a grand jury charging that a person or business committed a specific crime.
In-Custody Arrest	Arrest occurring for a new offense or offenses when the suspect is in custody for a different offense.
Information	An indictment or complaint.
Initiation of Charges	Action taken to initiate charges against an individual; certain events such as a physical arrest result in the initiation of charges. Plain English meaning; not a legal definition.
Intake	Processing an offender at the time of incarceration.
Interagency Index	An index that will provide criminal justice agencies the ability to locate pending disposition reports using search criteria beyond the PCN or CCID; other search criteria will include identifiers such State Identification Numbers (SID) and agency-unique identifiers, such as OCA. Concept was created in the *Arizona ICJIS Strategic Plan.*
JAD	Joint Application Design; a facilitated meeting in which system requirements and issued are discussed with stakeholders.
Law Enforcement Report	Report submitted by a law enforcement agency regarding an alleged offense; also called a police report, department report, or sheriff's report. Usually assigned an Originating Case Agency (OCA) number.
No Bill	A finding by a grand jury that the evidence presented was not sufficient to indict.
No File	A finding by a prosecutor that charges submitted to the prosecutor will not be pursued.
No Referral	A finding by a law enforcement agency that charges that have been initiated will not be referred to a prosecutor.
Non-Fingerprint Supported Records	Records that have not been associated with fingerprint identification.
Notice of Supervening Indictment	Court notice used if a defendant who is indicted by a Grand Jury has previously had an initial appearance under Rule 4.2; the court sends the defendant and defendant's counsel a notice of supervening indictment in lieu of issuing a warrant or summons.
Notifications	Notices sent by the DRM to agencies about key events in the disposition report process or to notify agencies of required data such as missing dispositions or fingerprints.
Offense Code Per Charge	Term used in Transaction Profiles to describe the statute related to an offense, regardless of whether the CSN or multiple fields are used for the transaction.
ORI	Originating Agency Identifier; the nine-character identifier assigned by the FBI to an agency.
PCN	Process Control Number; a unique alphanumeric number assigned to each arrest and non-arrest fingerprint card through AZAFIS.
Physical Arrest	An arrest event where the individual is arrested by law enforcement and brought to a booking unit for fingerprinting.
RMS	Records Management System; typically used to describe law enforcement incident and case management systems.
SID	State Identification Number; a unique number assigned to each individual in the ACCH record database.
Subscriptions	Subscription services allow system users to subscribe to receive specific

Term	Explanation
	information from the DRM and to be notified about specific events.
Summons	A legal document issued by the court directing law enforcement to notify the named defendant that a complaint has been filed and the defendant is required to appear and answer the complaint.
True Bill	An indictment by a grand jury; see Grand Jury Indictment.
TX10	DPS Transaction (TX) Message informing the end user (contributor) that a fingerprint transaction has been successfully processed by the FBI's IAFIS and providing the FBI number.
TX2	DPS Transaction (TX) Message containing the disposition report information returned after fingerprint data has been received by AZAFIS from a contributing agency.
TX8	DPS Transaction (TX) Message informing the end user (contributor) that a fingerprint transaction has been successfully processed by the AFIS; Type 01 prints will include the SID number.
Type 01 Fingerprints	Fingerprint type for arrests.
Type 22 Fingerprints	Fingerprint type taken at intake by the Department of Corrections
Warrant	An order directing law enforcement to bring a named person before the court.

1.4 PROJECT APPROACH AND REQUIREMENTS IDENTIFICATION

1.4.1 JOINT APPLICATION DESIGN AND OTHER PROJECT MEETINGS

To build the Conceptual Design for the DRM and to ensure that stakeholders' interests were represented in the project, ACJC and Northrop Grumman facilitated a series of JAD sessions throughout the state and conducted follow-up interviews with JAD participants and state agencies. A list of these meetings is shown in the following table:

Date	Meeting Type
April 7	Project Kickoff Meeting in Phoenix
April 27	Discussions with ACJC and Government Information Technology Agency
May 12	JAD I: Phoenix
May 13	Follow-Up Interviews: Department of Public Safety, and Administrative Office of the Courts
May 26	JAD II: Tucson
May 28	Follow-Up Interviews: Department of Public Safety and Phoenix Police Department
June 9	JAD III: Phoenix
June 11	Follow-Up Interview: Maricopa County

Date	Meeting Type
	ICJIS
June 16	JAD IV: Flagstaff
June 22	JAD VI: Yuma
June 24	JAD V: Phoenix
June 25	Follow-up Interview: Department of Public Safety
August 25	Follow-Up Interview: Department of Corrections
August 26	Follow-Up Interview: Department of Public Safety and DNA Lab
August 27	Follow-Up Interview: Administrative Office of the Courts
October 6	Follow-Up Meeting, Department of Public Safety

Minutes of the JAD sessions, which were all-day sessions with multiple participants, are included in Appendix A. Agencies participating in the JAD sessions are listed in the following table:

JAD Participating Agencies	JAD or Meeting Dates
Administrative Office of the Courts	Kickoff; JAD I; May 13 Interviews; JAD IV; August 27 Interviews
Arizona Department of Corrections	Kickoff; JAD III; August 25 Interviews
Arizona Department of Public Safety	Kickoff; May 13 Interviews; JAD III; May 28 Interviews; June 25 Interviews; August 26 Interviews
Arizona Department of Transportation	Kickoff; JAD I
Arizona Government Information Technology Agency	Kickoff; April 27 Meeting
City of Casa Grande	JAD III
City of Casa Grande Police Department	JAD III
Cochise County Superior Court	JAD II
Cochise County Sheriff's Office	JAD II
Coconino County Attorney's Office	JAD IV
Coconino County Courts	JAD IV
Coconino County Information Technology	JAD IV
Coconino County Sheriff's Office	JAD IV
El Mirage Police Department	Kickoff
Flagstaff Municipal Court	JAD IV

JAD Participating Agencies	JAD or Meeting Dates
Maricopa County Attorney's Office	Kickoff; JAD I
Maricopa County Clerk of Court	JAD V
Maricopa County ICJIS	Kickoff; JAD III; June 11 Interviews
Maricopa County Sheriff's Office	JAD I
Mohave County Courts	JAD IV
Mohave County Sheriff's Office	JAD IV
Phoenix City Prosecutor's Office	JAD I
Phoenix Municipal Court	JAD I
Phoenix Police Department	JAD I
Pima County Sheriff's Department	JAD II
Pinal County Attorney's Office	JAD III
Pinal County Information Technology	Kickoff; JAD III
Pinal County Sheriff's Office	JAD III
Pinal County Superior Court	JAD III
Santa Cruz County Superior Court	JAD III
Scottsdale City Court	JAD I
Scottsdale Police Department	Kickoff; JAD I
Tucson Police Department	JAD II
Yavapai County Attorney	JAD V
Yavapai County Superior Court	JAD V
Yuma County Justice Court	JAD VI
Yuma County Municipal Court	JAD VI
Yuma County Sheriff's Office	JAD VI
Yuma Police Department	JAD VI

1.4.2 REQUIREMENTS RECOMMENDATIONS

The information gathered during these meetings was incorporated in the development of the Conceptual Design in two ways. First, the information was used to develop high-level, generic process models for the key business functions to be supported by the DRM. Second, the information was used to help develop the functional requirements for the system and to expand on the general system requirements contained in the *Strategic Plan*. However, some of the recommendations will require policy decisions or legal analysis before being included in a final design; a determination will have to be made by the state whether or not to include the specific functionality being recommended. Other recommendations are not within the scope of the DRM or involved non-functional issues such as access and training. Nevertheless, all recommendations have been included in this document as documentation of stakeholder interests and of additional functionality that the state may want to consider in the future.

The recommendations of both these meetings and of the original *Strategic Plan* are summarized in the following table.

Please note that the current term "PCN" was used during the JAD sessions to describe the unique identifier given to a criminal history cycle. Both PCN and the proposed new terminology – "CCID" for Criminal Cycle Identifier – have been used in the following table. This has been done to avoid confusion as these recommendations are moved forward in the DRM system planning.

Recommended Requirements for the Disposition Reporting System[1]

Requirement Type	No.	Recommendation	JAD I	JAD II	JAD III	JAD IV	JAD V	JAD VI	Strategic Plan[2]	Interviews
Access	1	Allow access on mobile terminals.		√						
Access	2	Require passwords for access to the system						√	√	
Access	3	Provide access via the web by authorized users for queries and data entry.						√		
Access	4	Consider allowing limited public access, at least for victims.						√		
Automate Workflow	5	Automate the movement of the Disposition Report from criminal justice agency to the next as the individual moves through the arrest and adjudication cycle; automate trigger points for actions.	√	√		√			√	
Automate Workflow	6	Assist with reducing the backlog of Disposition Reports; create a web page to enter backlogged reports.	√	√						
Automate Workflow	7	Reduce duplicate data entry.	√		√				√	
Automate Workflow	8	Minimize the potential for data entry errors; reject errors immediately to require correction (real-time error checking).	√	√	√	√	√	√	√	
Automate Workflow	9	Assist with matching cases from one agency system to the next, as the case moves through the criminal justice process.	√							
Automate Workflow	10	Notify the appropriate agency to take action on missing or incomplete data.	√							
Automate Workflow	11	Consider/allow responsibility for creating a Disposition Report for some types of cases to be moved from law enforcement agencies to other agencies.		√						
Automate Workflow	12	The system should track arrests that are following a parallel course in different courts.		√					√	
Automate Workflow	13	Allow entry of agency data out of sequence and track								

[1] Recommendations that are outside the current scope of the project are identified at the end of the table

[2] Actual or similar requirement identified in the Arizona ICJIS *Strategic Plan*

Requirement Type	No.	Recommendation	JAD I	JAD II	JAD III	JAD IV	JAD V	JAD VI	Strategic Plan[2]	Interviews
		responsibility for the missing data.			√				√	
Automate Workflow	14	Simultaneously perform data entry on the same charge item (same PCN/CCID and charge in the database, count) by multiple users							√	
Automate Workflow	15	Allow agencies to correct entries but ensure that the record can be matched with the DPS record; the original contributor of data should have the authority to change a record. Authority to change data fields should be strictly controlled by agency type and user type.			√	√		√		
Automate Workflow	16	Allow modifications to dispositions that are made by the courts as a result of compliance or non-compliance with probation			√	√				
Automate Workflow	17	Include case referral capability to allow agencies to refer the Disposition Report to the appropriate agency to take the next action.				√				
Automate Workflow	18	An AKA or alias should be included.						√		
Automate Workflow	19	Consider using existing "transfer to" code in court automated systems to notify DRM of court transfers								√
Automate Workflow	20	Correct disposition reports errors on-screen and resubmit them for approval/acceptance							√	
Automate Workflow	21	Track and manage pre-identification Disposition Reports for cite/release and other non-arrest/booking scenarios in which charges are brought							√	
Automate Workflow	22	Assign a final disposition charge(s) as needed							√	
Automate Workflow	23	Complete dispositions for multiple PCN/CCIDs with a single live scan event							√	
Automate Workflow	24	Determine the count number for additional charges that may be amended to a disposition report (PCN/CCID)							√	
Automate Workflow	25	Declare that work on a given section of the disposition report is complete							√	

Requirement Type	No.	Recommendation	JAD I	JAD II	JAD III	JAD IV	JAD V	JAD VI	Strategic Plan[2]	Interviews
Automate Workflow	26	Receive rejected dispositions and DPS transmittals on-line							√	
Automate Workflow	27	Track individual charges associated with cases returned after Appellate Review and submit updates to DPS							√	
Information Sharing	28	Provide access to other agencies' disposition report data (particularly prosecutors, who would like to know if another jurisdiction also has an active case on the same individual); allow access to status of that disposition report.	√	√	√	√	√	√	√	
Information Sharing	29	Notify DOC of new sentencing events so that DOC does not release an individual that has been re-sentenced			√					√
Information Sharing	30	Standardize processing procedures and common terms used by the criminal justice community in the process of disposition reporting.				√				
Information Sharing	31	Add comments to Disposition Report or charges to provide important information to other criminal justice agencies							√	
Information Sharing	32	View court sentencing results for completed Disposition Reports and charges							√	
Information Sharing	33	Indicate DNA sample availability or include an indicator that a sample is needed.			√			√		√
Information Sharing	34	Indicate DNA sample has been tested.								√
Information Sharing	35	Show link between fingerprints and DNA sample for identification purposes								√
Information Sharing	36	Share additional information from the Disposition Report with DOC prior to or at time of intake.								√
Interfaces	37	Offer data feeds based on the interest of a specific agency.			√					
Interfaces	38	Interface with other electronic systems (at the local level).	√	√	√	√	√	√		
Interfaces	39	Interface with AZTEC and other court systems.				√				
Interfaces	40	Use standard XML transactions for data feeds.		√	√					
Interfaces	41	Make it convenient for current systems to push and pull data.		√						

Requirement Type	No.	Recommendation	JAD I	JAD II	JAD III	JAD IV	JAD V	JAD VI	Strategic Plan[2]	Interviews
Interfaces	42	Allow flexibility of transport modes of data from local systems.			√					
Notifications	43	Notify courts when fingerprints need to be ordered when the individual appears in court.	√	√			√	√	√	
Notifications	44	Notify law enforcement agencies when fingerprints are needed for a case.					√	√	√	
Notifications	45	Notify agencies of the final disposition.		√	√			√		
Notifications	46	Notify DOC of all dispositions involving incarceration, using a pre-formatted report.								√
Notifications	47	Consider e-mail notifications with links that must be selected to discontinue the notification, as a method to encourage the agency to review the information.			√					
Notifications	48	Include op in/op out features in notifications.			√	√		√		
Notifications	49	Notify agencies if a Disposition Report is beyond the allowable age for closure (depending on state policy on closing Disposition Reports).			√					
Notifications	50	Age by days each charge activity or charge event from the date of final disposition using a new 72-hour standard to identify tardy Disposition Reports							√	
Notifications	51	Notify prosecutors if a person has been arrested on subsequent charges.				√				
Notifications	52	Notify DOC of arrests of persons under DOC supervision								√
Notifications	53	Notify courts and law enforcement that a scheduled release of a DOC inmate has taken place								√
Notifications	54	Notify judges if new charges have been issued that violate an offender's conditions of probation or release.				√				
Notifications	55	Inform law enforcement when the County Attorney files a case				√				
Notifications	56	Notify agencies of time-sensitive deadlines.						√		

Requirement Type	No.	Recommendation	JAD I	JAD II	JAD III	JAD IV	JAD V	JAD VI	Strategic Plan[2]	Interviews
Notifications	57	System should not notify agencies of successful data transactions.					√			
Notifications	58	Get feedback from the process that work has been submitted successfully							√	
Notifications	59	"Op out" feature must have a end date after which an agency can no longer op out of notifications (DPS)								√
Notifications	60	If the recipient of a required notification does not take the required action, the notification should be elevated to someone in a higher level of responsibility in the agency (DPS)								√
Reporting	61	Produce reports on what the state has in each jurisdiction, so that each agency can verify what has been sent to their office; produce reports showing dispositions that DPS is expecting and has not yet received.	√		√	√				
Reporting	62	Show the current status of a disposition followed by a summary of the processing events to date; allow the user to drill-down for detailed information.				√				
Reporting	63	Allow prioritization of agency Disposition Report activity reports by seriousness of the charges and other factors.			√					
Reporting	64	Provide a common report generated for all agencies for agency Disposition Report activity reports.			√					
Reporting	65	Create reports on outstanding dispositions that are available to authorized users; provide an option to receive the report automatically or upon request.				√				
Reporting	66	Allow users to search for records by PCN/CCID or name and DOB. (Strategic Plan added search by agency case numbers)						√	√	
Reporting	67	Check agency's success rate for submission of disposition reports							√	
Reporting	68	Print a snapshot of the Disposition Report form at any stage								

Requirement Type	No.	Recommendation	JAD I	JAD II	JAD III	JAD IV	JAD V	JAD VI	Strategic Plan[2]	Interviews
		of the process, with time, date and name stamped by the system							√	
Reporting	69	Produce agency exceptions reports including corrective action required by the agency							√	
Reporting	70	View all Disposition Reports and charges in progress for a given person based on common SID; view all pre-booking records and charges in progress for a given person based on common demographic data and numbers like social security, MVD ID							√	
Security	71	Information on Grand Jury indictments must be strictly limited and not available to all users of the system.						√		
Security	72	Perform only those tasks permitted for their user profile and security level							√	
Tracking and Accountability	73	Assign missing agency numbers to records where not provided via a system interface or other automated update							√	
Tracking and Accountability	74	Track all changes made by agencies to correct previous entries.			√					
Tracking and Accountability	75	Identify missing and incomplete Disposition Reports.	√	√			√		√	
Tracking and Accountability	76	Generate a Disposition Report for charges that are initiated without fingerprints despite the potential problem of positively identifying the person adjudicated with the original suspect.	√							
Tracking and Accountability	77	Inform agencies of the current status of a Disposition Report.		√						
Tracking and Accountability	78	Help clarify names and aliases for the courts.		√						
Tracking and Accountability	79	Identify records that are not associated with fingerprints.			√		√			
Tracking and	80	Track record entries and changes by User IDs, so that								

Requirement Type	No.	Recommendation	JAD I	JAD II	JAD III	JAD IV	JAD V	JAD VI	Strategic Plan[2]	Interviews
Accountability		training and performance issues can be addressed.			√					
Tracking and Accountability	81	Provide tracking to minimize duplicate bookings.			√	√				
Tracking and Accountability	82	Track charges amended by prosecutors.			√					
Tracking and Accountability	83	Identify the agencies involved in a case so that contacts can be made if further inquiries are needed					√			
Tracking and Accountability	84	Recall and delete tracking system Pre-Booking records prior to PCN/CCID generation, or other agency data entry or update of a Disposition Report							√	
Tracking and Accountability	85	Audit the disposition reporting tracking system for edit history, status, user access, and processing history, including printing of Disposition Report form copies							√	
Training/System Administration	86	Allow training on-line; certify for system access on-line							√	
Training/System Administration	87	Access system help, rules, and procedures on-line							√	
Outside Current Project Scope										
Automate Workflow	88	Consider including all incidents including non-reportable charges				√				
Information Sharing	89	Inform interested agencies if there is an arrest on a warrant (specifically agencies that are not involved in the specific disposition event, but other interested agencies).		√						
Information Sharing	90	Include a blood test taken indicator for DUI cases.			√					
Information Sharing	91	Consider a tie-in between the Disposition Reporting system and the new probation system to be installed in courts.				√				
Information Sharing	92	Consider tracking outstanding warrants, sentencing information, and court dates.				√		√		

Requirement Type	No.	Recommendation	JAD I	JAD II	JAD III	JAD IV	JAD V	JAD VI	Strategic Plan[2]	Interviews
Interfaces	93	Consider a mug shot interface to add pictures to the Disposition Report.		√				√		
Interfaces	94	Consideration should be given to reporting felonies to the County Recorder or Secretary of state to meeting reporting requirements regarding voter registration eligibility.					√			
Interfaces	95	Consideration should be given to using the system to report motor vehicle violations to MVD/DOT.					√			
Notifications	96	Consideration should be given to including automation of victim notification requirements as part of the system.						√		
Notifications	97	Include address as a field and notify affected agencies when a change of address has occurred.						√		
Notifications	98	Notification that an offender scheduled to be turned over to DOC has been picked up by federal authorities and will not be incarcerated by DOC								√
Training/System Administration	99	Apply for TOC IDs on-line							√	

1.5 PROJECT REFERENCES

In addition to the information gathered from stakeholders and state agency subject experts and the *Strategic Plan*, the following state references were used as supplemental input to the project effort:

- Arrest and Disposition Information Manual – Criminal History Reporting, Arizona Department of Public Safety, June 2002
- Rules of Criminal Procedure, Arizona Supreme Court
- *Guide to Arizona Courts*, Arizona Supreme Court (http://www.supreme.state.az.us/guide/)
- Arizona Revised Statutes
- Maricopa County Disposition Report Map, Maricopa County ICJIS, June 11, 2004
- *Pinal County Data Process Flow*, Pinal County Justice Integration Project Office, December 29, 2003
- Criminal Justice Records Improvement Plan 2004, Arizona Criminal Justice Commission, March 2004
- *Report of the XML Data Dictionary Subcommittee,* Arizona Criminal Justice Commission, November 6, 2003
- *GSP III – Arizona Fingerprint Data Router Interface Control Document (ICD),* Arizona Department of Public Safety, February 25, 2004
- *Scanning Devices- GSP Interface Control Document (ICD),* Arizona Department of Public Safety, February 25, 2004
- *A Tracking System Feasibility Study,* Arizona Criminal Justice Commission, August 1996

2 DISPOSITION REPORTING INTEGRATION CONCEPTS

The complete accurate and timely collection of criminal history information is seen as a vital role in supporting public safety activity. The integration of criminal history information from various sources has been an issue that has perplexed most, if not all States engaged in collection of the information. It has also had a significant national impact. Several initiatives are underway with the goal of standardizing the data that is common to criminal justice practices, and to provide a means for organizing and displaying that data. The reality is that the ability to integrate disparate pieces of information from disparate sources in a means that is accurate, reliable, and useable by the criminal justice and civil communities is not a simple task. This challenge is exasperated by the fact that with criminal history data, a person's name, date of birth and other identifiers are not necessarily static, but are the product of what the person indicates that they are at the time the information is requested. The only reliable means to achieve positive identification is through use and comparison of biometrics such as fingerprint images. Since it is cost prohibitive to obtain fingerprint images at every point of contact with a criminal offender, other means must be used to link these pieces of information.

The sections that follow will give further explanation of the business constructs and requirements for integration, as well as defining a solution to meet those requirements. Additional information on the proposed solution is included in Appendix B, Disposition Reporting Integration Concepts Whitepaper.

2.1 INTEGRATION REQUIREMENTS

The collection of information that makes up criminal history data comes from a variety of sources, and typically from very disparate systems. Each of these systems is rightly designed to track and maintain data that is important to the specific agency's business requirements. Therefore, when one begins talking about integrating that data into a common set of information that can be called the entire criminal history picture, some concepts of common tracking numbers must be implemented. In Arizona, the Process Control Number (PCN) is utilized as a first step to matching this data from the various sources.

In order to fulfill its role as a tracking and gathering mechanism for complete and accurate disposition data to give to the ACCH for dissemination, the DRM must go further than the PCN. The current practice of using the PCN adequately tracks criminal cycles initiated by arrests where fingerprints are

obtained. However, the role of the DRM requires an expanded tracking ability, namely:

- The ability to track criminal cycles not initiated a fingerprint event; and
- The ability to track criminal history data at the charge level.

.

It must address the need to associate particular dispositions with particular charges and counts within a specific case. Since many arrests result in multiple police charges, and since initial police charges may be modified or augmented at later stages of the case (for example, after prosecutor screening, grand jury action or plea bargaining), it is common for repositories to receive court dispositions that do not match the charges initially reported. The DRM must incorporate a means to address this issue, and to make the associations so that a complete record can be achieved and reported to the criminal history repository.

While solving the problem of complete and accurate reporting, the DRM has another integration task. It is the task of ensuring the ability to track the collected information back to the source of that data. The DRM must be able to provide an audit trail that allows the data to be correlated back to the source database, and must also ensure that agencies only have access to see appropriate data and to modify only the data that belongs to the specific agency.

In sum, the DRM must address and successfully meet the following integration requirements:

- Utilization of a unique cycle tracking number
- Ability to track charges and counts at a detailed level for completeness and accuracy in reporting.
- Incorporation of a means to tie the integrated data back to the origination of that data.
- Security to allow only appropriate access to view and/or change data.
- Ability to send complete data in an appropriate format to the ACCH for dissemination.

2.2 RECOMMENDED SOLUTIONS

The concepts that Northrop Grumman has found to be an effective means to meet the integration requirements and thus make the appropriate associations of data include the following:

- Establishment of a Criminal Cycle Identifier
- Establishment of Charge Tracking Numbers
- Establishment of Interagency Indexing Information

Each of these concepts is explained in the sections that follow.

2.2.1 CRIMINAL CYCLE IDENTIFIER

The criminal cycle is the concept of an enterprise criminal justice case. This cycle is perhaps one of the most important and least understood notions in the criminal justice enterprise and the integration of its data. As a business concept, the criminal cycle is composed of arrest, prosecutor, court, corrections and probation information. These elements of the cycle are often referred to as the criminal cycle segments. The criminal cycle is initiated when charges are associated to an individual regarding an identified incident. Common means AZ criminal justice agencies use to initiate a case are summons, arrest reports, and grand jury indictments.

While being able to refer to a criminal cycle with a single identifying number is crucial to communication regarding that cycle, several of the current systems in a typical criminal justice enterprise are not constructed to store or communicate this common Criminal Cycle Identifier (CCID). Each agency has its own case identifying practice and set of identification numbers; for example, law enforcement record management systems use originating case agency number (OCA), prosecutors have case numbers, and courts use docket numbers. Northrop Grumman has found that the only means to associate exchanges relating to these disparate tracking identification numbers is through linking them utilizing the criminal cycle concept.

In the State of Arizona, inroads have already been taken at this level, where the PCN identifies the criminal cycle and is statutorily required. However, because the PCN is also an identifier for a specific set of fingerprint images, using the PCN for all initiated charges including those that are not initially associated with fingerprints can cause confusion as cycles are tracked over time. Although the PCN should and must continue to be assigned to fingerprints and used in current AFIS business processing, the CCID will replace the PCN as the identifier for all cycles. More detailed information on this proposal is included in Appendix B.

The DRM will expand the visibility and further enable the use of this concept, such that when an initiating document (data) is received by the DRM, it will assign the unique tracking number —the Criminal Cycle Identifier, or CCID-- identifying the specific cycle against which the document should be associated. Like the current procedures for the PCN, this CCID will be

communicated to all agencies sharing exchanges related to the initiating document (that is, all agencies who would be in contact with the typical Disposition Report or "Yellow Sheet"). The DRM will require that all automated agency responses or confirmations relating to the event contain the CCID so that the DRM can accurately match the information to the correct criminal cycle. The DRM will assign the CCID much like the Live Scan units currently assign the PCN. Therefore, for most agencies, the change to CCID from PCN should be transparent.

2.2.2 CHARGE TRACKING

While the linking of agency cases can virtually ensure that related information is associated with the right criminal cycle, the current PCN cannot in and of itself provide the basis for completeness of information, which can only be achieved through reliably associating particular dispositions with particular charges and counts within a particular cycle. Since many arrests result in multiple charges, and since initial police charges may be modified or augmented at later stages of the case (for example, after prosecutor screening, grand jury action or plea bargaining), it is common for agencies who receive court dispositions to not be able to match them to the charges initially reported.

This problem has been successfully addressed by implementing a refinement of the unique-number tracking system, usually referred to as the Charge Tracking Number (CTN). Under this approach, each charge in a particular case is assigned a number (01, 02, 03, for example). The charge information can be further refined by linking each charge to its appropriate statute through a common statute number (CSN).[3] These additional two numbers, in combination with the tracking number for the cycle (CCID), are used in all subsequent data exchanges. If, for example, a charge is dropped or modified by the prosecutor, this action is reported to the DRM with the specific CTN and CSN.

This type of communication allows the DRM to track the charge from initiation and to accurately depict what has happened to the charge as the cycle has progressed through the process. If, for example, the prosecutor adds

[3] The Common Statute Number does not have to be included in the cycle tracking sequence in order to realize most of the benefits of the expanded cycle tracking proposal. The identification of a statute as it appears at the time of the offense can be accomplished by including the effective and expiration dates of the particular statute describing the crime, which requires multiple fields for the statute identification. The CSN, in contrast, is a single field identifier for the statutory offense. Either approach can be used to complete the cycle identification. However, the use of the CSN as opposed to the multiple field approach will help track the exact nature of the offense over time as statute language changes due to legislative action; in addition, it does not require that all local systems contain and track multiple fields.

new charges, these charges are communicated to the DRM through use of the CCID and CSN, where they are assigned new Charge Tracking Numbers (CTNs) and the information is reported to the court. Court disposition information is then reported by tracking number (CCID), charge number (CTN), and statute number (CSN), and a disposition can thus be reported and recorded for each charge. This enables the DRM to account for each charge in the criminal cycle and eliminates a primary source of uncertainty common in information exchange.

The combination of the CCID, CTN, and CSN will provide the following benefits:

- Tracking cases from initiation to final disposition
- Accurate disposition for tracking criminal history
- Determining case status (when and if a case is closed)
- Tracking transformation of the charges as they progress through the system

For purposes of this document, it is assumed that the CSN will be used as part of the CCID sequence. However, if CSN is not implemented, it is assumed that the multiple field approach – called Offense Code Per Charge – will be used instead.

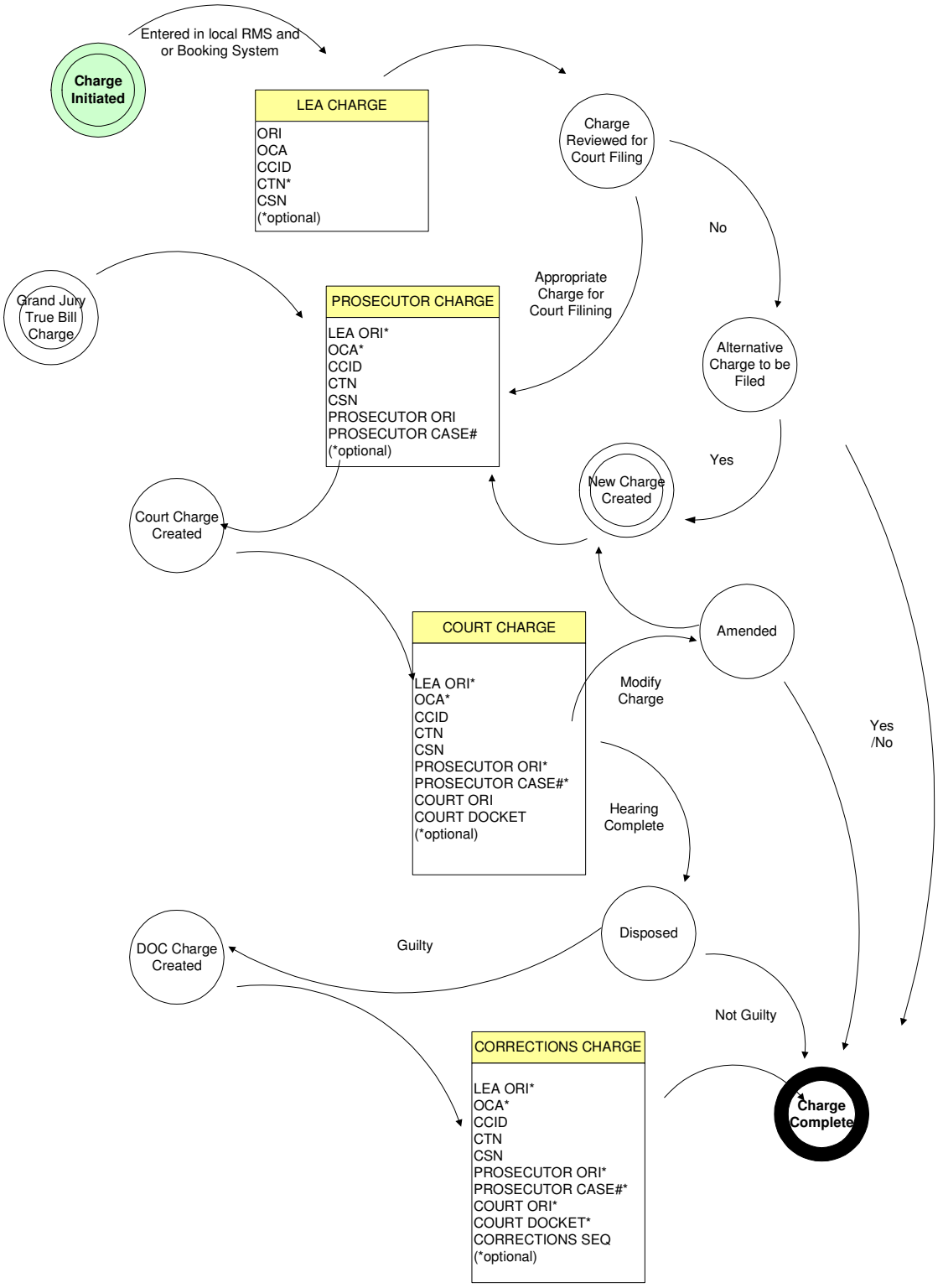
2.2.3 INTERAGENCY INDEXING

Another important part of the integration solution is the ability to store and match identification information from the entities who own/share the data so that the DRM can manage the exchanges between the agencies in the appropriate manner.

For example, when a law enforcement agency informs the DRM of a summons event, the DRM system will assign a CCID and save the OCA from the LEA, capturing the agency ORI and the OCA against the CCID. When the prosecutor response is received, the case number assigned by the prosecuting agency and that ORI will also be saved in relation to the CCID. When the prosecutor sends filing decisions regarding their case number to the LEA, the DRM will have the ability to look up the correct OCA to communicate in the exchange so the LEA can properly store the information in their own application.

This type of identification storage is known as interagency indexing and was one of the more significant recommendations in the *Strategic Plan*. It allows the DRM to effectively communicate with contributing agencies, utilizing identification numbers familiar to their systems, and still maintain the tracking functionality necessary for integration.

The diagram that follows depicts how the tracking numbers are utilized in the DRM, and the flow of information that would progress among the agencies involved.



Use of Agency Tracking Numbers in the DRM

3 BUSINESS PROCESS DEFINITIONS

3.1 OVERVIEW

This section describes the various business processes that will be supported by the DRM in collecting, updating, and reporting disposition data

3.1.1 IDENTIFICATION OF BUSINESS PROCESSES SUPPORTED BY THE DRM

Based on the information gathered during the JADs and other interviews, the high-level processes described in this section represent the events in which criminal charges are initiated and charge tracking begins. The term "initiation of charges" reflects the meaning in layman's terms and is not intended to be a legal definition. The processes that describe the initiation of charges that will be reported to the DRM are:

- Physical Arrest and Booking
- Cite and Release
- Law Enforcement Report Submitted for Prosecutor Review
- Grand Jury Indictment
- Information Filed Directly in Superior Court
- Court Initiated Charges

Additionally, the document addresses other important processes – or, more appropriately, sub-processes – that impact disposition reporting or provide additional information related to criminal cycles. These include:

- Court Transfers
- Custody and Supervision Status
- DNA Sample Data

These last processes can be sub-processes that may occur within the life cycle of a criminal charge. For example, the DNA Sample Data is actually a sub-process that has been analyzed separately to ensure that this type of data – which is not normally part of the disposition reporting responsibility – can be collected and reported during the criminal history cycle. Similarly, the Court Transfers process flow could occur within other processes when a case is moved from one court to another during the adjudication process.

It is important to point out that a criminal case may move through parallel paths or repetitive cycles as it moves through the criminal justice process. For example, events such as Initial Appearance may be going on simultaneously

as a prosecutor is making decisions on individual charges, declining some and preparing to file on others. A change in the conditions of a case can cause the sequence to change or even begin again. Additionally, the technical capability of agencies differs, so that some agencies will be able to report disposition data in near-real time (including reporting over a web browser, for instance), while others will report less frequently. In order to meet these challenges, the DRM system must be capable of accepting information out of sequence as it tracks the general business process flows described in this section.

The business processes described in this section do not attempt to capture every step in the criminal history cycle. Instead, the processes focus on the steps in a cycle that can or should result in the submission of data to the DRM system. These processes reflect best practices collected during the JAD sessions and do not represent any particular jurisdiction's current procedures. Northrop Grumman recommends that the state capture more detailed information on the data exchanges involved in these processes during the detailed design phase of the DRM project. The SEARCH Justice Information Exchange Model (JIEM) tool is recommended for this purpose; this web-based modeling tool can assist the state in capturing detailed information on the processes, events, agencies, data and conditions associated with the integration of criminal justice information. Additional information on JIEM can be found on the SEARCH web site at http://www.search.org/programs/technology/jiem.asp.

3.1.2 Interaction Between the DRM, ACCH, and AZAFIS

The reporting of criminal disposition data to the Arizona Computerized Criminal History system (ACCH) is linked to the submittal of fingerprint images and the associated demographic data and charge data to the Arizona Automated Fingerprint Identification System (AZAFIS). This link exists because the ACCH will only store criminal history data that is fingerprint-supported.

The link between the initiation of charges and reporting to ACCH is closest for cases that begin with a physical arrest followed by booking. However, when charges are initiated prior to a physical arrest, such as with a Cite and Release, criminal history data is available for collection before the identifying event of fingerprinting occurs. Because a substantial percentage of missing dispositions involves cases that are not initiated by a physical arrest, the DRM will provide a reliable method to track the progress of these cases and notify agencies of the need to obtain fingerprints so that the record can be reported to ACCH.

One of the desired outcomes recommended in the AZICJIS *Strategic Plan* is to ensure complete and accurate criminal history records are available to those criminal justice and non-criminal justice agencies that depend on this information for making decisions. The only true way to track charges throughout the disposition reporting process and ensure that the resulting records are as complete and accurate as possible is to begin that tracking process at the time that charges are initiated, and to use an identifier that meets the integration principles outlined in Section 2. It is the initiating event that must establish the Criminal Cycle Identifier or CCID to prepare the systems for the tracking and management of all future disposition information. The PCN will continue to be used to tie the cycle to fingerprint images and to meet processing requirements within DPS and current DPS business processing related to the PCN will not have to be changed.

The DRM, therefore, will not replace the current interaction between the ACCH and the AZAFIS. Instead, the DRM will provide a unique cycle identifier for all cycles, regardless of whether the initiating event corresponds immediately with fingerprinting. Besides providing this means to capture criminal justice information at the point in which it is originated, the DRM adds the level of tracking necessary for successful integration. It accomplishes this through the assignment of charge tracking numbers for all charges reported at the initiation of the cycle, as well as later charges that might result from amendments, or other agency actions. This level of tracking is essential to the accuracy and completeness of the reporting. Because the DRM is responsible for tracking and management of the cycle, it is imperative that the DRM assign the tracking numbers.

Upon initiation of a cycle, the DRM will create the cycle and charge tracking numbers, returning the assignments back to the initiating agency. If the cycle is a physical arrest and is being initiated with a fingerprinting event, the DRM will send the newly created CCID to the Live Scan unit so that it can be included with the fingerprint record along with the PCN. When fingerprints are taken for a cycle that has already been created and for which fingerprints are finally being added, the DRM will send the existing CCID sequence to AZAFIS.

In this case, the fingerprint technician will be able to query the DRM and load the charge data (including the DRM tracking numbers) into the LiveScan device through use of the existing CCID, saving key entry time and potential for data entry error.

3.1.3 STATUTORY AND RULE REQUIREMENTS

Statutory requirements related to the collection, reporting, and release of criminal history information have an impact on the processing of disposition

data. Arizona Revised Statute (ARS) § 41-1750 requires criminal justice agencies to report criminal history information to DPS. Criminal history and fingerprinting is required for felony offenses, offenses involving domestic violence as defined in § 13-3601, or a violation of Title 13, Chapter 14 (sexual offenses) or Title 28, Chapter 4 (driving under the influence). Fingerprinting for other offenses is allowed but is done at the discretion of the arresting agency.

In addition to these statutory requirements, the Arizona Rules of Criminal Procedure detail specific requirements related to collection and reporting of criminal history data, including fingerprints. Rule 3.2 allows the prosecutor to request an order from the court that a suspect be fingerprinted. The same rule requires the court to order fingerprinting in the case of a felony offense, a violation of Title 13, Chapter 14, or Title 28, Chapter 4 or a domestic violence offense as defined in § 13-3601. Rule 37 governs the reporting of court dispositions to DPS.

These requirements have been incorporated in the business process flows detailed in this section of the Conceptual Design Document, helping make the processes reflect best practices.

3.1.4 COMMON DOCUMENTS AND DATA SETS

Documents and data sets that are commonly exchanged between agencies during the disposition reporting process were identified during the JAD sessions and follow-up interviews. These documents or data sets contain the individual data elements that may become part of the Disposition Report. The documents listed are not intended to be a comprehensive list of all documentation exchanged; instead, they represent information typically exchanged during the movement of disposition data from agency to agency.

A summary of this information and the processes in which the information appears is included in the following table:

Documents and/or Data Sets Commonly Used in the Exchange of Disposition Data

Document or Data Set	Physical Arrest	Cite and Release	LEA Report Submission	Grand Jury Indictment	Superior Court Filing	Court Initiated Charges	Court Transfers	Custody and Supervision	DNA Tracking
Case File							√		
Charge Request	√								
Citation		√							
Complaint			√		√				
Court Disposition	√	√	√	√	√	√		√	√
Court-Filed Charges						√			
Decline Charge	√	√	√						
Decline/Return for Further Law Enforcement Investigation	√	√	√						
DNA Sample Capture Data									√
DNA Sample Testing Status									√
Fingerprint Card Data	√	√	√	√	√	√			
Form IV			√						
Grand Jury Indictment/True Bill				√					
Inmate or Parollee Status								√	
Intake Fingerprint Data								√	
Law Enforcement Report	√			√					
No Bill				√					
No File Disposition	√	√							
No Referral Disposition	√	√							
Notice of Supervening Indictment				√					
Prosecutor Charge Decision	√	√	√				√		
Summons			√	√		√			
Warrant			√	√		√			

3.2 DESCRIPTION OF BUSINESS PROCESSES

3.2.1 PHYSICAL ARREST AND BOOKING

The Physical Arrest and Booking process, viewed in the context of the processes to be supported by the DRM, consists of three types of events:

- Physical Arrest
- In-Custody Arrest
- Citation and Fingerprinting

The term "booking" is used here to mean the fingerprinting of a suspect and the transmission of fingerprint images and fingerprint card data to the state.

3.2.1.1 High-Level Process Flow

The physical arrest and booking process starts with an arrest event followed by booking of the suspect. The state is notified of the initiation of charges when the suspect is brought to a booking unit and the fingerprints, demographic data, and associated charges are submitted to AZAFIS, which forwards the arrest information to the DRM. The DRM assigns a CCID and charge tracking numbers, creates a criminal cycle within the DRM for the arrest event, and then forwards the information to the ACCH. For purposes of this Conceptual Design Document, the booking process describes the fingerprinting and reporting steps of booking and does not include the jail and inmate management aspects of booking.

The physical arrest and booking process actually encompasses three possible scenarios: the arrest event followed by booking, an in-custody arrest leading to new charges, and a Citation event where fingerprints are taken immediately upon issuance of the citation. Each of these three scenarios is discussed below as the entry point of criminal cycle information into the DRM.

3.2.1.2 Physical Arrest Event

When the arrest event and subsequent booking is the first step in a new criminal cycle, there will be no information pertaining to this arrest or charge data in the DRM at the time of booking. In these cases, the booking unit will process fingerprints, charge data and demographics through the Live Scan or Card Scan. In addition to its current transaction flow, AZAFIS will forward copies of standard return transaction messages TX2, TX8 and TX10 to the DRM, which will initiate new charge records in the DRM with the CCID, SID and the FBI number (if available). In turn, the DRM will notify the booking agency of the CCID and the charge tracking number assigned to

each charge by the DRM. Agency specific tracking numbers such as booking number or common case number will be retained in the DRM interagency index and linked to the specific CCID to facilitate future communications with the charge-initiating agency.

3.2.1.3 In-Custody Arrests

A suspect currently in custody may be arrested and booked for a criminal event that is unrelated to the arrest for which they were originally being held. This new arrest is processed through the LiveScan just as any other physical arrest, even though they have already been positively identified and assigned or associated to an SID. The appropriate printing and assignment of the AFIS PCN will be initiated by a LiveScan Transaction and submitted to the DRM to begin the new criminal cycle through assignment of the CCID. The process followed, therefore, is the same as any physical arrest.

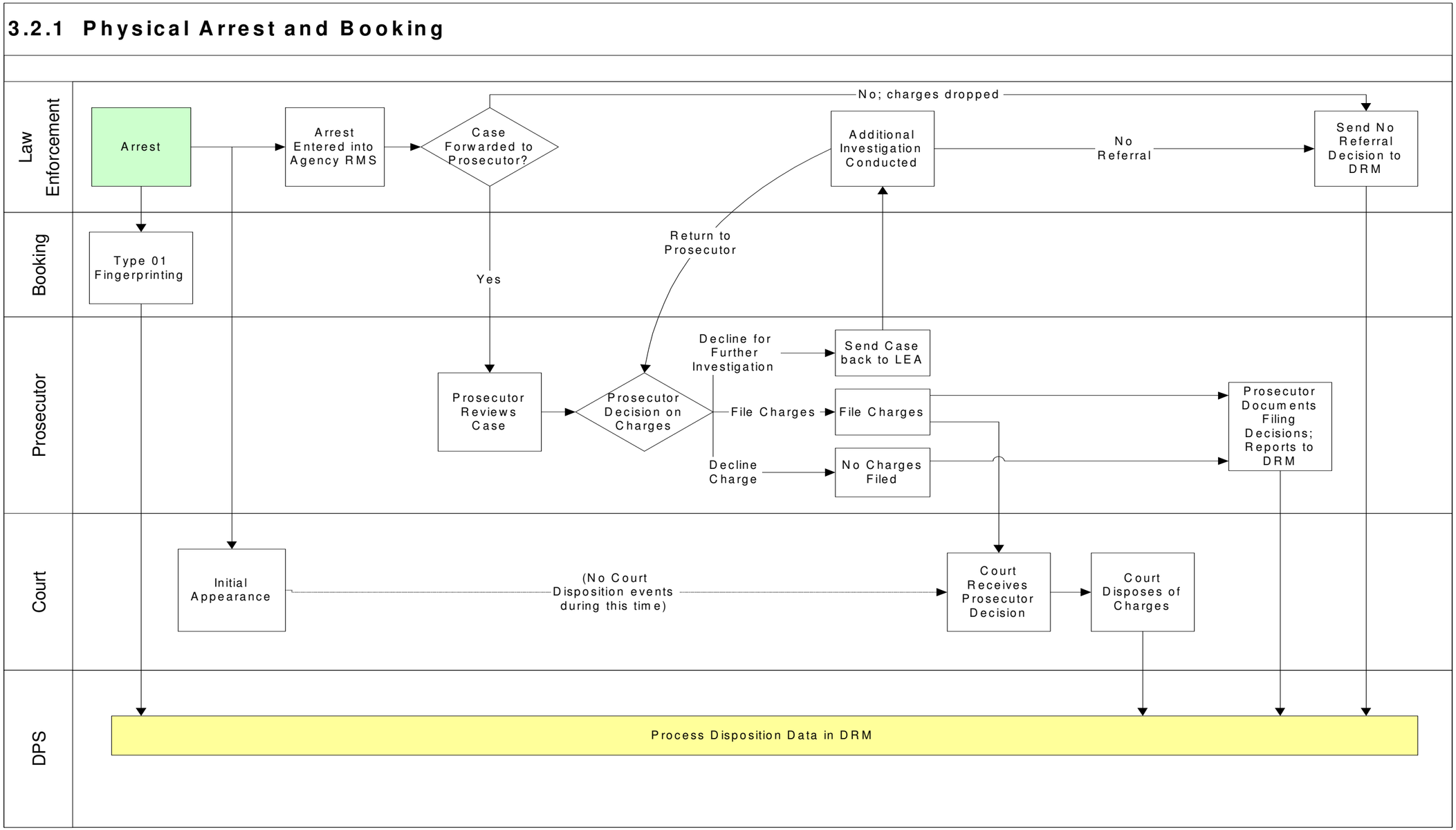
3.2.1.4 Citation and Fingerprinting

This is a variation of the arrest/booking process that occurs in situations where a citation is issued, the suspect is immediately taken to a booking or fingerprinting unit for fingerprinting, and then the suspect is released. The charges are actually initiated by the Citation, but the first notification to the state of these charges occurs when the live scan transaction is received. The CCID will be created and a cycle opened in the DRM when this transaction is transmitted to the DRM.

3.2.1.5 Processing After Fingerprinting: Physical Arrest

After fingerprinting has occurred, the process continues based on the type of charge initiation. Non-physical arrest charge events are described in the next sections of this document. For Physical Arrest events, the following process flow typical of the movement of the case through the criminal justice system:

3.2.1 Physical Arrest and Booking



The key steps in the Physical Arrest process flow are summarized below:

- Physical Arrest occurs.
- Suspect is brought to booking for Type 01 fingerprinting; the fingerprints are submitted to AZAFIS.
- The AZAFIS data is transmitted to the DRM, a CCID is assigned and a new criminal cycle is created in the DRM.
- Law enforcement enters the arrest event in the agency Records Management System (RMS) and decides whether it will be referred for prosecution:
  - If the law enforcement agency decides to drop charges and not forward the case for prosecution, the No Referral disposition is sent to the DRM
  - If the law enforcement agency decides to continue the case, it is referred to the prosecutor.
- The Initial Appearance is held; the prosecutor may or may not have made a charging decision at this point.
- The prosecutor reviews the case:
  - If the prosecutor declines to pursue the charges, the No File decision is entered into the prosecutor's case management system (CMS) and forwarded to the DRM
  - If the prosecutor determines additional information or investigation is needed, the case is sent back to the law enforcement agency. The law enforcement agency can conduct the additional investigation and return the charges to the prosecutor, or the agency may decide that the charges will not be referred. If charges are not referred, the No Referral decision is sent to the DRM.
  - If the prosecutor decides to pursue the charges, the charges will be filed in court; the filing decision is documented in the prosecutor's CMS and forwarded to the DRM.
- The court disposes of the charges and forwards the court disposition to the DRM

3.2.1.6 Data Exchanged

During the Physical Arrest process, the following types of documents or categories of information are typically exchanged within and between agencies; they contain the individual data elements that will become part of the Disposition Report:

- Fingerprint Data
- Law Enforcement Report
- Charge Request
- No Referral Disposition

- No File Disposition
- Decline/Return for Further Law Enforcement Investigation
- Decline Charge
- Prosecutor Charge Decision
- Complaint
- Court Disposition

3.2.1.7 Notifications

The DRM will be capable of generating notifications to agencies about key events in the disposition report process or to notify agencies of required data such as missing dispositions and fingerprints. This functionality is described in detail in Section 4.3.6 of this document. A more complete list of notification types should be developed during the Detailed Design phase of the DRM system.

The following are some of the possible notifications generated by the DRM during the Physical Arrest cycle:

- Notification to Prosecutor and Court of charge initiation
- Notification of dispositions due from law enforcement
- Notification of dispositions due from prosecutors
- Notification of charges filed
- Notification of dispositions due from courts
- Notification of final disposition
- Notification of charges appealed
- Notification of No Files and No Referrals
- Notification to Corrections of a defendant sentenced to custody.
- Notification to Probation of a defendant sentenced to probation.

3.2.1.8 Issues

During the JAD sessions, several jurisdictions expressed concern about a recurring error of double booking that results in two arrest records initiated in ACCH. An example of double booking is when a municipal jurisdiction obtains and submits fingerprints at the municipal level prior to booking the suspect at the county jail; another example is booking on an arrest warrant in one jurisdiction when the individual is wanted in another jurisdiction. If both sets of fingerprints are submitted as "Type 01" AFIS transactions, duplicate entries are committed to ACCH.

DRM will assist in minimizing these occurrences because after the first booking is submitted to the DRM, the second booking unit can query and retrieve the data entered from the first booking. This can have an added bonus of eliminating duplicate data entry for the second booking if the

booking unit is capable of downloading DRM data into the local agency application. In addition, through the notification subscription process the DRM can notify the county jail that fingerprints have been taken, and the jail can associate their prints with the CCID assigned to the cycle at the time of local printing.

The process described for physical arrests anticipates that fingerprints will be submitted using a Live Scan or Card Scan. Different procedures will have to be developed for agencies that are still inking prints. The DRM can assist in this process by providing CCID information for use on the fingerprint card.

3.2.2 CITE AND RELEASE

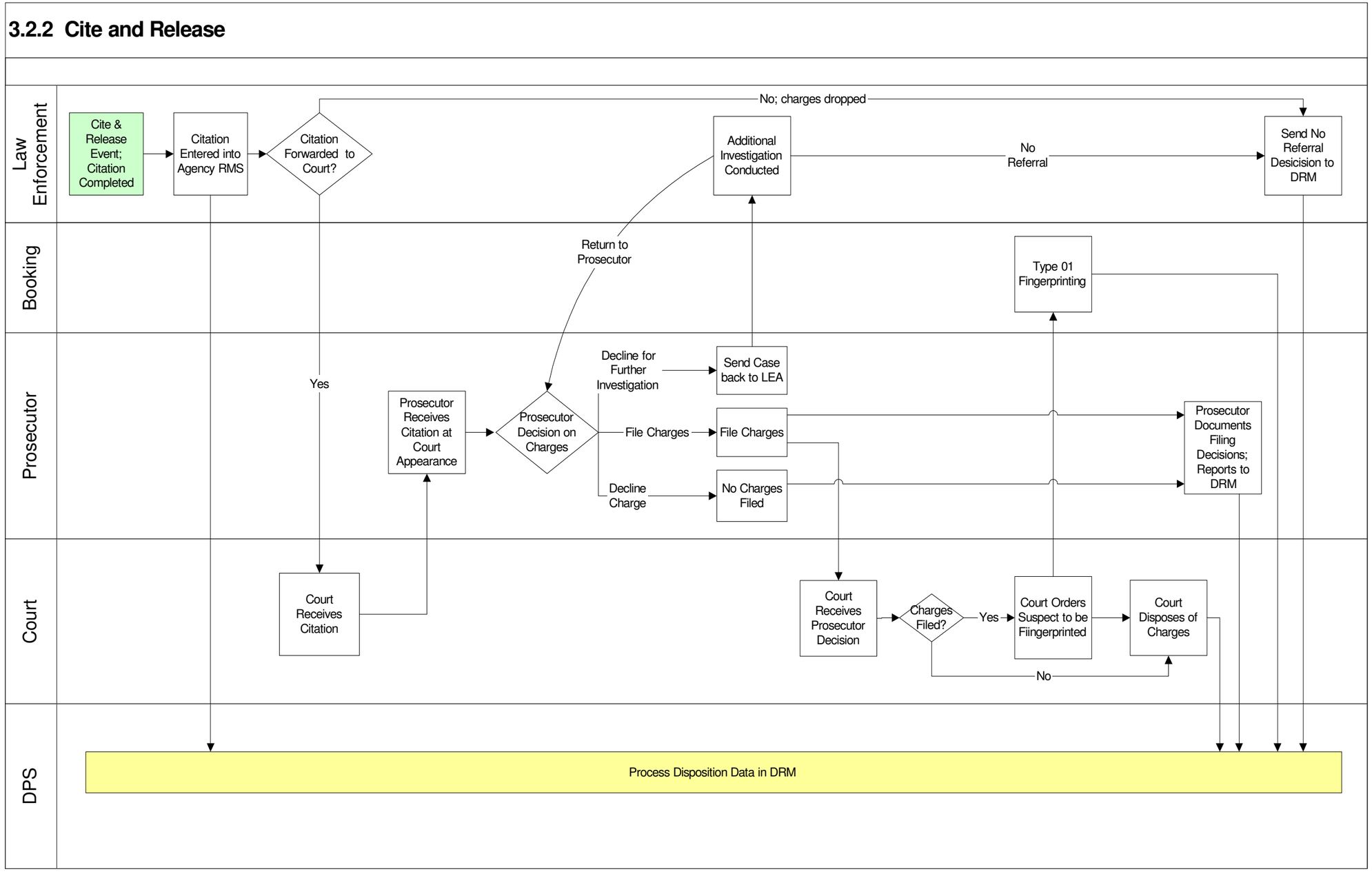
3.2.2.1 High-Level Process Flow

Charges are initiated in the Cite and Release process when an officer issues a citation (i.e., a Notice to Appear in court for alleged offenses) and the individual is released. Typically the suspect is not fingerprinted immediately after the citation has been issued; instead, fingerprinting for misdemeanors and reportable offenses should occur at some point in the adjudication process so that fingerprints can be added to the DRM record and submitted to the ACCH. For a discussion on citations immediately followed by fingerprinting, please refer to Section 3.2.1 concerning Physical Arrest.

According to JAD participants, Cite and Release cases represent the most under-reported cases to ACCH. The ability of the DRM system to track cases that do not yet have fingerprints and to enforce the requirement for obtaining those fingerprints will be critically important for these types of cases.

The process typically followed by a citation as it moves through the initiation and adjudication of charges demonstrates the ability of the DRM to create a disposition report even if fingerprints have not yet been obtained, and to anticipate key events that will complete the disposition reporting process. The following process model depicts the typical citation process:

3.2.2 Cite and Release



The process model shown above depicts the following steps:

- The citation is issued by an officer
- The citation is entered into the law enforcement agency's records management system (RMS) and forwarded to the DRM; a new disposition record is created and cycle/charge tracking numbers assigned
- If the agency reviews the case and decides not to refer it to the court for prosecution, and the decision is made prior to the court appearance date, the No Referral decision is entered into the RMS and forwarded to the DRM
- If the agency has decided to pursue the charges, citation is forwarded to the court
- At the court appearance, the prosecutor reviews the case:
  - If the prosecutor declines to pursue the charges, the No File decision is entered into the prosecutor's case management system (CMS) and forwarded to the DRM.
  - If the prosecutor determines additional information or investigation is needed, the case is sent back to the law enforcement agency. The law enforcement agency can conduct the additional investigation and return the charges to the prosecutor, or the agency may decide that the charges will not be referred. If charges are not referred, the No Referral Decision is sent to the DRM.
  - If the prosecutor decides to pursue the charges, the court is informed of the decision during the court appearance; the filing decision is documented in the prosecutor's CMS and forwarded to the DRM.
- If charges are filed in court, the court orders the suspect to be fingerprinted; the existing CCID is included in the order
  - The booking unit prints the suspect (Type 01) and submits the prints using the existing CCID to AZAFIS
  - The DRM is updated to include the fingerprint data
- When the court disposes of the filed charges, the disposition is sent to the DRM

3.2.2.2 Data Exchanged

During the Cite and Release process, the following types of documents or categories are typically exchanged within and between agencies; they contain the individual data elements that may become part of the Disposition Report:

- Citation
- Decline/Return for Further Law Enforcement Investigation

- Decline Charge
- No File Disposition
- No Referral Disposition
- Prosecutor Charge Decision
- Fingerprint Data
- Court Disposition

3.2.2.3 Notifications

During the Cite and Release process, the following notifications will be created by the DRM:

- Notification of requirement for fingerprinting
- Notification of dispositions due from law enforcement
- Notification of dispositions due from prosecutors
- Notification of charges filed
- Notification of dispositions due from courts
- Notification of final disposition
- Notification of charges appealed
- Notification of No Files and No Referrals

3.2.2.4 Issues

In some instances, charges may be dropped prior to fingerprints being obtained (such as No Referral and No File decisions). In these cases, the record will never be associated with fingerprint identification unless the court proceeds with an order to obtain fingerprints. The record will likely be reported to DRM but it will not be forwarded to ACCH. Procedures on how to deal with these "orphaned" cycles will need to be determined during detailed design for the DRM.

Currently, many courts report the filed charges on behalf of the prosecutors; in some jurisdictions, the prosecutor is reporting No Files to DPS. The DRM will be designed to receive filing decisions from prosecutors.

3.2.3 LAW ENFORCEMENT REPORTS SUBMITTED FOR PROSECUTION REVIEW

3.2.3.1 High-Level Process Flow

In addition to physical arrests and citations, charges can also be initiated when a law enforcement agency submits an investigative report directly to a prosecutor without a prior arrest or citation event. In these circumstances, the prosecutor's decision to file charges is the first notification to the state that charges exist. The investigative report is usually in the form of a Law

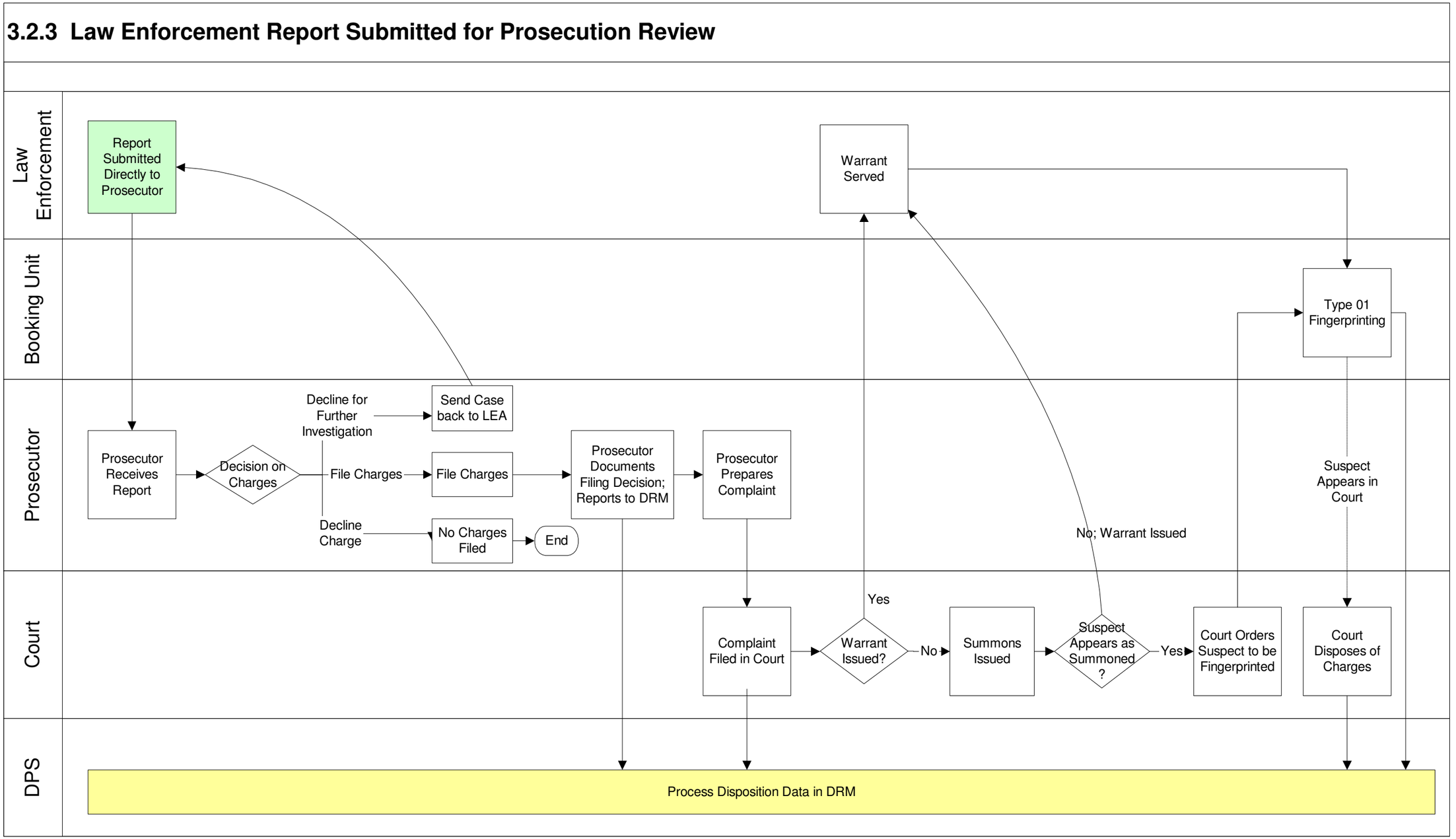
Enforcement Report and may be accompanied by an Officer's Affidavit of Probable Cause (Form IV). The report is delivered directly to the prosecutor without being preceded by an arrest or citation. If the prosecutor decides to file charges, charges are filed and a Complaint (or "Long Form") is prepared by the prosecutor and submitted to the appropriate court.

As the case progresses, fingerprinting of the suspect can occur in two ways: 1) a Warrant is issued and served, and the suspect is brought to a booking unit for fingerprinting; or 2) a Summons is issued and the suspect is ordered by the court to be fingerprinted. The Summons may include a date on which the individual is ordered to report to a booking unit for fingerprinting, or the individual may receive the order to be fingerprinted after appearance in court.

According to JAD participants, the "Long Form" or Complaint cases make up the second most commonly non-reported cases, second only to Cite and Release.

The Law Enforcement Report process flow is shown on the following page:

3.2.3 Law Enforcement Report Submitted for Prosecution Review



The key steps in the Law Enforcement Report process are summarized below:

- A law enforcement report is presented to a prosecutor for consideration; an Officer's Affidavit of Probable Cause (From IV) may also be included with the report.
- The prosecutor makes a decision on the case:
  - If the prosecutor declines the case, it is closed and no further action occurs with regard to the initiation of charges; no record is created in DRM.
  - If the prosecutor decides to take the case, the charges may be filed as requested or as otherwise determined by the prosecutor; the prosecutor's charges are reported to DRM where a new CCID is issued and charge tracking numbers assigned.
- If the prosecutor has decided to pursue the case, a Complaint is filed in court with a request for a warrant or a summons.
  - If a warrant is issued and served, the suspect will be taken to a booking unit for fingerprinting. The warrant should include the assigned CCID; the booking unit prints the suspect (Type 01) and submits the prints using the existing CCID to AZAFIS. The DRM is updated to include the fingerprint data.
  - If a summons is issued instead of a warrant, the summons may include an order to be fingerprinted at a specific date and time or the suspect may be ordered for fingerprinting at the time of the court appearance. When the suspect appears at the booking unit for fingerprinting, the summons will include the assigned CCID; the booking unit prints the suspect (Type 01) and submits the prints using the existing CCID to AZAFIS. The DRM is updated to include the fingerprint data.
  - If the suspect does not respond to a summons, a warrant may be issued and the same procedure described above will be followed to obtain fingerprints and report to the DRM.
- When the court disposes of the charges in the complaint, the disposition is sent to the DRM for processing.

3.2.3.2 Data Exchanged

During the Law Enforcement Report process, the following types of documents or categories of information are typically exchanges and they contain data that will become part of the Disposition Report:

- Summons
- Warrant
- Complaint
- Form IV
- Decline Charge for Further Investigation
- Decline Charge
- Prosecutor Filed Charges
- Fingerprint Data
- Court Disposition

3.2.3.3 Notifications

During the Law Enforcement Report process, the following notifications would be created by the DRM:

- Notification of requirement for fingerprinting
- Notification of dispositions due from prosecutors (if court data is submitted prior to prosecutor data)
- Notification of charges filed
- Notification of dispositions due from courts
- Notification of final disposition
- Notification of charges appealed

3.2.3.4 Issues

As discussed previously, most courts report the filed charges on behalf of the prosecutors; in some jurisdictions, the prosecutor is reporting No Files to DPS. The DRM will be designed to receive filing decisions from prosecutors.

3.2.4 GRAND JURY INDICTMENT

3.2.4.1 High-Level Process Flow

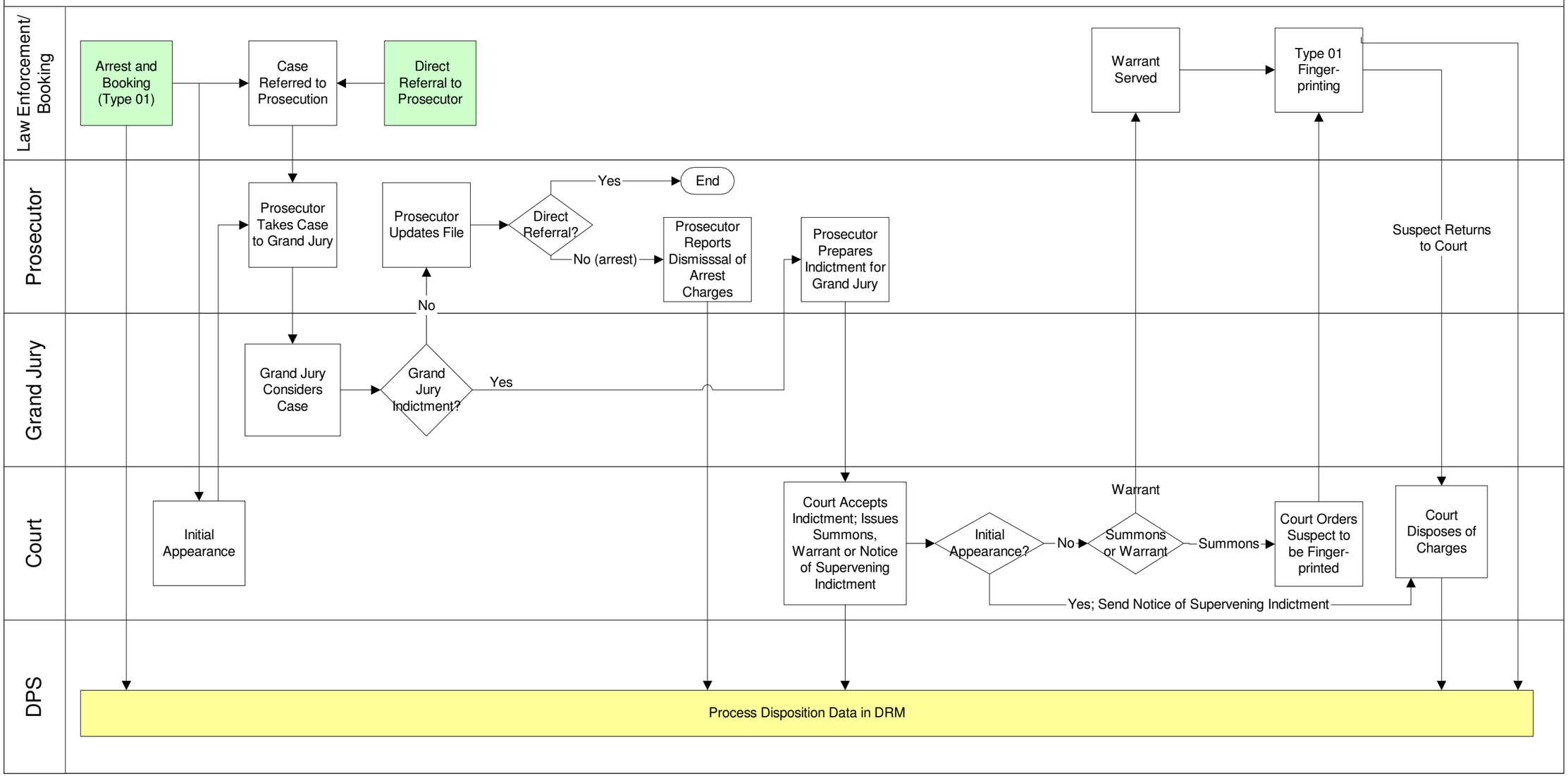
The Grand Jury process can begin as a result of an arrest event or a direct referral of a case from law enforcement to the prosecutor, who then submits the case to the Grand Jury for review. The primary difference in these entry points is that no charges will ever be initiated in the DRM system for the direct referral unless the Grand Jury returns an indictment.

For arrest events that go to a Grand Jury, fingerprinting will occur at the time of arrest and booking. The arrest event will initiate the record in DRM. In contrast, there are several points in the Grand Jury process when fingerprinting can occur for direct referrals. The DRM will accommodate the various fingerprinting opportunities by checking the status of the record and sending notifications to the courts or appropriate law enforcement agencies that fingerprints are still needed. And like other criminal justice processes,

the Grand Jury process flow can have several activities going on at the same time in different agencies.

The Grand Jury process flow is shown on the following page:

3.2.4 Grand Jury Indictment



The steps in the Grand Jury process are summarized below for arrest events:

- An arrest event occurs followed by booking:
  - The booking unit prints the suspect (Type 01) and submits the prints to AZAFIS
  - The DRM is notified by AZAFIS, assigns a CCID, and creates a new cycle record that includes the fingerprint data
- The case is sent to the Prosecutor and the Initial Appearance is conducted.
- The prosecutor presents the case to the Grand Jury for review and consideration:
  - If the Grand Jury does not return an indictment, the prosecutor updates the case file and sends notification of the No Bill (dismissal of arrest charges) to the DRM system
  - If the Grand Jury decides to return an indictment, the prosecutor prepares the indictment and submits it to the court for the Grand Jury
- The court accepts the indictment and issues a Notice of Supervening Indictment pursuant to Rule 12.7 (c) of the Rules of Criminal Procedure; the court updates the DRM with the indictment.
- The court disposes of the charges and submits the disposition to the DRM.

The steps in the Grand Jury process for a direct referral are summarized below:

- A case is referred directly from law enforcement to the prosecutor
- The prosecutor decides to take the case to a Grand Jury
- The prosecutor presents the case to the Grand Jury for review and consideration:
  - If the Grand Jury does not return an indictment, the prosecutor updates the case file. No report is initiated in the DRM
  - If the Grand Jury decides to return an indictment, the prosecutor prepares the indictment and submits it to the court for the Grand Jury.
- The court receives the indictment and sends the charges to the DRM; a CCID is assigned and a new cycle record is initiated in the DRM system.
  - If a warrant is issued and served, the suspect will be taken to a booking unit for fingerprinting. The warrant should include the assigned CCID; the booking unit prints the suspect (Type 01) and

submits the prints using the existing CCID to AZAFIS. The DRM is updated to include the fingerprint data.

- If a summons issued instead of a warrant, the summons may include an order to be fingerprinted at a specific date and time or the suspect may be ordered for fingerprinting at the time of the court appearance. When the suspect appears at the booking unit for fingerprinting, the summons will include the assigned CCID; the booking unit prints the suspect (Type 01) and submits the prints using the existing CCID to AZAFIS. The DRM is updated to include the fingerprint data.

- When the court disposes of the charges in the complaint, the disposition is sent to the DRM for processing.

3.2.4.2 Data Exchanged

During the Grand Jury process, the following types of documents or categories of information may be exchanged within and between agencies; they contain the individual data elements that will become part of the Disposition Report:

- Law Enforcement Report
- Fingerprint Data
- Warrant
- Summons
- Grand Jury Indictment (True Bill)
- Notice of Supervening Indictment
- No Bill
- Court Disposition

3.2.4.3 Notifications

During the Grand Jury process, the following notifications would be created by the DRM:

- Notification of requirement for fingerprinting
- Notification of dispositions due from prosecutors (on behalf of Grand Jury)
- Notification of charges filed in indictment
- Notification of dispositions due from courts
- Notification of final disposition
- Notification of charges appealed

3.2.4.4 Issues

Cases that are referred directly to the Grand Jury without an arrest event are considered confidential during referral and Grand Jury consideration. These cases should not be entered into the DRM system until such time as the Grand Jury indictment has been submitted to court.

If a case involves an arrest and the Grand Jury does not return an indictment, the Rules of Criminal Procedure requires that the court be informed. If the court normally submits the No Bill (dismissal of charges) to DPS, the DRM will have to accommodate receipt of this information from either the prosecutor or the court.

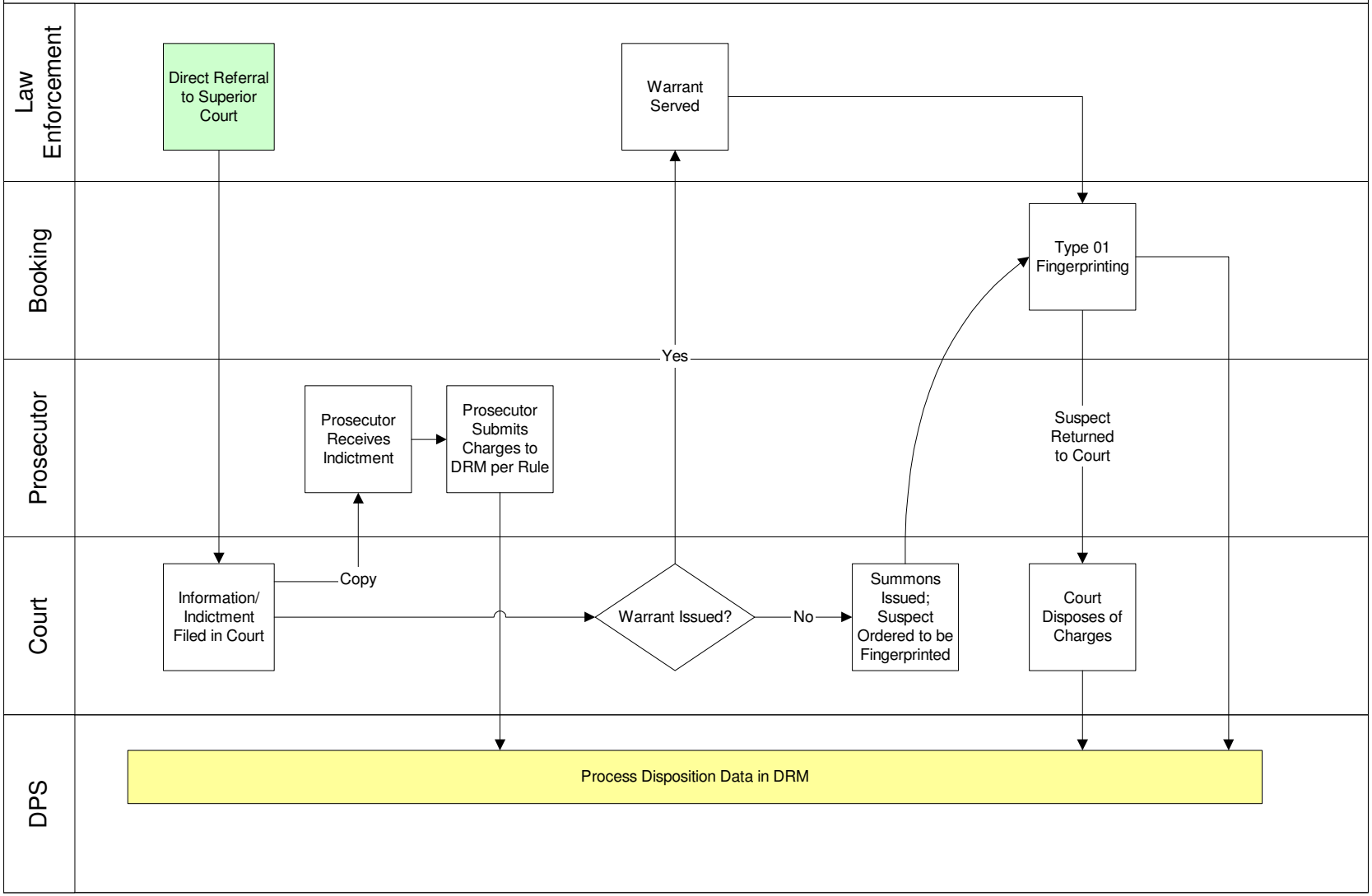
3.2.5 INFORMATION FILED DIRECTLY IN SUPERIOR COURT

3.2.5.1 High-Level Process Flow

Rule 37.2 (c) of the Rules of Criminal Procedure states that "If the action is commenced by indictment or an information filed directly in superior court, the prosecutor shall file the disposition form at the time of the filing of the indictment or information." The process allows law enforcement to take a complaint directly to court, where the charges are initiated and forwarded to the prosecutor. The first notification to the DRM system will be when the prosecutor receives the indictment or information and submits the prosecutor segment to the DRM.

The procedure is not commonly used and most JAD participants were not familiar with how the rule is currently used. However, ensuring that the record is created and updated in the DRM will not be difficult because the procedure borrows from other court and prosecutor processes to move the case through adjudication. The DRM will not expect to receive an initiating charge segment from a law enforcement agency.

3.2.5 Information Filed Directly in Superior Court/Rule 37.2 (c)



The key steps in the process are summarized below:

- Law enforcement refers a case directly to Superior Court by filing an information or indictment.
- The court sends a copy of the information or indictment to the prosecutor.
- The prosecutor files the prosecutor segment with the DRM system to establish a new cycle record, as required by the rule.
- If the court issues a warrant, law enforcement will serve the warrant and the suspect is taken to booking for fingerprinting. The fingerprint data from booking is sent to the DRM to be associated with the existing DRM record.
- If a Summons is issued, the Summons includes an order for the suspect to appear at a booking unit for fingerprinting; the booking data is submitted to the DRM and associated with the existing DRM record
- The court disposes of the charges and submits the final disposition to the DRM.

3.2.5.2 Data Exchanged

During the Information Filed Directly in Superior Court process, the following types of documents or categories of information are typically exchanged; they contain data that will become part of the Disposition Report:

- Information or Indictment
- Fingerprint Data
- Court Disposition

3.2.5.3 Notifications

During this process, the following notifications would be created by the DRM:

- Notification of requirement for fingerprinting
- Notification of charges filed
- Notification of dispositions due from courts
- Notification of final disposition
- Notification of charges appealed

3.2.5.4 Issues

The Information Filed Directly in Superior Court process does not include a law enforcement segment for the initiation or updating of charges; the only data received from a law enforcement agency will be fingerprint data from a booking unit. The DRM will be required to establish different expectations for the segments that are expected to be reported during this process.

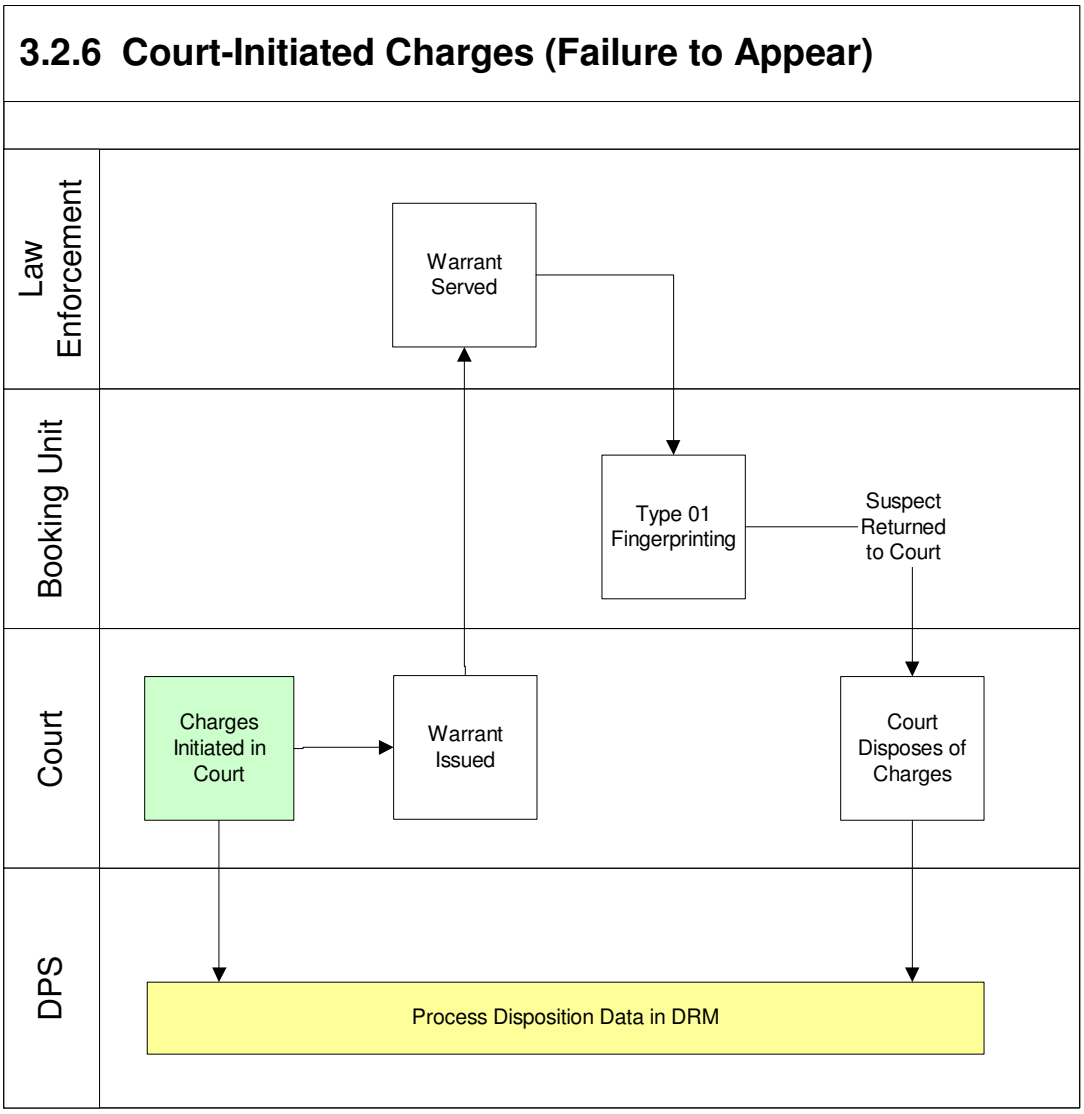
3.2.6 COURT-INITIATED CHARGES

3.2.6.1 High-Level Process Flow

Courts can initiate charges for Failure to Appear, which is a reportable offense. A warrant is also issued at the time that the charges are issued. If the suspect is arrested on the warrant and returned to court, the charges are disposed at that time.

In order to assure proper processing and fingerprinting for a Failure to Appear record, the court should report the charges to the DRM at the time charges are initiated. The CCID would then be generated by the DRM and used when the suspect is arrested and fingerprinted. Courts could either use the DRM web page to submit these charges or report the charges electronically using the interface between the court CMS and the DRM.

3.2.6 Court-Initiated Charges (Failure to Appear)



The steps involved in this process are:

- The court charges an individual with Failure to Appear
- The court submits the charges to the DRM; a new disposition record is created and charge tracking numbers assigned
- The court issues a warrant for the suspect's arrest on the Failure to Appear charges
- The warrant served, the suspect is fingerprinted, and the fingerprint data is sent to the DRM to be added to the existing DRM record
- The court disposes of the charges and reports the final disposition to the DRM

3.2.6.2 Data Exchanged

The Court-Initiated Charges can involve the following exchanges of documents and data:

- Court-Filed Charges
- Warrant
- Fingerprint Data
- Court Disposition

3.2.6.3 Notifications

The notifications related to this process can include:

- Notification of charges filed
- Notification of dispositions due from courts
- Notification of final disposition
- Notification of charges appealed

3.2.6.4 Issues

Courts are not routinely submitting a Disposition Report to DPS at the time Failure to Appear charges are initiated. This process would require the courts adjust current business practice to report these charges at the time of initiation if they are submitting dispositions manually, or to adjust the data reported electronically through an interface between the court CMS and the DRM.

By initiating the charges in DRM so that the CCID can be used when the arrest warrant is served, the fingerprints and the associated criminal history record can be processed correctly and efficiently to ensure that a record is created correctly in ACCH. This is particularly important if there is a gap in time between the issuance of the Failure to Appear charges and the actual arrest, because it will be easier to tie the two events together if there is an existing CCID. If the court does not report the initiated charges to DRM, the court will have to obtain the CCID from the arrest and add the court disposition in order for the record to be processed correctly by DRM and reported to ACCH.

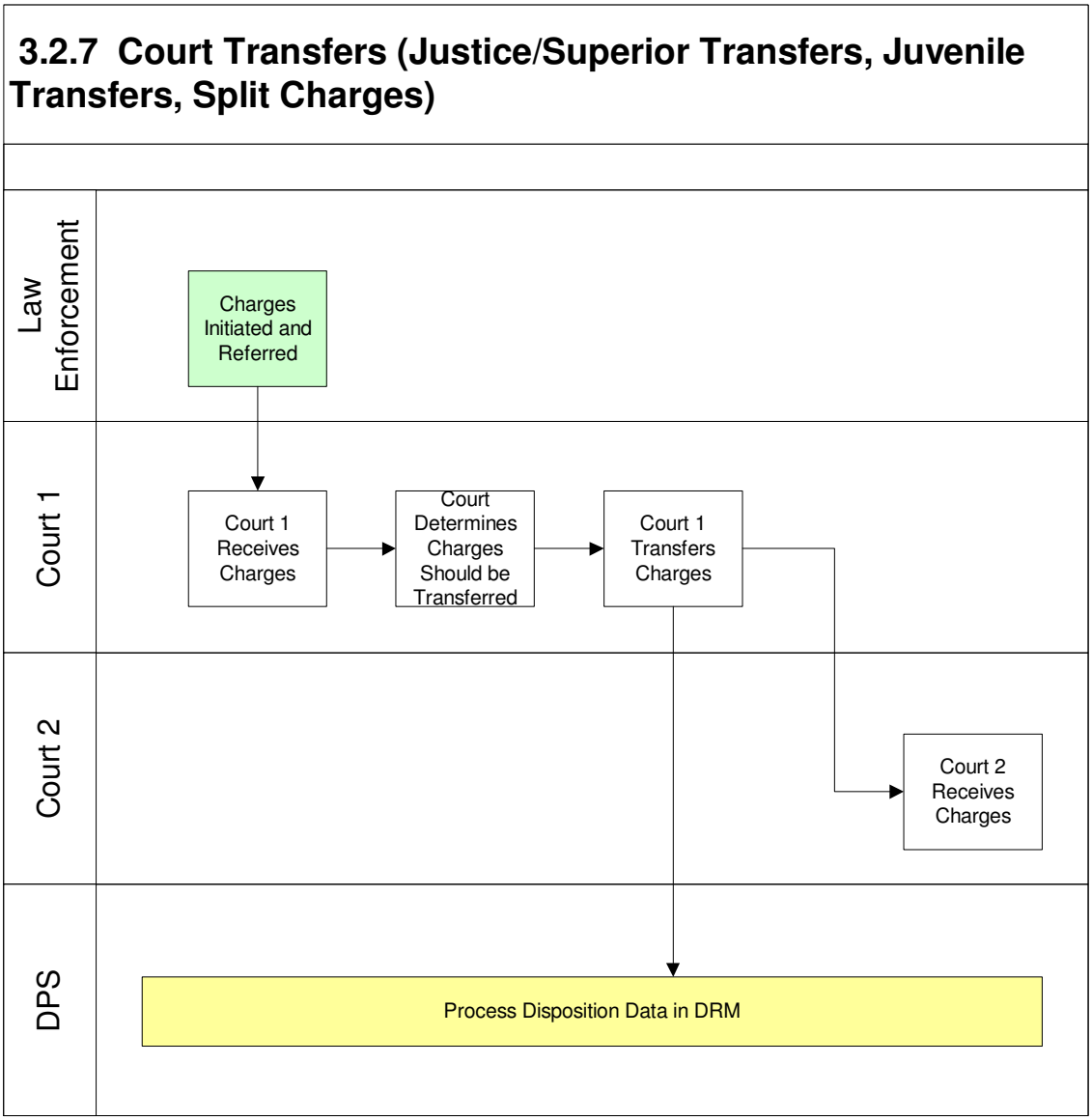
3.2.7 COURT TRANSFERS

3.2.7.1 High-Level Process Flow

The Court Transfer process is really a sub-process that can occur when a court and/or prosecutor determines that a case should be adjudicated in a different court or jurisdiction. It can also occur when juveniles are transferred to a different court to be adjudicated as an adult. The DRM system must record

the transfer properly so that the charges can be tracked and notifications sent to the appropriate agencies.

Once the transfer has been reported to the DRM, the charges follow the process in which they were initiated. The following diagram illustrates the transfer process.



3.2.7.2 Data Exchanged

The following document is typically exchanged during this sub-process:

- Case File

3.2.7.3 Notifications

Only one notification is required for this sub-process:

- Notification of change in court

3.2.7.4 Issues

Business procedures and interface reporting used by courts will have to be adjusted in order to report transfers correctly to DPS. For example, one procedure currently used is for the first court to report a case that is to be transferred as dismissed. By changing procedures and interface transactions to notify the DRM that an actual transfer has occurred, the criminal cycle will be reported correctly. For example, AZTEC courts the "transfer to" code could be used to report the transfer. Courts may also choose to use the DRM web page to report the transfer.

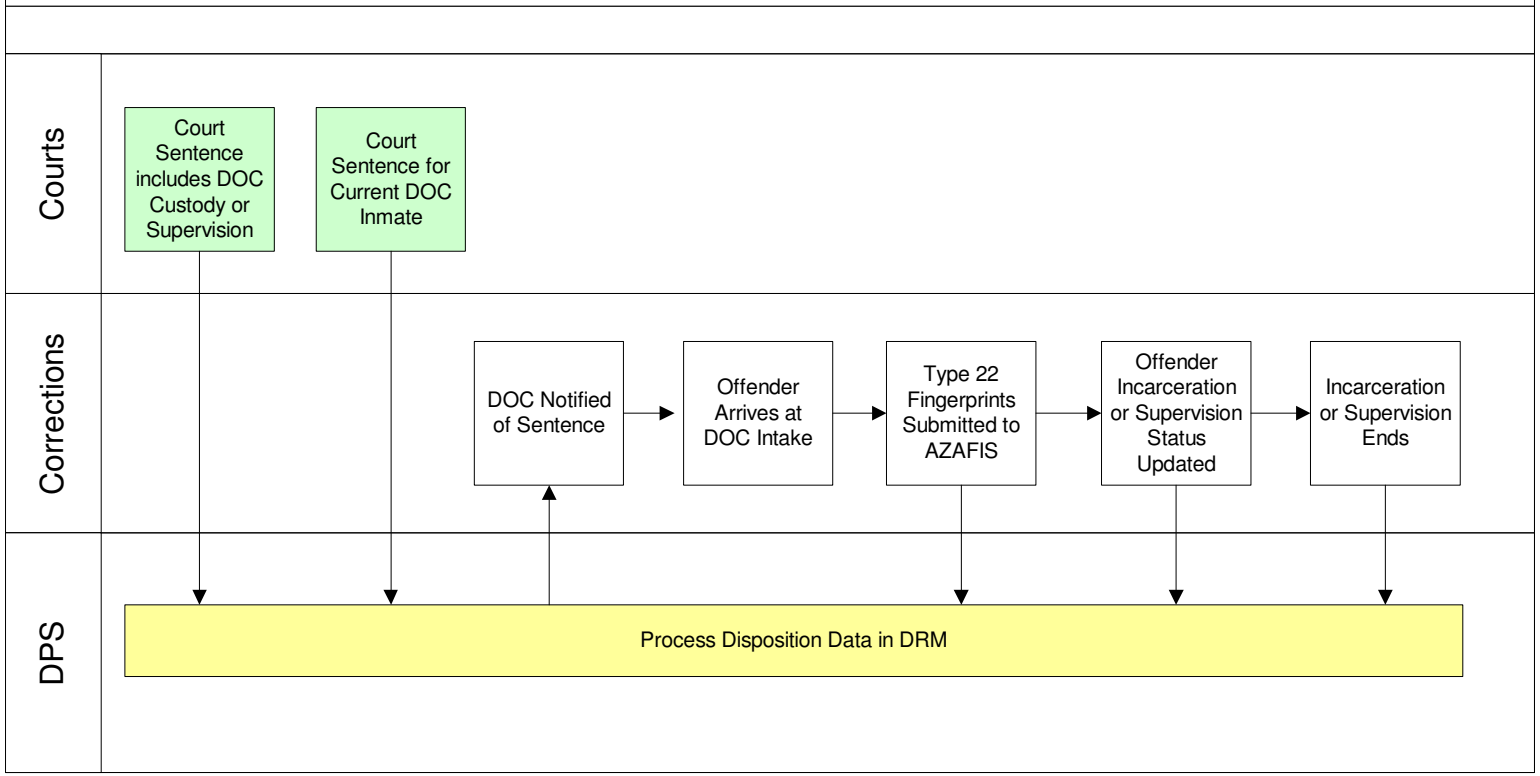
3.2.8 DOC CUSTODY AND SUPERVISION STATUS

3.2.8.1 High-Level Process Flow

Currently, information from the Department of Corrections (DOC) regarding inmates and parolees is sent to DPS in two ways: 1) at intake, inmates are fingerprinted (Type 22 fingerprinting) using Live Scans or Card Scans and the fingerprint data is transmitted to AZAFIS; and 2) inmate and parolee status data from the DOC database (AIMS) is transmitted to DPS each week to be input in the Offender Based Tracking System (OBTS). This information is used to respond to the custody status portion of rap sheet requests.

DOC receives the court sentencing documents at the time of intake, but the department does not get prior notification in all cases that an offender has been sentenced to DOC custody. The high-level process flow illustrated below will change current information flows by providing DOC with notification of all sentencing activities that involve incarceration. In addition to these notifications, the DRM will be available to assist in managing custody and supervision information for input to the ACCH. Details on the exact nature of the interaction among the offender-related information maintained within DPS will be determined at later phases of design. Accordingly, the process flow does not include any specifics on the movement of this data within DPS databases.

3.2.8 DOC Custody and Supervision



The key steps in the DOC custody and supervision process flow are:

- An offender is sentenced to the custody of DOC; the court disposition is reported to the DRM
- The DRM notifies DOC (using a formatted report) of all sentences involving DOC custody
- At DOC intake, the offender is fingerprinted (Type 22) and the fingerprints are transmitted to AZAFIS and forwarded to DRM to update the criminal cycle; the DRM reports to ACCH so that the criminal history record can be updated and the cycle can be completed.
- Inmate and parolee status updates (such as facility change, release, re-incarceration) are sent from the DOC AIMS system to DPS for input to the OBTS.
- The OBTS information is forwarded to the DRM which will determine if the cycle is still open and update the record in both DRM and ACCH, if appropriate

3.2.8.2 Data Exchanged

The following documents or data sets are typically exchanged during this process:

- Court Disposition
- Intake Fingerprint Data
- Inmate and Parolee Status

3.2.8.3 Notifications

The notifications related to this process can include:

- Notification of final disposition
- Notification of inmate/parolee status due from DOC
- Notification of completion of sentence requirements

3.2.8.4 Issues

The process described above focuses on individuals under the custody or supervision of DOC. Other statewide databases have been or are being developed to compile probation and custody status information from county detention centers. Adult probation is administered by the Superior Court in each county and probation status information will be provided from the courts through the ACJIS in a separate project to be completed in 2004. Additional

analysis should be undertaken during the Detailed Design phase to evaluate interfaces between these new systems and the DRM.

Another decision that will be required during Detailed Design of the DRM concerns the retention of records in the DRM and how these timing issues will affect the updating of custody and supervision status. The DRM will need to receive status information so that any open cycles can be updated and closed. Whether or not the DRM will also receive updates on cycles that have already been completed and are only available from the ACCH for reporting purposes will have to be determined during the next phase of the project. This will require an analysis of the interaction between DRM, OBTS, and ACCH.

DOC will be receiving statewide, pre-formatted court sentencing notifications for the first time; the contents and notification schedule for these reports from the DRM to DOC will have to be determined during the detailed design of the DRM system.

3.2.9 DNA SAMPLE DATA

3.2.9.1 High-Level Process Flow

The State of Arizona requires that DNA samples be taken for all defendants convicted of a felony offense or required to register as a Sex Offender. The agency responsible for taking the sample is the DOC if the offender is sentenced to DOC custody; a county detention facility if the offender has been sentenced to serve at that facility; or a county probation department if the offender has been placed on probation.

The desirability of reporting and sharing information on the availability of DNA samples was identified during the planning effort for the JAD sessions. This recommendation was confirmed during the JAD sessions, as well as a recommendation that the DRM include notification that a DNA sample is required upon conviction for an eligible offense.

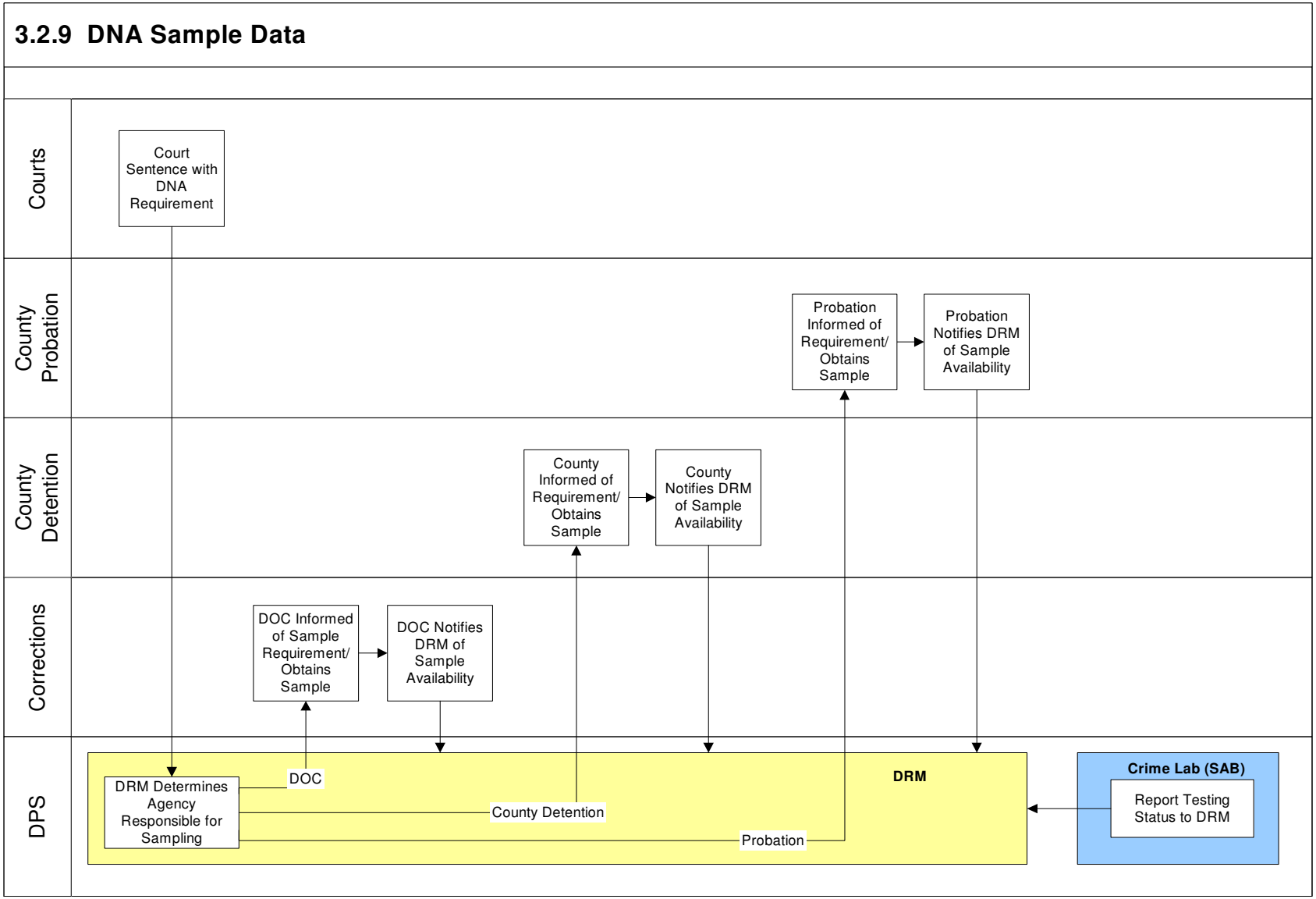
There is currently no uniform statewide business process in place to move or share this information on DNA sample availability or need. Because the requirements for sampling are related to the conviction process and are therefore linked to disposition reporting, the DRM system is a logical application to assist in the tracking the availability of DNA samples and profiles. This DNA information can also be moved from the DRM to ACCH to be included in rap sheets, pursuant to the national standard for rap sheets.

During detailed design and development for the DRM system, the state may choose to consider extending the amount of information available about DNA samples, such as adding an indicator showing that a sample has been tested or

a field showing the submitting agency of a sample. Detailed requirements for the DNA sample process should be developed at that time.

The process recommended here is intended to outline a method for obtaining and reporting the DNA sample data availability and can be considered a sub-process of the other process flows depicted in this document.

3.2.9 DNA Sample Data



The key steps in this process are:

- The court disposition is sent to DRM
- DRM determines that the conviction type requires DNA sampling
- DRM determines the agency responsible for sampling, based on the sentence and jurisdiction
- DRM notifies the appropriate agency (DOC, County Detention, or County Probation) of the DNA sample requirement
- The appropriate agency obtains the sample and notifies DRM of the sample availability
- DRM updates the disposition report to include DNA sample availability
- DPS scientific Analysis Bureau notifies DRM of the assigned LIMS identifier for received samples
- (Possible future enhancement) DPS Scientific Analysis Bureau notifies DRM that the sample has been tested
- (Possible future enhancement) DRM prints DPS standard DNA sample submission form for DPS crime lab.

3.2.9.2 Data Exchanged

The following documents or data are likely to be exchanged during this sub-process:

- Court Disposition
- DNA Sample capture data
- DNA Sample testing status

3.2.9.3 Notifications

The notifications related to this process can include:

- Notification of requirement for DNA testing
- Notification of sample acquisition
- Notification of sample testing completion

3.2.9.4 Issues

The receipt of DNA sample status information is likely to be reported to the DRM after the completed charge cycle has been reported to ACCH and the cycle closed in the DRM. The DRM must retain the capability of receiving the DNA sample information, retrieving ACCH data if necessary to associate the DNA information to the correct record, sending notifications as needed, and moving the availability status to the ACCH. DPS is considering

modifying ACCH to hold DNA sampling indicators; this information could include a sample availability flag, sample ID (from LIMS), sampling ORI, PCN (if available) of concurrently obtained fingerprint images, and the associated cycle as referenced by CCID.

The state may want to consider how the DNA sample information in DRM can be used to assist the DPS crime lab in tracking incoming samples. For example, a report from the DRM could alert the crime lab to the number of incoming samples even before they have arrived at the lab. Or a list of subject demographics might be matched against existing sample demographics in LIMS to locate and possibly divert or consolidate duplicate samples. A report from the DRM might contain the conviction statute, pending charges, or pending release of a subject that could be used to indicate an increased priority for the processing of that subject's sample.

To comply with security requirements of the CODIS system, DNA profiles are submitted to CODIS with an originating crime lab identifier, and local crime lab sample identifier. When a profile match is generated through CODIS, the local sample identifier is then used to match the CODIS data back to the sample submission data through the local crime lab laboratory information management system (LIMS). In this way, CODIS users are prevented from seeing person identifiers until after a positive match has been made, and DNA profile data is stored separately from the person demographics.

In practice, this has led to a situation where submitting agencies do not receive a report of the laboratory results or a confirmation that the sample has been received or tested. As submitting agencies are not notified when a DNA sample has been received or tested, they will often submit duplicate DNA samples when faced with a recidivist offender so as to be sure that they are complying with Arizona statute. To deal with these issues, the DPS crime lab is planning an online LIMS query gateway for submitting agencies to locate and verify existence of a sample at the crime lab. The crime lab is working at a disadvantage in trying to do this because DNA samples are not necessarily submitted with a common unique person identifier, such as an SID.

DPS has already started considering a policy to require that DNA sample submissions to the DPS crime lab be accompanied by a PCN that was generated at the time of DNA sampling, i.e., the DNA sample and a set of fingerprints were taken at the same time. Following this policy would facilitate tracking of samples through the crime lab and associating CODIS records to criminal history rap sheets, as well as create a positive link between DNA samples and the biometrically identified subject of the DNA sample. It is anticipated that the DPS LIMS system will provide batch updates to DRM

that show the LIMS ID assigned to incoming DNA samples and the unique identifiers (CCID, PCN, SID, ARN) provided with the sample. Samples that can be matched to existing DRM records will have the DNA sample availability flag set with notification sent to ACCH.

4 DRM SYSTEM REQUIREMENTS

This section identifies the major system requirements for the new disposition reporting system. This section builds on the recommendations contained in the *Arizona ICJIS Strategic Plan* and requirements defined during the JAD meetings and related interviews. An overview of each function, the specific functional requirements, and, where applicable, a profile of transactions included in the function are outlined in the following sections. Transaction profiles include the types of records to be transmitted in the process, processing and protocol considerations, and possible responses to transactions.

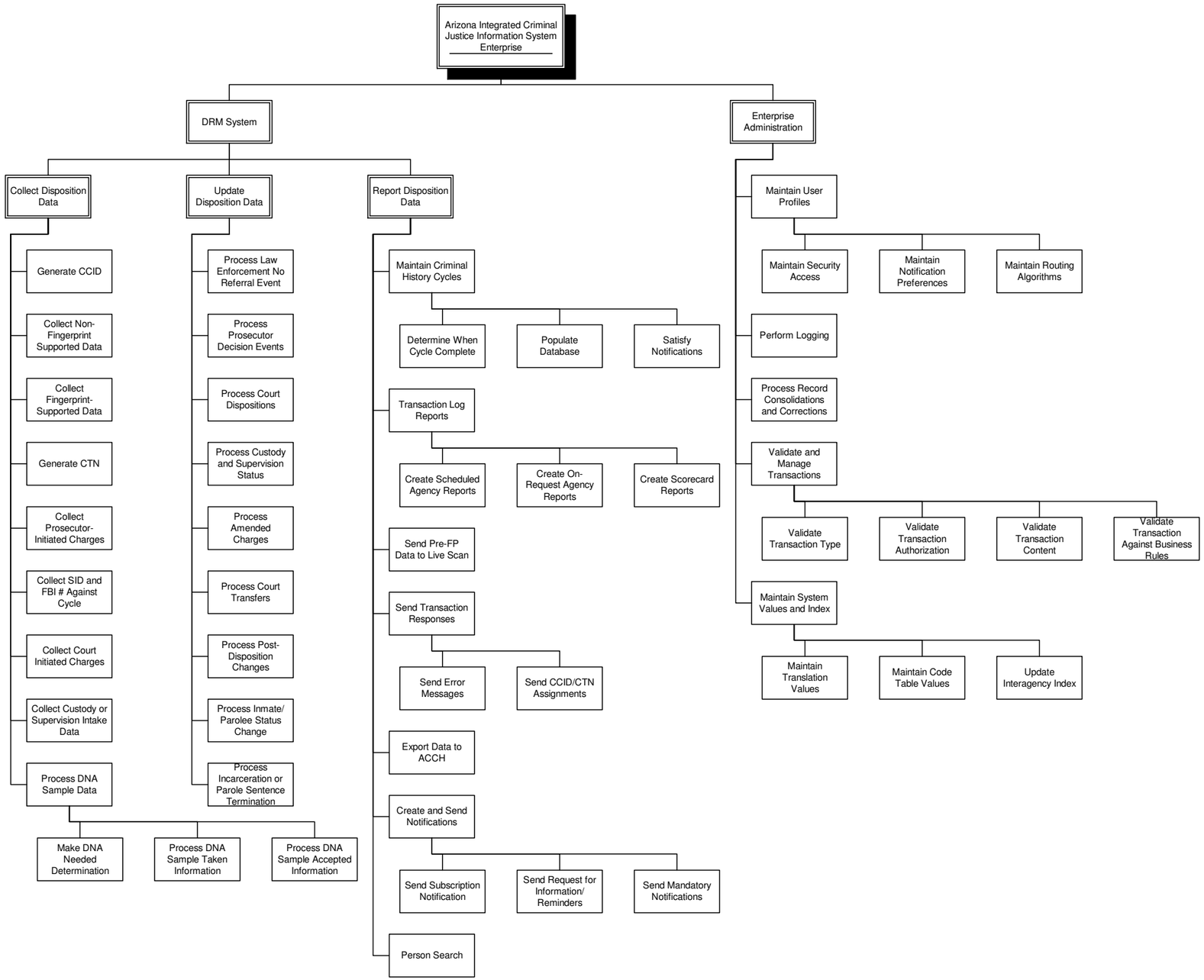
4.1 FUNCTIONAL HIERARCHY DIAGRAM

The DRM system requirements are categorized into the two general categories of functional areas within the larger enterprise that represents the Arizona Integrated Criminal Justice Information System:

- DRM System and Enterprise Administration functionality
- Disposition Reporting System functionality, consisting of:
  - Disposition Information Collection and Management
  - Disposition Information Reporting and Notification Management

The following Functional Hierarchy Diagram (FHD) is a graphical representation of these functional areas. The FHD shows the decomposition of activities in an organization in a hierarchical manner and it provides a starting point for the creation of the automated DRM system and the enterprise-level administration functions that will support it as well as other integration efforts. The diagram is intended to be used to guide the prototyping stage of system development and to ensure the accuracy and completeness of systems.

The sections following the FHD describe each functional area in detail.


Arizona Integrated Criminal Justice Information System Enterprise
DRM System
Enterprise Administration
Collect Disposition Data
Update Disposition Data
Report Disposition Data
Maintain User Profiles
Generate CCID
Collect Non-Fingerprint Supported Data
Collect Fingerprint-Supported Data
Generate CTN
Collect Prosecutor-Initiated Charges
Collect SID and FBI # Against Cycle
Collect Court Initiated Charges
Collect Custody or Supervision Intake Data
Process DNA Sample Data
Make DNA Needed Determination
Process DNA Sample Taken Information
Process DNA Sample Accepted Information
Process Law Enforcement No Referral Event
Process Prosecutor Decision Events
Process Court Dispositions
Process Custody and Supervision Status
Process Amended Charges
Process Court Transfers
Process Post-Disposition Changes
Process Inmate/ Parolee Status Change
Process Incarceration or Parole Sentence Termination
Maintain Criminal History Cycles
Determine When Cycle Complete
Populate Database
Satisfy Notifications
Transaction Log Reports
Create Scheduled Agency Reports
Create On-Request Agency Reports
Create Scorecard Reports
Send Pre-FP Data to Live Scan
Send Transaction Responses
Send Error Messages
Send CCID/CTN Assignments
Export Data to ACCH
Create and Send Notifications
Send Subscription Notification
Send Request for Information/ Reminders
Send Mandatory Notifications
Person Search
Maintain Security Access
Maintain Notification Preferences
Maintain Routing Algorithms
Perform Logging
Process Record Consolidations and Corrections
Validate and Manage Transactions
Validate Transaction Type
Validate Transaction Authorization
Validate Transaction Content
Validate Transaction Against Business Rules
Maintain System Values and Index
Maintain Translation Values
Maintain Code Table Values
Update Interagency Index

4.2 DRM DISPOSITION INFORMATION COLLECTION AND MANAGEMENT

4.2.1 LAW ENFORCEMENT SEGMENT

4.2.1.1 Overview

The DRM will support the collecting of demographic data and the initiation of charges related to a criminal event, whether or not the event resulted in a physical arrest and capture of fingerprints. The Booking segment in Section 4.2.2 describes the capture of data when the initial communication of charges to the DRM includes the submission of fingerprints, such as what occurs in a physical arrest event. This Law Enforcement segment describes the system functionality required to accept non-fingerprint-supported charge data for charges initiated through Cite and Release or other non-fingerprinting events. In addition, the Law Enforcement Segment supports the filing of "Not Referred" dispositions for charges that are not referred for prosecution.

4.2.1.2 Functional Requirements

The DRM will support several functions pertaining to the collection and management of the Law Enforcement Segment of the criminal cycle. Each of these functions is described at a high level in the following sections.

4.2.1.2.1 Accept and Store Non-Fingerprint Supported Demographics and Charges

When a law enforcement segment is entered into the DRM from a source other than an AFIS transaction, this segment will be stored in the DRM as pre-fingerprinting data. The receipt of this information will initiate the establishment of the record, including DRM assignment of a CCID to the record.

4.2.1.2.2 Send CCID Assignment Response

When the law enforcement segment submission results in the creation of a new criminal history cycle in the DRM, the cycle and charge tracking numbers assigned will be returned to the sending agency either through a response message or display on the input web screen.

4.2.1.2.3 Send Pre-Fingerprinting Data to Live Scan Device

If the pre-fingerprinting segment is followed by an arrest and fingerprinting, the DRM will support query from the Live Scan device to pre-populate the Live Scan with the information entered into the DRM. The key for the query

will be the CCID that the DRM assigned at the time that the initial charges were captured.

4.2.1.2.4 Record OCA in Interagency Index

An important part of the integration of data from all agencies that correspond regarding a particular criminal cycle is the ability for each agency to utilize their own agency identification numbers to access their data. The DRM will support recording the originating case agency number into the interagency index and associating it with the assigned CCID. By doing so, the DRM will be able to include the OCA in further communications with the LEA and with other agencies that may also refer to the OCA, such as the prosecutors and courts.

4.2.1.2.5 Create and Track Notification of Fingerprints Needed

Because a characteristic of pre-fingerprint records in the DRM is that fingerprints have not yet been taken and associated with the charges, an important follow-up necessary for this cycle will be the submission of fingerprints. The DRM will create the appropriate notifications regarding the requirement to obtain fingerprints for the cycle. To ensure that positive biometric identification is eventually obtained, the DRM will also support the creation of subsequent messages, as well as delivery of escalation notifications when necessary because there has been no response to previous messages. In addition, the fact that fingerprinting is still needed will be included as part of any interactions the DRM may have with agencies, including both notifications and on-line access to the specific cycle.

4.2.1.2.6 Record No Referrals

When a law-enforcement segment results in one or more charges that the LEA determines it will not refer for prosecution, the agency will be responsible for reporting the disposition of those charges to the DRM. The DRM will support the collection of No Referral dispositions from the law enforcement agency that submitted the charge. If AFIS positive identification has been made for the cycle, the DRM will also report this action as the disposition of the law enforcement segment on the given charge to the ACCH, so that the updated information can be disseminated to law enforcement through standard rap sheet inquiries to the ACCH.

4.2.1.2.7 Return Charges to Prosecutor After Further Investigation

One of the functional requirements of the prosecutor segment will be the ability for the DRM to notify the appropriate law enforcement agency of

charges that the prosecutor declined and returned for further investigation. When a law enforcement agency receives this notification and performs the required investigation, the DRM will support notification to the prosecutor of the results of the investigation or of the decision to not refer the charge(s).

4.2.1.3 Transaction Profile

The DRM will support four incoming transactions in support of the law enforcement segment processing. These transactions include the following:

- Pre-fingerprinting Transaction
- Live-scan Request for Pre-fingerprinting Information
- No-referral Disposition Reporting
- Add Clarifying Information to Cycle/Charge

Each of these transactions is described in the following table.

Pre-Fingerprinting Transaction		
Purpose	To allow law enforcement agencies to enter pre-fingerprinting information into the DRM to initiate charges and establish a CCID before processing of a fingerprint card.	
Initiator	Law Enforcement Agency	
Types of Records to be Processed	Pre-arrest information – typically information stored in an RMS	Typical fields to include: ♦ ORI ♦ OCA ♦ Offense Date ♦ Demographics fields ♦ Charge Information ♦ Offense Code per Charge
Transaction Interface Protocol	XML Document composed of fields compliant with GJXDM schema, transported using SOAP over HTTPS	
Expected Response	Return Message including CCID and CTN numbers assigned by the DRM	
Response Interface Protocol	XML Document composed of fields compliant with GJXDM schema, transported using SOAP over HTTPS	
Live Scan Request for Pre-Fingerprinting Information		
Purpose	To process a request from a Live Scan Device to pre-populate the Live Scan with appropriate pre-	

	fingerprinting information entered into DRM before the fingerprinting event occurred.	
Initiator	Live Scan Device	
Types of Records to be Processed	NIST-based Transaction – Likely an SRE or other simple Message Format	Must include: ♦ ORI ♦ CCID ♦ Offense Date
Transaction Interface Protocol	MIME encoded NIST Formatted Transaction transmitted to the DRM via SMTP over a TCP/IP connection	
Expected Response	NIST-transaction including all of the Type1 and Type2 data in the DRM for this arrest event	
Response Interface Protocol	MIME encoded NIST Formatted Transaction transmitted to the DRM via SMTP over a TCP/IP connection	
No-Referral Disposition		
Purpose	To process a law enforcement agency disposition of a charge through the recording of a no-referral disposition against the charge.	
Initiator	Law Enforcement Agency	
Types of Records to be Processed	Disposition Information, provided at one disposition per charge (CTN)	Must include: ♦ ORI ♦ CCID ♦ CTN ♦ Offense Code per charge ♦ Disposition Code ♦ Action Date
Transaction Interface Protocol	XML Document composed of fields compliant with GJXDM schema, transported using SOAP over HTTPS	
Expected Response	No Response	
Response Interface Protocol	N/A	
Add Clarifying Information to Existing Cycle/Charges		
Purpose	To allow law enforcement to record additional information against a criminal history cycle or	

	charge when a prosecuting agency has referred a charge back to the LEA for further investigation.	
Initiator	Law Enforcement	
Types of Records to be Processed	Arrest Comments, submitted on either a cycle or a charge level	Must Include: ♦ ORI ♦ CCID ♦ Comments May Include: ♦ CTN ♦ Offense code per charge
Transaction Interface Protocol	XML Document composed of fields compliant with GJXDM schema, transported using SOAP over HTTPS	
Expected Response	No Response	
Response Interface Protocol	N/A	

4.2.2 BOOKING SEGMENT

4.2.2.1 Overview

As stated earlier in the discussion of business processes supported by the DRM, the term "booking" as used in this document describes the fingerprinting and reporting steps of booking. It does not include the jail and inmate management aspects of booking.

The DRM Booking Segment will support the input of fingerprint-related data to the DRM as a result of several different business processes. This includes the collecting of demographic data and the initiation of charges related to a criminal event when charges result in a physical arrest and submission of fingerprints to the AZAFIS system. It also includes the processing that will occur any time during the lifecycle of the criminal cycle where fingerprints are captured in support of the initiation of charges.

The Booking Segment also supports the routing of applicable notifications, including notification to the law enforcement Jail Management System (JMS), as well as the ability to cease notification of requirement for fingerprinting to occur when this type of follow-up notification is pending.

4.2.2.2 Functional Requirements

The DRM will support several functions pertaining to the collection and management of the Booking Segment of the criminal cycle. Each of these functions is described at a high level in the following sections

4.2.2.2.1 Create/Update Record in DRM

AZAFIS will return a TX2 message to the originating agency when it has accepted a LiveScan transaction for processing. The return TX2 message contains the demographic and charge data, as submitted to AZAFIS, that are applicable to disposition reporting. Besides sending the TX2 message to the originating agency, the AZAFIS will also forward this TX2 message to the DRM. If the incoming TX2 transaction includes a CCID for which the DRM has pre-fingerprinting information, the DRM will compare the submitting agency with the agency that owns the DRM record. If the agency is the same, the pre-fingerprinting information, including charge information will be completely overridden in the DRM with the data contained in this TX2 message.

If the agency owning the DRM record is a prosecutor, or agency other than the submitter of the AFIS information, as would happen with a warrant or summons situation, the DRM will compare the charges submitted in the TX2 transaction with charges existing in the DRM. If these sets of charges do not match, DRM will report a warning message to the submitting agency. No charge information will be updated by the AFIS transaction, as it cannot be modified from the charges submitted to the DRM when the warrant or summons was reported to the DRM. This processing will help to alleviate data processing errors, and also supports the requirement that only the agency that submits the information is allowed to make modifications to it.

If the transaction involved the initiation of charges that have not been assigned a CCID by the DRM, such as a physical arrest, the DRM will assign the CCID, and initiate a new cycle.

4.2.2.2.2 Associate SID to Cycle

A SID number will be assigned or associated to the record during the processing of fingerprints through AZAFIS. The return TX8 message will contain the SID. The TX8 message will be sent to the DRM, where this process will associate the SID to the criminal cycle, and ensure that the SID is included as a means for searching within the interagency index.

4.2.2.2.3 Associate FBI Number to Cycle

If an FBI number is assigned or associated to the record during the processing of fingerprints through AZAFIS, the return TX10 message will contain the FBI ID. Similar to the process of storing the SID against the cycle, this process will associate the FBI number included in the TX10 message to the DRM record.

4.2.2.2.4 Notify Operator of Assigned CCID/CTN

If a new criminal history cycle was initiated during the processing of the TX2 message, the DRM will assign a CCID to the cycle. If the cycle existed in the DRM before this event, the DRM will validate the CCID and associated charges. The CCID and charge tracking numbers assigned by the DRM will be communicated to the submitter for possible update in their system. .

4.2.2.2.5 Update ACCH

Once the DRM has received the TX2 message from the AZAFIS for a given criminal history cycle, all information recorded in the DRM to date for the cycle is reportable to the ACCH. Therefore, part of the processing of the booking segment in the DRM will include creating and sending the appropriate transaction(s) to the ACCH to update the criminal record with information from the DRM pertaining to the cycle.

4.2.2.2.6 Print Disposition Information Sheet

The contributors of disposition information expressed a desire to be able to print for file a current disposition information sheet. In addition, some processing of disposition information will always remain manual. Therefore, the DRM must support the ability to print a disposition information sheet. For those cases when manual disposition information processing is required, agencies must be able to print the disposition sheet and manually mail it to other agencies for their input into the cycle. Those agencies that require manual receipt of information will be identified in the agencies' user profile. No information that is considered confidential (such as a SID for certain agencies) will appear on this version of the disposition information sheet, unless the agency that requests the information is an authorized requestor.

4.2.2.2.7 Send Notification of Charges to Prosecuting Agency

At the time that the charges, as submitted through the AFIS transaction, are posted, the DRM will create the appropriate notification messages to subscribed prosecuting agencies to notify them of the charges (see Section 4.3.6 for information on notification subscriptions).

4.2.2.2.8 Cease Notification

Upon receipt of a fingerprint transaction, any pending notifications requesting fingerprinting for the cycle will be marked as complete. In addition, all on-line DRM query screens will stop displaying a warning that positive fingerprint identification is outstanding.

4.2.2.3 Transaction Profile

The DRM will support three incoming transactions in support of the booking segment processing. These transactions will all originate at the AZAFIS. In addition, the DRM will support an update transaction to the ACCH at the time that fingerprints are received. This update transaction will submit all disposition information recorded for the cycle to date at the time that the prints are received. The transactions that support the booking functions include the following:

- TX2 Transaction
- TX8 Transaction
- TX10 Transaction
- Update to ACCH

Each of these transactions is described in the following table.

TX2 Transaction		
Purpose	To process incoming arrest information as reported on a fingerprint card, and store that information in the DRM.	
Initiator	AZAFIS	
Types of Records to be Processed	CAR transactions	Must be of valid NIST format for a CAR transaction
Transaction Interface Protocol	MIME Encoded NIST Formatted Transaction transmitted to the DRM via SMTP	
Expected Response	No Response	
Response Interface Protocol	N/A	
TX8 Transaction		
Purpose	To process a SID assignment against an established CCID, and essentially link the person to the criminal event.	

Initiator	AZAFIS	
Types of Records to be Processed	CAR transactions with SID Assigned	Must be of valid NIST format for a CAR transaction, and include the AZ SID
Transaction Interface Protocol	MIME Encoded NIST Formatted Transaction transmitted to the DRM via SMTP	
Expected Response	No Response	
Response Interface Protocol	N/A	
TX10 Transaction		
Purpose	To process an FBI assignment against an established CCID, linking this Federal Identifier to the criminal history event.	
Initiator	AZAFIS	
Types of Records to be Processed	CAR transactions with FBI number assigned	Must be of valid NIST format for a CAR transaction, and include the FBI number
Transaction Interface Protocol	MIME Encoded NIST Formatted Transaction transmitted to the DRM via SMTP	
Expected Response	No Response	
Response Interface Protocol	N/A	
Update ACCH		
Purpose	To update the ACCH with disposition information recorded in the DRM.	
Initiator	DRM	
Types of Records to be Processed	Disposition Information, provided at one disposition per charge (CTN)	Transaction will include: ♦ ORI that reported information ♦ CCID ♦ CTN ♦ CSN or Offense Code Information ♦ Disposition Code ♦ Action Date
Transaction Interface	XML Document composed of fields compliant with	

Protocol	GJXDM schema, translated to a flat file format for processing within the ACCH
Expected Response	Acceptance Message or Error Message
Response Interface Protocol	XML Document

4.2.3 PROSECUTOR SEGMENT

4.2.3.1 Overview

The DRM will support prosecutor actions against existing criminal history cycles, including

- Recording prosecutor actions, and the initiation of added or amended charges in the state repository
- Filing "No File" (NF) dispositions to the ACCH, and
- A notification to law enforcement, such as when the prosecutor determines that further investigation of a charge is required. In this case the DRM will notify the originating law enforcement agency that the case is being returned. .

The DRM will also support prosecutor-initiated cycles/charges. In this case, the DRM will also support the necessary notifications to other agencies, such as requests for fingerprinting, and notification to the court. Each of these functional requirements is explored at a high level in the sections that follow.

4.2.3.2 Functional Requirements

4.2.3.2.1 Process Prosecutor-Initiated Charges

Prosecutor-initiated charges can be of two types. The first type is the initiation of new charges within an existing cycle. The other type of initiation of charges occurs when the prosecuting segment is the first received segment of the criminal history cycle. If the DRM receives an incoming transaction to add charges to an existing cycle, the CCID for the cycle and Offense code information will be required in the incoming transaction. The DRM will assign a CTN for each new charge received. If the transaction is initiating a new cycle as well as charges, the prosecuting agency will submit charges against specific charge statute numbers, but will not include a CCID. In this case, the DRM will process the request, assigning both CCID and CTN numbers to the cycle and charges, respectively.

4.2.3.2.2 Send CCID/CTN Assignment Response

When the prosecuting agency submission results in the creation of a new criminal history cycle in the DRM, the cycle and charge tracking numbers assigned (CCID/CTN) will be returned to the sending agency either through a response message or display on the input web screen. When the submission results in just the creation of new charges, the CTNs assigned to each new charge will be returned to the submitting agency.

4.2.3.2.3 Record Prosecutor Case Number in Interagency Index

To support the requirement of allowing each agency to utilize their own agency identification numbers to access their data, the DRM will support recording the prosecutor case number into the interagency index and associating it with the appropriate CCID. By doing so, the DRM will be able to include the case number in further communications with the prosecutor and with other agencies that may also refer to the agency-specific case number.

4.2.3.2.4 Process Disposition

The prosecutor may send a No File decision on a given charge to the DRM. This decision is considered a disposition against the charge, causing the DRM to process the transaction as a disposition. When the DRM processes this decision, it also sends out notifications to any agencies that have subscribed to receive notification about this type of event against a given cycle.

4.2.3.2.5 Process Amended Charge

This action can only occur if a CCID/CTN/Offense Code that matches the input transaction already exists in the DRM; that is, the amended charge being submitted is a modification to an existing charge. The DRM will process a disposition of amended to the existing charge, and will create a new charge that reflects the prosecutor action.

4.2.3.2.6 Decline Charges for Further Investigation

Another action that a prosecutor may take is to decline a charge or charges on a given cycle for further investigation. When the DRM processes a prosecutor transaction for this purpose, the DRM will mark the charge with the action and will send the appropriate notification to law enforcement in order to obtain further information on the charge.

4.2.3.2.7 Create Notification for Court Segment

This process creates a notification for the Court Segment with all prosecutor elements that are required for the creation of the Court Segment. This

notification will at minimum contain CCID, CTN, Charge Offense information, action, and action date. The DRM will send notification to the court whenever a prosecutor transaction takes action against any of the charges for the given cycle.

4.2.3.2.8 Update ACCH

As long as the cycle that the prosecutor action pertains to includes AFIS identification, all updates to the cycle, including prosecutor file, No File, and amended actions are eligible to become part of the criminal record in ACCH. Therefore, whenever the DRM processes a prosecutor transaction for such a record, the DRM will send an update transaction to the ACCH.

4.2.3.3 Transaction Profile

The DRM will support three incoming transactions in support of prosecutor actions against criminal history cycles. Each of these actions will trigger an update transaction to the ACCH as long as fingerprints have been received for the cycle. This update transaction will submit the new disposition information recorded for the cycle to the ACCH. The transactions that support the prosecutor segment include the following:

- Add Charges
- Process Charges
- Process Charge Amendment
- Update ACCH

Each of these transactions is described in the following table.

Add Charges		
Purpose	The purpose of this transaction will be to add a new set of charges to an existing criminal history cycle, or to initiate a new criminal history cycle.	
Initiator	Prosecutor	
Types of Records to be Processed	Prosecutor Charging/filing information	Must include: ♦ ORI ♦ Action Date ♦ Charge Information ♦ Offense Code per Charge May include: CCID (when adding charges to an existing cycle)

Transaction Interface Protocol	XML Document composed of fields compliant with GJXDM schema, transported using SOAP over HTTPS	
Expected Response	Return Message including CCID and/or CTN numbers assigned by the DRM	
Response Interface Protocol	XML Document composed of fields compliant with GJXDM schema, transported using SOAP over HTTPS	
Process Disposition		
Purpose	To record the disposition against a charge or set of charges within the DRM	
Initiator	Prosecutor	
Types of Records to be Processed	Prosecutor Action of No File Event	Must include: ♦ ORI ♦ CCID, CTN, Offense Code per Charge ♦ Action Date ♦ Action Code
Transaction Interface Protocol	XML Document composed of fields compliant with GJXDM schema, transported using SOAP over HTTPS	
Expected Response	No Response	
Response Interface Protocol	N/A	
Process Charge Amendment		
Purpose	To record the amendment of charges indicating a final disposition of amended against an existing charge, and opening new charges for a cycle.	
Initiator	Prosecutor	
Types of Records to be Processed	Prosecutor Action of Amend Charges	Must Include: ♦ ORI ♦ CCID, CTN, Offense Code of charge to be amended ♦ Charge Offense information for new charge to be added.
Transaction Interface Protocol	XML Document composed of fields compliant with GJXDM schema, transported using SOAP over	

	HTTPS	
Expected Response	No Response	
Response Interface Protocol	N/A	
Update ACCH		
Purpose	To update the ACCH with disposition information recorded in the DRM.	
Initiator	DRM	
Types of Records to be Processed	Disposition Information, provided at one disposition per charge (CTN)	Transaction will include: ♦ ORI that reported dispo ♦ CCID ♦ CTN ♦ CSN or Offense Code Information ♦ Disposition Code ♦ Action Date
Transaction Interface Protocol	XML Document composed of fields compliant with GJXDM schema, translated to a flat file format for processing within the ACCH	
Expected Response	Acceptance Message or Error Message	
Response Interface Protocol	XML Document	

4.2.4 COURT SEGMENT

4.2.4.1 Overview

The DRM will support the collection of court segment information against existing criminal cycles, as well as the initiation of a criminal cycle through receipt of court information. In addition, the DRM will support several notifications of action throughout the processing of court data within the DRM.

4.2.4.2 Functional Requirements

4.2.4.2.1 Refer Case to Different Court

After receiving a case, a court may determine that the case should be referred to a different court. In this instance, the DRM must record the court action

and make all necessary modifications to notifications so that the new court that will be handling the case is the recipient for any further court-specific notifications on the cycle.

4.2.4.2.2 Add or Amend Charges

A second possible outcome of a court decision is the decision by the court to either add new charges or amend existing charges for a cycle. In either case, the court will send the charge information to the DRM. If the purpose of the transaction is to add new charges to an existing cycle, the presence of the CCID and new statutory offense information will prompt the DRM to assign new charge tracking numbers to each statute received and to return these numbers to the submitting court. If the purpose of the transaction is to amend an existing charge, the presence of the CCID, CTN, and existing Common Statute Number, along with the new Charge Offense information will prompt the DRM to record an amended disposition against the given CTN, and to create a new CTN for the new statute provided by the court. If the CSN is implemented as part of the CCID sequence, this transaction will require only the CSN -for the statute in order to specify the statute directly related to the offense.

4.2.4.2.3 Initiate Cycle in DRM

In some cases, the receipt of court information may be the first indication of a new cycle being reported to the DRM. Examples of this are court-initiated charges and Grand Jury Indictments that have not been preceded by an arrest. In this type of situation, the DRM will assign a new CCID to the cycle and will respond to the court with the CCID assigned. Any charges submitted within the transaction will receive DRM-assigned CTN numbers, which will also be communicated to the agency. The DRM will also immediately send the appropriate notifications to request the receipt of fingerprint card data in order to be able to report this cycle to the ACCH.

4.2.4.2.4 Send CCID/CTN Assignment Response

When the court process initiates or amends charges, or when the court process initiates the entire cycle in the DRM, the cycle and charge tracking numbers assigned (CCID/CTN) will be returned to the sending agency either through a response message or display on the input web screen.

4.2.4.2.5 Record Court Case Number in Interagency Index

The DRM must support update of the interagency index with court information. Therefore, upon receipt of court information, the court case number will be associated to the appropriate CCID. This association will

allow the DRM to include the court case number in further communications with the court and with other agencies that may also refer to the specific case number, and will enable the court to perform inquiries of the DRM utilizing their own case number.

4.2.4.2.6 File Disposition

Besides adding or amending charges, another outcome against a cycle is the court decision to file a disposition against a given charge. In this case, the DRM will record the disposition for the charge, along with any sentencing information provided.

4.2.4.2.7 Update ACCH

At the time that the court files a disposition against a charge, as long as the cycle that the court action pertains to includes AFIS identification the action is eligible to become part of the criminal record. Therefore, whenever the DRM processes a court transaction for such a record, the DRM will send an update transaction to the ACCH.

4.2.4.2.8 Process Post-Disposition Changes

When a new disposition request is made against a criminal history cycle that has already been closed, the DRM must be able to process the new disposition and report the information to the ACCH. Upon such a transaction request, the DRM will have to determine that the cycle is no longer being retained in the DRM database and request the record from the ACCH. The DRM will then process the new disposition and will create the appropriate update transactions to the ACCH. Should this update again close the cycle, the information will be removed from the DRM after update to the ACCH. Otherwise, the cycle will remain in the on-line part of the system until such time as all expected dispositions for the cycle have been received and processed.

4.2.4.3 Transaction Profile

The DRM will support four incoming transactions in support of court actions against criminal history cycles. Most of these actions will also trigger an update transaction to the ACCH provided the cycle has AFIS identification. This update transaction will submit the new disposition information recorded for the cycle to the ACCH. The transactions that support the court segment include the following:

- Addition of Charges
- Disposition of Charges
- Amendment of Charges

- Update to ACCH
- Transfer of Case to Different Court

Each of these transactions is described in the following table.

Addition of Charges		
Purpose	The purpose of this transaction will be to add a new set of charges to an existing criminal history cycle, or to initiate a new criminal history cycle.	
Initiator	Court	
Types of Records to be Processed	Court Charging /disposition information	Must include: ♦ ORI ♦ Action Date ♦ Charge Information ♦ Offense Code per Charge May include: ♦ CCID (when adding charges to an existing cycle)
Transaction Interface Protocol	XML Document composed of fields compliant with GJXDM schema, transported using SOAP over HTTPS	
Expected Response	Return Message including CCID and/or CTN numbers assigned by the DRM	
Response Interface Protocol	XML Document composed of fields compliant with GJXDM schema, transported using SOAP over HTTPS	
Disposition of Charges		
Purpose	To record the disposition against a charge or set of charges within the DRM	
Initiator	Court	
Types of Records to be Processed	Court Disposition and Sentencing Information	Must include: ♦ ORI ♦ CCID, CTN, Charge Offense Code ♦ Action Date ♦ Disposition Code
Transaction Interface Protocol	XML Document composed of fields compliant with GJXDM schema, transported using SOAP over HTTPS	

Expected Response	No Response	
Response Interface Protocol	N/A	
Amendment of Charges		
Purpose	To record the amendment of charges indicating a final disposition of amended against an existing charge, and opening new charges for a cycle.	
Initiator	Court	
Types of Records to be Processed	Court Action of Amend Charges	Must Include: ♦ ORI ♦ CCID, CTN, Offense Code of charge to be amended ♦ Charge Offense Information of new charge to be added
Transaction Interface Protocol	XML Document composed of fields compliant with GJXDM schema, transported using SOAP over HTTPS	
Expected Response	No Response	
Response Interface Protocol	N/A	
Update to ACCH		
Purpose	To update the ACCH with disposition information recorded in the DRM.	
Initiator	DRM	
Types of Records to be Processed	Disposition Information, provided at one disposition per charge (CTN)	Transaction will include: ♦ ORI that reported dispo ♦ CCID ♦ CTN ♦ CSN or Offense Code Information ♦ Disposition Code ♦ Action Date
Transaction Interface Protocol	XML Document composed of fields compliant with GJXDM schema, translated to a flat file format for processing within the ACCH	
Expected Response	Acceptance Message or Error Message	

Response Interface Protocol	XML Document	
Transfer to Different Court		
Purpose	To initiate the actions within the DRM necessary to transfer a cycle to a different court, including the update of any pending or future notifications.	
Initiator	Court	
Types of Records to be Processed	Court Action of Refer to Another Court	Must Include: ♦ ORI ♦ CCID ♦ Court Action Date ♦ Court Action ♦ New ORI
Transaction Interface Protocol	XML Document composed of fields compliant with GJXDM schema, transported using SOAP over HTTPS	
Expected Response	No Response	
Response Interface Protocol	N/A	

4.2.5 CUSTODY AND SUPERVISION SEGMENT

4.2.5.1 Overview

Upon sentencing of a defendant to either probation or incarceration, the court makes the appropriate notification to the probation department, county jail or Department of Corrections with a properly executed and signed sentencing order. The DRM will support the notifications that should accompany such actions, as well as the update of custodial status at the point of intake and completion of sentence. In addition, the functionality of the DRM will support the tracking of requirements to obtain DNA samples from the defendant.

4.2.5.2 Functional Requirements

4.2.5.2.1 Notify Custodial or Supervisory Agency of Final Disposition

When the DRM receives sentencing information from the court that includes requirements for custody or supervision, the DRM will send a notification to

the participating custodial and supervisory agencies. This notification will include a disposition report that includes information similar to what is on the current disposition report. In addition, the notification will include information regarding whether DNA sampling is required of the defendant (see functional requirement below).

4.2.5.2.2 Process Custodial Intake Information

At the time that the offender is incarcerated, the DOC or county custodial agency may initiate fingerprinting. If printed at the DOC, the fingerprints will be taken as a print Type 22 record, and the AZAFIS will process the record for identification purposes. The DRM will receive a copy of the AZAFIS response record, facilitating the creation of the corrections segment of the cycle and closing the cycle if appropriate. After updating the cycle with the corrections information, the DRM will supply the information to ACCH according to processing requirements to be determined by DPS.

4.2.5.2.3 Make DNA Needed Determination

Whenever sentencing information is processed in the DRM, the system will utilize AZ policy to determine whether DNA sampling is necessary. This policy is based on the severity of the charges for which the person was convicted, as well as whether a prior DNA sample is available for the given identified SID. If a DNA sample has already been taken for the person, as tracked in the DRM, the disposition report sent to the corrections agency prior to intake will indicate that this requirement is already fulfilled. If DNA sampling is needed, the disposition report will indicate the necessity to take the sample. The determination process will be run immediately following receipt of sentencing information, and prior to the notification event to the custodial agency.

4.2.5.2.4 Process DNA Sample Taken Information

At the time that the agency responsible for taking the DNA sample has taken the sample and forwarded it to DPS, the agency will report that the person has provided DNA. When possible this process should occur after fingerprinting so that positive identification is made against the person providing the sample. At this time, the DPS lab could subscribe to receive notification that the sample has been taken, and is in transit. Within the DRM, the processing that will occur is updating the person record with information indicating that DNA is available, the date that the sample was taken, and the agency ORI responsible for taking that sample. In the future, the DRM could also store the CODIS number assigned to the sample, and could provide additional notifications regarding the sample, such as when it was tested and the results of the testing.

4.2.5.2.5 Process Inmate/Parolee Status Change

During the period of incarceration or parole, an inmate or parolee may change status. Status changes may include such items as facility change, supervising agency changes, parole violation, or re-incarceration. The DRM will process status changes for cycles that it is responsible for managing, and will provide updated inmate and parolee status information to the ACCH as appropriate. If the record is no longer managed by the DRM, the cycle information will be retrieved from ACCH in order to process the new data.

4.2.5.2.6 Process Incarceration or Parole Termination

At the time of either completion of the incarceration or parole period, or termination of parole requirements, the DOC will again notify the DRM of the status change. For completed cycles, no longer available in the DRM, the DRM will have to retrieve the cycle information from ACCH to update the record. This update will be handled differently than other status change updates, as it will involve the creation of applicable notifications to subscribed agencies to inform them of the completion of the segment. As in other status changes, the DRM will have the ability to forward the termination information to the ACCH.

4.2.5.2.7 Update ACCH

Similar to the other segments of the cycle, changes that occur in the custody and supervision segment will trigger automatic updates to the ACCH. The types of events that could be communicated to the ACCH will include intake information, custody status changes, DNA availability information, and custody or parole terminations.

4.2.5.3 Transaction Profile

The DRM will support four incoming transactions in support of custody and supervision segment processing. Each of these actions could trigger an update transaction to the ACCH in order to communicate action on the segment. The transactions that support the corrections segment include the following:

- Segment Initiation (Receive Type 22 FP Card Information)
- Process DNA Sample Taken Information
- Process Offender Incarceration or Supervision Status Update
- Process Termination of Custodial Segment
- Update to ACCH

Each of these transactions is described in the following table.

Segment Initiation (Receipt of Type 22 FP Card Information)		
Purpose	The purpose of this transaction will be to initiate the custodial and supervision segment of the criminal history cycle.	
Initiator	Corrections Agency	
Types of Records to be Processed	Corrections Segment Information	Must include: ♦ ORI, ♦ Incarceration or Parole Start Date, ♦ CCID
Transaction Interface Protocol	Live scan Type 22 Transmission	
Expected Response	Return Message indicating successful transmission upon successful update to ACCH	
Response Interface Protocol	XML Document composed of fields compliant with GJXDM schema, transported using FTP across a secure connection	
Process DNA Sample Taken Information		
Purpose	To record in the DRM information pertinent to DNA samples being taken for a given criminal offender.	
Initiator	Corrections Agency	
Types of Records to be Processed	DNA Sample Taken information	Must include: ♦ ORI who took sample, ♦ SID or CCID, ♦ Sample Taken Date
Transaction Interface Protocol	XML Document composed of fields compliant with GJXDM schema, transported using FTP across a secure connection	
Expected Response	No Response	
Response Interface Protocol	N/A	
Process Offender Status Update		
Purpose	To record any inmate or parolee status changes during the parole or incarceration period.	

Initiator	Corrections Agency	
Types of Records to be Processed	Status Change Information to be defined	Must Include: ♦ ORI, ♦ CCID, ♦ Status, ♦ Status Change Date
Transaction Interface Protocol	XML Document composed of fields compliant with GJXDM schema, transported using FTP across a secure connection	
Expected Response	No Response	
Response Interface Protocol	N/A	
Process Termination of Custodial Segment		
Purpose	To update the DRM and ultimately the ACCH with custodial segment complete information.	
Initiator	Corrections Agency	
Types of Records to be Processed	Discharge or Parole Completion Information to be defined	Must include: ♦ ORI, ♦ CCID, ♦ Termination Date
Transaction Interface Protocol	XML Document composed of fields compliant with GJXDM schema, transported using FTP across a secure connection	
Expected Response	No Response	
Response Interface Protocol	N/A	
Update ACCH		
Purpose	To report/update information in the ACCH in response to custodial or supervision status (corrections segment changes) that are recorded in the DRM.	
Initiator	DRM	
Types of Records to be Processed	Corrections Segment Information	Must Include: ♦ ORI, ♦ CCID, ♦ Status, ♦ Action Date

Transaction Interface Protocol	XML Document composed of fields compliant with GJXDM schema, transported in format of Type 22 AZAFIS submission
Expected Response	No Response
Response Interface Protocol	N/A

4.2.6 JAD RECOMMENDATIONS RELATED TO DISPOSITION COLLECTION AND MANAGEMENT

The JAD and *Strategic Plan* recommendations from Section 1.4.2 that are related to disposition collection and management are listed on the following table. The system requirements provide the basic functionality needed to meet these recommendations; whether or not these specific recommendations will actually be implemented can be determined in the detailed design and development of the DRM system.

JAD Recommendation Type/ No.	JAD/Strategic Plan Recommendation	Relevant DRM System Requirement Section or Sub-section
Automate Workflow/5	Automate the movement of the Disposition Report from criminal justice agency to the next as the individual moves through the arrest and adjudication cycle; automate trigger points for actions.	4.1 Disposition Information Collection and Management
Automate Workflow/6	Assist with reducing the backlog of Disposition Reports; create a web page to enter backlogged reports.	4.1 Disposition Information Collection and Management
Automate Workflow/7	Reduce data entry.	4.1 Disposition Information Collection and Management
Automate Workflow/8	Minimize the potential for data entry errors; reject errors immediately to require correction (real-time error checking).	4.1 Disposition Information Collection and Management
Automate Workflow/9	Assist with matching cases from one agency system to the next, as the case moves through the criminal justice process.	4.1 Disposition Information Collection and Management
Automate Workflow/11	Consider/allow responsibility for creating a Disposition Report for some types of cases to be moved from law enforcement agencies to other agencies.	4.1 Disposition Information Collection and Management
Automate Workflow/12	The system should track arrests that are following a parallel course in different courts	4.1.4 Court Segment
Automate Workflow/13	Allow entry of agency data out of sequence and track responsibility for the missing data.	4.1 Disposition Information Collection and Management
Automate Workflow/14	Simultaneously perform data entry on the same charge item (same PCN/CCID and charge in the	4.1 Disposition Information Collection and Management

JAD Recommendation Type/ No.	JAD/Strategic Plan Recommendation	Relevant DRM System Requirement Section or Sub-section
	database, count) by multiple users	
Automate Workflow/15	Allow agencies to correct entries but ensure that the record can be matched with the DPS record; the original contributor of data should have the authority to change a record. Authority to change data fields should be strictly controlled by agency type and user type.	4.1 Disposition Information Collection and Management
Automate Workflow/16	Allow modifications to dispositions that are made by the courts as a result of compliance or non-compliance with probation	4.1.4 Court Segment
Automate Workflow/17	Include case referral capability to allow agencies to refer the Disposition Report to the appropriate agency to take the next action.	4.1 Disposition Information Collection and Management
Automate Workflow/18	An AKA or alias should be included.	4.1 Disposition Information Collection and Management
Automate Workflow/19	Consider using existing “transfer to” code in court automated systems to notify DRM of court transfers	4.1.4 Court Segment
Automate Workflow/20	Correct disposition reports errors on-screen and resubmit them for approval/acceptance	4.1 Disposition Information Collection and Management
Automate Workflow/21	Track and manage pre-identification Disposition Reports for cite/release and other non-arrest/booking scenarios in which charges are brought	4.1 Disposition Information Collection and Management
Automate Workflow/22	Assign a final disposition charge(s) as needed	4.1.4 Court Segment
Automate Workflow/23	Complete dispositions for multiple PCN/CCIDs with a single live scan event	4.1.2 Booking Segment
Automate Workflow/24	Determine the count number for additional charges that may be amended to a disposition report (PCN/CCID)	4.1 Disposition Information Collection and Management
Automate Workflow/25	Declare that work on a given section of the disposition report is complete	4.1 Disposition Information Collection and Management
Automate Workflow/26	Receive rejected dispositions and DPS transmittals on-line	4.1 Disposition Information Collection and Management
Automate Workflow/27	Track individual charges associated with cases returned after Appellate Review and submit updates to DPS	4.1.4 Court Segment
Information Sharing/31	Add comments to Disposition Report or charges to provide important information to other criminal justice agencies	4.1 Disposition Information Collection and Management
Information Sharing/33	Indicate DNA sample availability or include an indicator that a sample is needed.	4.1.5 Custody and Supervision Segment
Information Sharing/34	Indicate DNA sample has been tested.	4.1.5 Custody and Supervision Segment
Information Sharing/35	Show link between fingerprints and DNA sample for identification purposes.	4.1.5 Custody and Supervision Segment
Tracking and Accountability/75	Identify missing and incomplete Disposition Reports.	4.1 Disposition Information Collection and Management
Tracking and	Generate a Disposition Report for charges that are	4.1 Disposition Information Collection

JAD Recommendation Type/ No.	JAD/Strategic Plan Recommendation	Relevant DRM System Requirement Section or Sub-section
Accountability/76	initiated without fingerprints despite the potential problem of positively identifying the person adjudicated with the original suspect.	and Management
Tracking and Accountability/78	Help clarify names and aliases for the courts.	4.1.4 Court Segment
Tracking and Accountability/84	Recall and delete tracking system Pre-Booking records prior to PCN/CCID generation, or other agency data entry or update of a Disposition Report	4.1 Disposition Information Collection and Management

4.3 DRM DISPOSITION INFORMATION REPORTING

The DRM will need to support several different types of reporting and reporting-related requirements. These requirements vary from the ability of the DRM to provide disposition information on printable reports by specific transaction or agency, to the ability to report disposition information to the ACCH for dissemination, to the ability to provide robust notification and subscription reporting capabilities. In the sections that follow, each of these unique reporting requirements is discussed and the specific functional requirements are identified.

4.3.1 DRM CRIMINAL HISTORY CYCLE MANAGEMENT

Although it is not a reporting function in the strictest sense, criminal history cycles must be managed in order to report record transactions properly and create notifications based on the status of the cycle. Criminal history cycle management refers to the system-level functionality that must occur as records are being processed in order to maintain the state and status of the cycles. For example, upon receipt of a disposition for any charge on a cycle, the status of the cycle itself will need to be determined. It is this type of global "behind the scenes" processing that is captured in this set of requirements for the DRM.

4.3.1.1 Overview

One of the key cycle management tasks that the DRM must perform is making determination of cycle complete. A complete cycle is defined as one for which all expected dispositions have been received, positive identification through fingerprints has been obtained, and any necessary corrections cycles have been initiated. Cycles that meet these criteria are candidates for

movement into the ACCH pursuant to DPS retention rules, while generic data is retained in the DRM for statistical reporting purposes.

Another cycle management task that accompanies the cycle complete determination is the migration of disposition information from the ACCH back into the DRM for any post disposition updates. A complete cycle determination is the trigger that causes a record to become unavailable in the DRM for query and normal update during the time period set by DPS for retention in the DRM. When the DRM receives a transaction that qualifies for accessing such a record, the DRM must include the functionality to bring that record back from the ACCH into active use and management. This means that if the record has been removed from the DRM, the DRM must be able to retrieve the record from the ACCH in order to process the new information. Updates to cycles after they have been moved into the ACCH could include changes in correctional status and post-disposition court changes.

The final requirement in the area of cycle management refers to the satisfaction of notifications. Many of the notifications that the DRM will generate will include "tickler" information for subsequent notifications. Thus, the DRM must make internal decisions upon receipt of any new information of not only whether notifications are necessary, but also whether this information satisfies an outstanding notification. A good example of this is the notification for fingerprinting. This notification must be marked as satisfied at the time that fingerprinting information is received by the DRM to prevent further notifications from being sent for this event.

4.3.1.2 Functional Requirements

The functions that the DRM will need to support for cycle management include the following:

- Making cycle complete determinations
- Retrieving records from the ACCH as needed for post disposition update
- Assessment of notification-complete status

4.3.1.3 Recommendations

The retention period for completed cycles within the DRM will have to be determined and business rules established to ensure that specific disposition information is no longer available from the DRM. System functionality must be flexible and configurable through system parameters utilizing table updates whenever possible that are maintained by system administrators, so that the retention period can be changed to reflect changes in state policy over time.

4.3.2 TRANSACTION LOG REPORTING

4.3.2.1 Overview

Transaction log reporting is the concept that the DRM must be able to provide a detailed view of all disposition information processed through the DRM related to a single criminal history cycle. This detailed view is in essence a history of events that have occurred for a given cycle. Reporting DRM activity in this manner is an essential part of the functionality of the DRM, as it provides chronological information on activities, typical data origination places, length of time between origination of a cycle and final disposition, and other statistical information pertaining to a single criminal history event. Information on queries that are agency-based rather than cycle-based is included in Section 4.3.3 Disposition Scorecard.

4.3.2.2 DRM Functionality

The transaction logging report will be available through a Web interface to the DRM. In order to provide the user with the greatest flexibility in choosing a cycle on which to report, the webpage should provide the user with a series of fields where the user can enter various query parameters. The parameters available should include but not be limited to such things as a date range, transaction type, transaction status, CCID, user created by, and destination agency. In addition, fields should be provided to allow the user to query on various person parameters, such as name and date of birth. Once the user inputs the desired parameters into the page, the system will generate an XML transaction that will be sent to the DRM for processing.

The DRM will process the XML transaction, and will compile the results into a response transaction that will be returned to the user interface screen. Unless a detailed report on CCID was initially requested, the results will be presented in a manner that will allow the user the ability to "drill down" into more details. For example, if the transaction returns a list of CCIDs that have been entered by a certain agency, the user will be able to select a specific CCID to see detailed information on the transactions that have occurred against that CCID. The type of information that the transaction will contain includes the actions that occurred against the CCID, the originator of each action, the date and time that each action occurred, the result of that action, and other specific transaction details. The DRM will also report an overall status of the cycle, including whether information has posted to the ACCH, and whether the cycle is complete. (Please refer to section 4.3.6 for a detailed explanation of cycle complete.) This report is not intended to provide details on the cycle itself, but to instead provide information on the transactions that have occurred for the given cycle.

4.3.2.3 Functional Requirements

In order to provide transaction log information, the DRM must meet the following functional requirements:

- Include a highly-parameterized, web-based query screen
- Provide drill-down capability from a summary list to detailed information on a CCID-by-CCID basis
- Deliver information from the query screen to the database in XML format
- Ensure that only the appropriate fields are included on the report, based on user security rules
- Clearly indicate which records are fingerprint-based

4.3.2.4 Recommendations

Some of the information that resides in the DRM is considered confidential even to some of the users of the system. Because of the differing information that various users of the DRM should be able to see, Northrop Grumman recommends that the initial web screen for the request of the logging report be configured based upon the security of the user logged into the DRM. For instance, if the user is a system administrator at the highest security level, full search capability should be enabled. User access and roles should be determined by policy.

4.3.3 DISPOSITION SCORECARD REPORTING

4.3.3.1 Overview

As detailed in the *Arizona ICJIS Strategic Plan*, the agencies that contribute disposition information are in need of a reporting mechanism that will give them statistical information regarding their performance in reporting disposition information and highlight any potential deficiencies. The lack of this type of reporting tool has made it difficult for agencies to determine whether they are in compliance with reporting requirements or goals.

In addition, DPS could use such a reporting mechanism in order to make determination on the completeness of the records in the ACCH. This same mechanism could be used to assess training needs of the user community.

The reporting capability suggested in the *Strategic Plan* is in the form of a "Disposition Scorecard." The anticipated functionality is that the DRM would be able to utilize the data captured by the transaction logging functions of the system to create reports that meet these critical reporting needs.

4.3.3.2 DRM Functionality

The Disposition Scorecard report will be available through a Web interface to the DRM. Similar to the other transaction log reports, the webpage will provide the user with a series of options or query parameters to include when running the report, based on the user's security clearance into the system. The parameters available should include such things as a date range, distinct agency ORI or set of ORIs, and the option to choose either YTD percentages or actual numbers. The Web interface will transform the inquiry parameters entered on the screen into an XML transaction that will be sent to the DRM for processing.

The DRM will process the XML transaction, and will compile the results into a response transaction that will be returned to the user interface screen. The system will utilize information in the logging tables to ascertain the statistics for several different categories of information. As specified in the *Arizona ICJIS Strategic Plan* and further defined in requirements gathering JAD sessions, the type of information available on the Scorecard will include such statistical data as:

- Pre-booking data for the given date range and ORI, including:
  - Number of open pre-booking charges
  - Number of pre-booking charge transfers
- CCID summary data for the given date range and ORI, including:
  - Number of open cycles
  - Number of rejected charges
  - Number of resubmitted charges
  - Number of completed charges/cycles
  - Number of cycles pending AFIS identification
- Appropriate agency YTD snapshot data, including:
  - Percentage of cycles completed
  - Percentage of cycles open
  - Percentage of cycles with rejected charges
  - Of the number rejected, percentage of cycles with dispositions resubmitted
  - Percentage of cycles lacking AFIS identification
  - Average number of days between different events, such as charge initiation and disposition
- Percentage of charges that are in each of the categories:
  - Felony
  - Domestic Violence
  - Driving Under the Influence

- DNA
- Other

Statistical reports for each agency that submits data to the DRM will be available to that agency, with the summary information tailored to the type of agency submitting the inquiry.

While the statistical scorecard results available to agencies to track and monitor their performance is intended to be limited to the specific agency's data, DPS may want to compare an agency's performance with other agencies of the same type. The scorecard report should have an option to provide both agency-specific information as well as comparative information for an agency based on other agencies of the same type.

4.3.3.3 Functional Requirements

The scorecard-reporting requirement of the DRM mandates the following functional requirements:

- Include a highly-parameterized, web-based query screen
- Deliver information from the query screen to the database in XML format
- Ensure appropriate access to statistical information, based on user security rules.

4.3.3.4 Recommendations

Northrop Grumman recommends that Disposition Scorecard reports be built separately for each type of agency that interacts with the DRM, as a scorecard for a prosecuting agency would likely need to contain different statistical data than a scorecard for a court agency. DPS, on the other hand, would probably want to see reports for all categories, but to see them in a manner in which like agencies are compared against like agencies for statistical purposes.

4.3.4 CUSTOM REPORTING

4.3.4.1 Overview

As DPS and other agencies start using the DRM for tracking and reporting on dispositions, they will develop new reporting requirements that were not identified during the design of static reports for the system. Sometimes these reports will be one-time requests for statistical information, and at other times the reports will become standardized and will be run on a frequent basis to obtain information. This type of reporting requirement is typically referred to as ad-hoc or custom reporting. It provides the capability to perform one-time

or even ongoing inquiries against a database for certain planning or statistical analysis purposes.

An example of a custom reporting request may include a request to provide a count of cycles that have gone through the court transfer process within a certain time-frame, grouped by the type of charges that the cycle contains. Typically, these reporting needs are requests to provide counts of records that meet certain criteria or provide information on the time-between occurrence of certain events for timeliness reporting.

4.3.4.2 DRM Functionality

As with any organized collection of data, reporting needs against that data often surface well after the design of static reports. Frequently, these reporting requests come from legislative entities or other interested public parties asking questions about the data. At other times the agency that owns the system may want to obtain some summary information on the performance of their system.

Regardless of the source of the request, the DRM must be designed with custom reporting requirements in mind. This advanced planning must be taken into consideration during the design of the database so that it is optimized for typical inquiry needs. In addition, providing the ability to run custom reports against a system also requires the configuration of security, so that when a system administrator logs into the DRM in a report mode, the system will be configured to only allow query access to the data. This type of configuration ensures that the user not be able to inadvertently modify data while building reports against that data.

4.3.4.3 Functional Requirements

In order to support the custom reporting requirements of the system, the DRM must be built with the following functionally in mind

- The data model must include relational design concepts that support logical queries against data
- The physical database must be created utilizing such objects as indexes to support required custom reporting response times
- Security configuration must include a set of users who will be inquiry-only users against the data

4.3.4.4 Recommendations

Northrop Grumman recommends that DPS utilize third-party software such as Seagate Crystal Reports for performing custom reports on the DRM. Such reporting packages are typically configured with the ability to connect to

different databases supporting native or ODBC connectivity. The software chosen should support a wide variety of report types including sub-reports, conditional, summary, cross-tab, form, drill down, OLAP, and Top N.

Typically the task of creating custom reports lies with the system administrator or with someone else who is intimately familiar with the data within the system and the relationships between the entities that hold that data. Northrop Grumman recommends that at least initially only a small number of people have access to the custom reporting capability of the system until access and training issues have been resolved.

4.3.5 REPORTING TO ACCH

4.3.5.1 Overview

An important function of the DRM will be that of ensuring that all reportable disposition information is sent to the ACCH immediately upon receipt by the DRM. Arizona requires that before any criminal history information is considered reportable, it must be supported by positive AFIS identification. Because AFIS identification may not occur until after agencies have already completed their interaction with the criminal history cycle, much of the information that should become part of the criminal record of a person is currently not being reported. The DRM will provide agencies with a place to record disposition information before the AFIS identification has occurred, and will forward all disposition information collected on a cycle to the ACCH upon receipt of the AFIS identification.

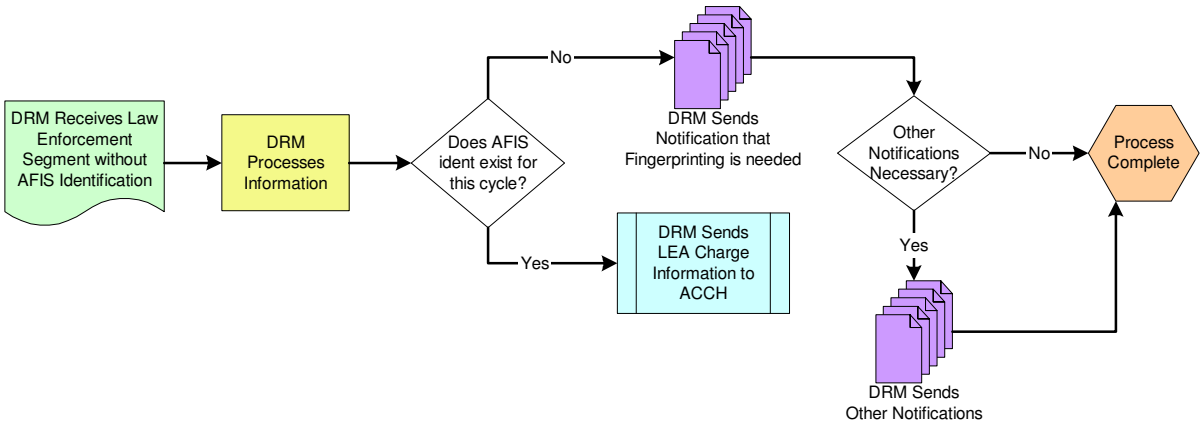
When positive identification has occurred, the DRM will be able to report any subsequent disposition information to the ACCH upon receipt of that information. By maintaining the status of the disposition information, the DRM will manage when and how to report information to the ACCH, taking the burden of that responsibility from the agencies and allowing them to report their information as it is collected.

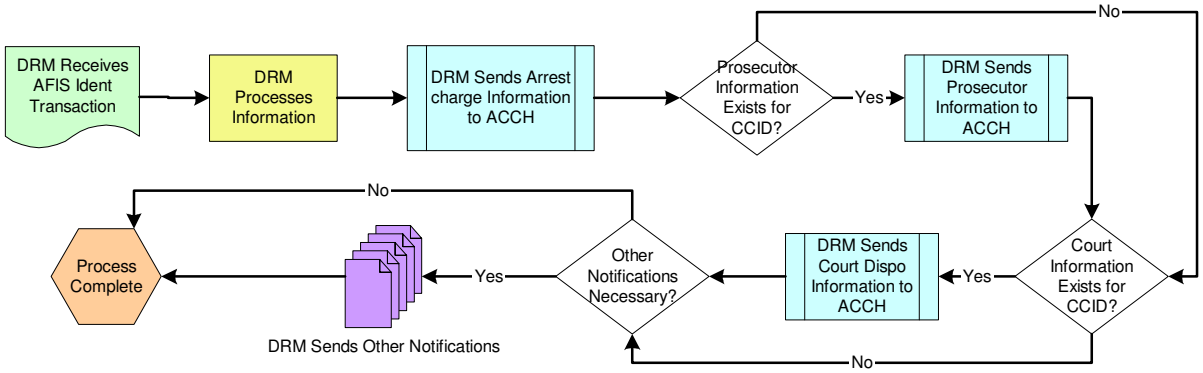
Another limitation of the current paper process for the reporting of disposition information is that the information is only available to the collective criminal justice community at the time that it hits an electronic system – such as AZAFIS, or a court system that has the ability to interface with the ACCH, or the ACCH itself. Therefore, the availability of criminal history information is limited to certain points within the process. The DRM will make the disposition information more readily available at the time it is created by providing a single electronic system for recording that information with the ability to report the information immediately to the ACCH. The result is that criminal history information is available within the ACCH in real-time.

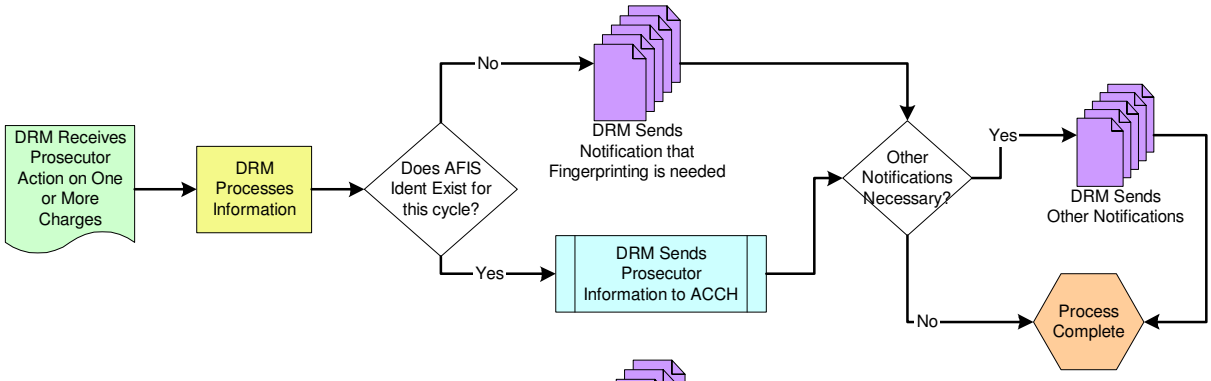
The goal of this reporting requirement of the DRM will be to ensure that the ACCH has the latest disposition information possible for each reportable criminal history cycle, while providing agencies with a means to store and track information until such time as it becomes reportable.

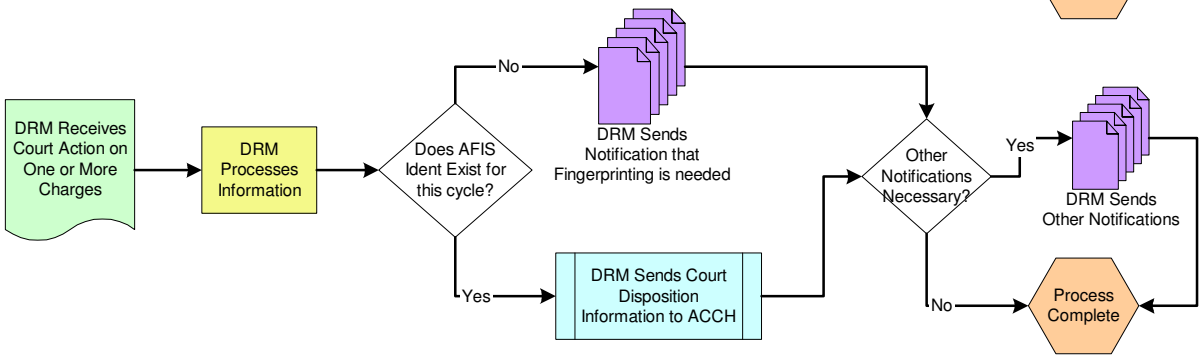
4.3.5.2 DRM Functionality

The DRM will manage the status of all criminal history cycles, and will perform all reporting to ACCH through the e-disposition transaction message queue currently used by AZTEC, Coconino County and Maricopa ICJIS as well as any future revisions or additions to these transactions. Reporting of disposition information will occur as the information is entered into the DRM, so long as the cycle has had positive biometric identification. If no AFIS identification has occurred, the DRM will store all disposition information until such time as the positive identification is received. At that time, all disposition information in the DRM will be available for transfer to the ACCH. The diagram that follows depicts the interaction between the DRM and ACCH for the purpose of reporting disposition information, showing cycle segment information coming in from various sources.


DRM Receives Law Enforcement Segment without AFIS Identification
DRM Processes Information
Does AFIS ident exist for this cycle?
No
DRM Sends Notification that Fingerprinting is needed
Yes
DRM Sends LEA Charge Information to ACCH
Other Notifications Necessary?
No
Process Complete
Yes
DRM Sends Other Notifications


DRM Receives AFIS Ident Transaction
DRM Processes Information
DRM Sends Arrest charge Information to ACCH
Prosecutor Information Exists for CCID?
Yes
DRM Sends Prosecutor Information to ACCH
No
Court Information Exists for CCID?
Yes
DRM Sends Court Dispo Information to ACCH
Other Notifications Necessary?
Yes
DRM Sends Other Notifications
No
Process Complete
No


DRM Receives Prosecutor Action on One or More Charges
DRM Processes Information
Does AFIS Ident Exist for this cycle?
No
DRM Sends Notification that Fingerprinting is needed
Yes
DRM Sends Prosecutor Information to ACCH
Other Notifications Necessary?
Yes
DRM Sends Other Notifications
No
Process Complete


DRM Receives Court Action on One or More Charges
DRM Processes Information
Does AFIS Ident Exist for this cycle?
No
DRM Sends Notification that Fingerprinting is needed
Yes
DRM Sends Court Disposition Information to ACCH
Other Notifications Necessary?
Yes
DRM Sends Other Notifications
No
Process Complete

The DRM will utilize the DPS reporting specifications document, "Local Agency – Arizona Computerized Criminal History System Interface ACCH Disposition Transaction User Specifications" (05/04/2004), as its specification for format and means of transmitting disposition information to the ACCH. Because the DRM will be the only source of reporting disposition information to the ACCH, the DRM will also need to accept the electronic disposition information currently reported by agencies directly to the ACCH. By having this information go through the DRM, the DRM will be able to manage the entire cycle and the ACCH will only need to support one interface for the purpose of receipt of disposition information.

Each time the DRM reports disposition information to the ACCH, the DRM must make determination of whether all expected information for the cycle has been reported. If all dispositions for the cycle have been captured and reported to the ACCH, the DRM will mark the cycle as complete and will store only the information on the cycle that is required for statistical reporting purposes.

4.3.5.3 Functional Requirements

In the reporting of disposition information to the ACCH, the DRM will need to provide the following functionality.

- Accept electronic disposition data from existing applications in DPS e-dispo format
- Validate disposition data against internal business rules
- Format disposition report data into DPS e-dispo format
- Transmit e-dispo transactions to the DPS ACCH input queue
- Archive cycle data for statistical purposes and in accordance with DPS retention rules after successful reporting to ACCH of the complete criminal history cycle

4.3.5.4 Recommendations

Northrop Grumman recommends that the DRM be implemented as a "day-forward" system in order to alleviate the synchronization issues that could occur with trying to manage dispositions for cycles in two different systems. In order to track which cycles will be handled in which system, Northrop Grumman recommends that a flag be added to all records in ACCH to indicate whether or not that record is being managed by DRM. This flag would be set to TRUE for all records managed by the ACCH. This would constitute all records that exist in the ACCH on the system cutover date. All records marked as TRUE would continue to be managed using the current business processes and reporting mechanisms.

All records initiated in the DRM after the cutover date must be sent to the ACCH through the DRM to ACCH interface. Upon receipt of these records, the ACCH would set the "managed in ACCH" flag set to FALSE, preventing any disposition updates to this cycle outside of the DRM interface. The defining event for making determination on the appropriate system for tracking the information should be the date of initiation of charges. Should the DRM receive information on a cycle when the initiation of charges date falls before the cutover date, the DRM should send an error message to the agency, indicating that the legacy means for communication regarding the cycle is required.

4.3.6 CREATING AND SENDING NOTIFICATIONS

4.3.6.1 Overview

Notification and Subscription Processing is a key component of the workflow management functionality of the DRM. It allows users of the system the ability to subscribe to receive specific information and also the ability to be notified via various methods about specific events. Subscriptions can be thought of as "newsgroups" within the DRM solution. Users of the system can subscribe to receive information regarding events or processes that occur within the DRM. Notifications are the means by which the DRM will communicate to a specific user or group of users when actions are needed.

Currently, the "trigger" that an agency needs to complete a part of a given criminal history cycle is physical receipt of the "yellow sheet," the paper form of the Disposition Report. The problems with this type of notification are many, including:

- If more than one agency needs to contribute information, the form must be duplicated and sent to various agencies
- An agency cannot see the form to know what data has been entered and where the cycle is in the process unless that agency is in possession of the form
- The data contained on the form must be interpreted and also keyed into several different systems
- Routing the form to the next destination must be done manually
- Just physically moving the form from one location to the next impacts the total time necessary to complete the disposition
- Agencies often do not know that information, such as positive identification through fingerprints is needed until after the opportunity to obtain that information has already passed

The creation and delivery of notifications functionality of the DRM will alleviate these and other problems inherent in the current manual process.

4.3.6.2 DRM Functionality

The creation and distribution of notifications from the DRM will be a robust feature of the system. Utilizing notification and subscription profiles configured for each notification type and agency, the DRM will have the ability to meet the workflow requirements of the system while also customizing notifications to meet the needs of the recipients. As data is posted to the DRM, any required notifications pertaining to the transaction will be assembled. Using specification information in the DRM at the time that the notification is processed, the DRM will transform the data into a format specified by the agency for the notification type, and will deliver the notification in the delivery format and means specified in the notification profile. One of the greatest benefits of this type of configuration for notifications is that it allows agencies the freedom to change the notification destinations or delivery formats in "real time" without interruption to service.

Several events that occur within the DRM will trigger the creation and delivery of notifications. Whenever information is posted against the DRM, a requirement of the system will be to ascertain whether notifications need to be sent, or whether agencies have subscribed to receive information for this event. If any notifications or subscriptions are needed, the DRM will query the specific notification profile information for the particular agency, and will configure the notification to meet that profile. For example, an agency may subscribe to receive a notification when the event of subsequent arrest for a person with an open Disposition Report occurs. In this case, the DRM will query the notification profile information associated with that particular prosecuting agency and notification type. It will create the notification in the desired format and deliver it to the agency via the means currently identified in the notification profile.

For more information on notification profiles, please refer to Section 4.4.1.3 Create and Maintain Notification Preferences.

Notifications may be sent by the DRM via common delivery mechanisms such as:

- E-Mail
- FAX
- Administrative Messages (NLETS style)
- Queued System Responses
- Splash-screen
- Report

Once a notification has been created, information regarding that notification will be logged in the transaction log tables and attached to the CCID associated with the notification.

On a regularly scheduled basis, follow-up notification messages will be created and sent according to the time interval configured at the time that each notification profile is created. If information comes into the DRM before a follow-up notification message has been sent, the notification cycle will be marked as complete and no follow-up notifications will be created. In addition, users with certain security levels will have the ability to manually disable or auto-complete certain notifications, as well as to re-enable these or any notification message. This functionality will be provided for in the web interface with the DRM.

Besides notifications that are configured and known by the DRM, other notification functionality will be required. Such functionality includes the ability for agencies to send ad-hoc notifications to agencies for clarification of information or decisions. The DRM will support the creation of such notifications and delivery of those notifications via default notification routing profile information, which will be configured in the system when the account is created.

4.3.6.3 Functional Requirements

In order to provide the desired robustness of creating and sending notifications the DRM must meet the following functional requirements:

- Allow agencies to subscribe to notifications based on certain transactions or events that occur within the DRM
- Include mandatory notifications for specific DRM events
- Allow agencies to modify the transmission formats and destinations of the notifications, and have that modification apply to all future notifications
- Allow for more than one recipient to receive a given notification type
- Provide agencies with ad-hoc notification creation functionality
- Automatically complete a notification upon receipt of information that renders the notification no longer necessary
- Allow system administrators to auto-complete notifications and to enable notifications that have been "turned off"
- Create and send notifications in a variety of formats, utilizing a variety of delivery mechanisms

4.3.6.4 Recommendations

In order to ensure that agencies receive notifications for important events, such as the need for fingerprinting, Northrop Grumman recommends that DPS identify a certain set of notifications as mandatory. These notifications would be configured for all agencies, and agencies would not have the ability to turn them off. In addition, certain notifications should be defined so that only a specified set of delivery formats and/or means are allowed. For example, a policy decision could be made that the notification that fingerprints are required must have a delivery requirement of email or splash-screen notification, rather than allowing an agency to specify a report as the delivery means.

4.3.7 PERSON SEARCH

The ICJIS *Strategic Plan* discussed a needed disposition-reporting process improvement of being able to use agencies' own case numbers to query the statewide tracking system about Disposition Reports charges or persons. In addition, agencies interviewed during this process reported differences in procedures used to handle aliases leading to the inability of the agencies to use their own names and identification information when searching on individuals. Establishment of the interagency index is intended to help meet these needs. However, the availability of the interagency index for recording agency-specific identification numbers must be coupled with indexed searches on these numbers, as well as names and other person identifiers (such as DOB and SOC) to allow agencies to find the subjects and disposition reports they are looking for.

4.3.7.1 Overview

To accommodate on-line transaction processing and querying, the DRM will include a person search web page that will interact with a person search service. This web page will allow users to enter search criteria, including items such as name, DOB, CCID, docket number, and others, to query the DRM system. The person search service will receive the search criteria submitted through the web page. It will use criteria based on the submitter and type of search initiated to perform a scored search of the records contained in the DRM. All candidates that receive a score that is above a configured threshold value on the match will be returned to the search result candidate web page, where the user will be able to choose the appropriate candidate.

Batch and other non-interactive transactions that the DRM processes will also utilize the person search functionality. In these cases, the DRM will utilize the search criteria in an attempt to find one person and event that matches the submitted values. Because system-to-system exchanges of information will

contain such identifiers as CCID and CTN, as well as agency-specific case numbers, these searches are anticipated to result in a positive single match in the majority of cases. For those cases when a single person is not identified, the DRM will return an error message to the sending system, requesting manual intervention to assist with the match.

4.3.7.2 Functional Requirements

In order to serve the needs of the agencies that will report information to the DRM, it must include a person-search module that meets the following functional requirements:

- Scored matches with configurable threshold settings
- Searches against the interagency index as well as name and identifier value combinations
- Transaction-specific rules that determine what constitutes a positive match
- Web screens that support entry of search criteria as well as display and "drill-down" capability of returned candidate lists
- Highly-visible indicators on the query web screen that a disposition report is or is not associated with fingerprints
- "Soundex" matches on names

4.3.7.3 Recommendations

Due to the variety of spellings of persons' names, Northrop Grumman highly recommends utilization of a soundex-based name-searching algorithm. Soundex searches allow you to compare words that are spelled differently, but sound alike in English. For example, searches against the name Smith, would be phonetically compared rather than utilizing typical character-by-character matches so that submission of the name "SMYTH" would constitute a possible match.

4.3.8 JAD Recommendations Related to Disposition Reporting

The JAD and *Strategic Plan* recommendations related to disposition reporting are listed on the following table. The system requirements provide the basic functionality needed to meet these recommendations; as stated earlier, whether or not these recommendations will actually be implemented can be determined in the detailed design and development of the DRM system.

JAD Requirement Type	JAD/Strategic Plan Recommendation	Relevant DRM System Requirement Section or Sub-section
Automate Workflow/10	Notify the appropriate agency to take action on missing or incomplete data.	4.2.5 Creating and Sending Notifications
Information Sharing/28	Provide access to other agencies' disposition data (particularly prosecutors, who would like to know if another jurisdiction also has an active case on the same individual); allow access to status of that disposition.	4.2 Disposition Information Reporting
Information Sharing/29	Notify DOC of new sentencing events so that DOC does not release an individual that has been re-sentenced.	4.2.5 Creating and Sending Notifications
Information Sharing/32	View court sentencing results for completed Disposition Reports and charges	4.2 Disposition Information Reporting
Notifications/43	Notify courts when fingerprints need to be ordered when the individual appears in court.	4.2.5 Creating and Sending Notifications
Notifications/44	Notify law enforcement agencies when fingerprints are needed for a case.	4.2.5 Creating and Sending Notifications
Notifications/45	Notify agencies of the final disposition.	4.2.5 Creating and Sending Notifications
Notifications/47	Consider e-mail notifications with links that must be selected to discontinue the notification, as a method to encourage the agency to review the information.	4.2.5 Creating and Sending Notifications
Notifications/48	Include op in/op out features in notifications.	4.2.5 Creating and Sending Notifications
Notifications/49	Notify agencies if a Disposition Report is beyond the allowable age for closure (depending on state policy on closing Disposition Reports).	4.2.5 Creating and Sending Notifications
Notifications/50	Age by days each charge activity or charge event from the date of final disposition using a new 72-hour standard to identify tardy Disposition Reports	4.2.5 Creating and Sending Notifications
Notifications/51	Notify prosecutors if a person has been arrested on subsequent charges.	4.2.5 Creating and Sending Notifications
Notifications/52	Notify DOC of arrests for persons under DOC supervision	4.2.5 Creating and Sending Notifications
Notifications/53	Notify courts and law enforcement that a scheduled release of a DOC inmate has taken place	4.2.5 Creating and Sending Notifications
Notifications/54	Notify judges if new charges have been issued that violate an offender's conditions of probation or release.	4.2.5 Creating and Sending Notifications
Notifications/55	Inform law enforcement when the County Attorney files a case	4.2.5 Creating and Sending Notifications
Notifications/56	Notify agencies of time-sensitive deadlines.	4.2.5 Creating and Sending Notifications
Notifications/57	System should not notify agencies of successful data transactions.	4.2.5 Creating and Sending Notifications
Notifications/58	Get feedback from the process that work has been submitted successfully	4.2.5 Creating and Sending Notifications
Notifications/59	"Op out" feature must have a end date after which	4.2.5 Creating and Sending

JAD Requirement Type	JAD/Strategic Plan Recommendation	Relevant DRM System Requirement Section or Sub-section
	an agency can no longer op out of notifications (DPS)	Notifications
Notifications/60	If the recipient of a required notification does not take the required action, the notification should be elevated to someone in a higher level of responsibility in the agency (DPS)	4.2.5 Creating and Sending Notifications
Reporting/61	Produce reports on what the state has in each jurisdiction, so that each agency can verify what has been sent to their office; produce reports showing dispositions that DPS is expecting and has not yet received.	4.2.2 Disposition Scorecard Reporting
Reporting/62	Show the current status of a disposition followed by a summary of the processing events to date; allow the user to drill-down for detailed information.	4.2 Disposition Information Reporting
Reporting/63	Allow prioritization of agency Disposition Report activity reports by seriousness of the charges and other factors.	4.2.2 Disposition Scorecard Reporting
Reporting/64	Provide a common report generated for all agencies for agency Disposition Report activity reports.	4.2.2 Disposition Scorecard Reporting
Reporting/65	Create reports on outstanding dispositions that are available to authorized users; provide an option to receive the report automatically or upon request.	4.2.2 Disposition Scorecard Reporting
Reporting/66	Allow users to search for records by PCN/CCID or name and DOB. (Strategic Plan added search by agency case numbers)	4.2 Disposition Information Reporting
Reporting/67	Check agency's success rate for submission of disposition reports	4.2.2 Disposition Scorecard Reporting
Reporting/68	Print a snapshot of the Disposition Report form at any stage of the process, with time, date and name stamped by the system	4.2 Disposition Information Reporting
Reporting/69	Produce agency exceptions reports including corrective action required by the agency	4.2.2 Disposition Scorecard Reporting
Reporting/70	View all Disposition Reports and charges in progress for a given person based on common SID; view all pre-booking records and charges in progress for a given person based on common demographic data and numbers like social security, MVD ID	4.2 Disposition Information Reporting
Tracking and Accountability/77	Inform agencies of the current status of a Disposition Report.	4.2 Disposition Information Reporting

4.4 DRM SYSTEM AND ENTERPRISE ADMINISTRATION

This section describes the management functions that will support DRM system administration. These functions include the management of user access, notifications and subscriptions, and code tables, as well as enabling record updates and cycle management, translation and indexing services, and logging. Although the following functionality is described in the context of DRM administration, these same functions could be reused for AZICJIS enterprise administrative purposes for other integration applications.

4.4.1 CREATE AND MAINTAIN USER PROFILES

4.4.1.1 Overview

User profiles are the user-specific details that must be contained within the DRM. These profiles fall into one of two categories. The first category is the profile information needed to guarantee appropriate access to DRM modules. This includes the initialization of roles and security measures that enforce data access control based on those roles. The second category of profile information is related to the configuration of default routing and notification hierarchies for supporting the notification functionality of the DRM. Each of these components of the user profile is discussed in the sections that follow.

4.4.1.2 Create and Maintain Security Access

For criminal justice information, particularly information that contains both fingerprint supported and non-fingerprint supported data, strict control on access to that data is paramount. In addition to the authentication access control that will be handled at the architecture layer, access control to specific types of information must also be provided at the data access layer.

4.4.1.2.1 Security Access Overview

The DRM will be designed so that the access to data and specific screens within the DRM is controlled through configurable user profiles. A single user of the DRM may use the system for different purposes. Thus, the DRM must take access control to another detail level so that access to specific information within the system is dependent upon the role the user is assuming at the time that access is made to the DRM.

4.4.1.3 Create and Maintain Notification Preferences

One of the current disposition reporting challenges is the lack of an efficient and effective means for timely communication among the agencies that work with a particular criminal cycle about the information and action needs of the cycle. This type of interaction and communication is commonly referred to

from a system design perspective as *workflow*. In order to effectively communicate the expected next input steps in the process, a mechanism must exist for notifying appropriate agencies of the current status of that cycle. In addition, reminder or "tickler" as well as escalation notification mechanisms must be in place to ensure the timely reporting of information critical to the progression of the cycle through the system. The notification component of the DRM will address these needs and will provide the ability to configure notifications at a notification type level, as well as providing agencies the flexibility to "opt in" or "opt out" of certain optional notification types. The notification preferences configuration will establish the appropriate notification relationships and the means and format by which notification to agencies will occur.

4.4.1.3.1 Notification Management Overview

While many of the notifications that the DRM will support will be configurable through "subscriptions" that are set up and maintained by the specific entities, some of these notifications will be mandatory because the information contained in the notification is considered critical. The mandatory notifications will require default routing and delivery instructions, and thus must be configured at the time that the new entity profile is created. Default routing and delivery profiles can be overridden through notification management configuration that is performed on a notification type basis; however, agencies will not have the ability to disable mandatory notifications.

The subscription functionality of the DRM will allow the users to turn on or off subscriptions to various types of information or events. Similar to other common newsgroup subscriptions, the ability to choose those areas in which the agency wishes to subscribe to receive information will be configurable at an agency level. In order to support this functionality, the DRM will have a notification and subscription maintenance screen.

When an account is initialized in the DRM, default notification routing information will be keyed into the system. This information will include, at a minimum, such items as:

- Delivery mechanism (such as email, splash screen, reports)
- Notification destination (such as email address, system IP address)
- Escalation notification destination

The default notification routing information will only be used when specific notification profile information is not present. Agencies will have the ability to enter specific notification information on the notification and subscription maintenance screen in order to designate delivery mechanism and destination, as well as other notification preferences by notification type. For example, an

agency may want to be notified via email whenever fingerprints are needed for a particular criminal cycle, but may prefer to receive notification via a "splash screen" upon entry into the DRM when the agency needs to report action on a specific cycle. Details of mandatory notification profiles will be modifiable by both the agency receiving the notification and the system administrator. The DRM System Administrator will be the only user authorized to disable or inactivate such notifications.

Besides notifications for required or missing information and for workflow routing purposes, the DRM will also include subscription notification functionality. Similar to notification maintenance, subscriptions will also be configurable by type, with the ability to determine both the destination of the subscription notification and the delivery mechanism. Unlike notifications, subscriptions will not use default routing and configuration information but will rely on the routing and delivery preferences designated at the time the agency creates the subscription. The agencies will access the notification and subscription maintenance screen to subscribe to information regarding events or actions that take place within the DRM. Agencies will be allowed to freely turn on or off such subscriptions and to change the preferences associated with each subscription type. As with all data within the DRM, only data that the agency is authorized to see will be available through subscriptions.

When agencies receive notifications, a possibility exists that the agency is not the appropriate entity to receive the notification. When this occurs, the agency will have the ability either forward the notification to the appropriate agency or to reply to the DRM that the notification is not appropriate. Such responses to the DRM will be sent to an error queue for appropriate re-routing. System Administrators will be able to view the information in this queue, providing them the opportunity to make adjustments to default routing assignments within the DRM if they find that messages are being returned on a regular basis for a given event from a particular agency.

4.4.1.4 Functional Requirements

A System Administrator or other appropriate level personnel will create and maintain user profiles through the Web Interface to the DRM. After logging in as a System Administrator, this administrator will act as an account manager to establish all new accounts that access the DRM and to define the privileges and default notification routing relationships for each account. In addition, the administrator will configure all mandatory notifications for each agency that participates with the DRM. The system requirements that must be in place to support this functionality include:

- Access by the System Administrator in order to create new accounts and new roles for existing accounts
- Ability to set default delivery means, format and location for mandatory messages
- Ability to establish specific delivery means, format, and location(s) on a notification or subscription type level
- Ability to designate certain notifications as mandatory, preventing agencies from disabling them
- Ability to provide a robust offering of subscription notification opportunities for agencies to receive information about events that occur within the DRM
- Flexibility to change the routing or formatting of notifications or subscriptions and have those changes take effect for all notifications that the DRM sends from that point forward
- Capability to support automatic query, push, pull, publish, and subscribe features

4.4.1.5 Recommendations

Northrop Grumman recommends that DPS require all agencies that will use the DRM system to complete a user agreement form. The intent of this form will be to ensure that the agency understands the specific data-sharing rules that are part of the DRM as well as the required notifications that the agency will receive. In addition, the agency will use this form to define the communication relationships with other agencies as well as the default notification destination and delivery mechanism. All unique accounts (that is, a user account assigned to one person) and roles associated with these accounts will also be identified in the agreement.

Another recommendation is that DPS employ a concept of user classes for the configuration of users. User classes are the groups that users may be associated to specific agency types; for example, the Law Enforcement Agency Class would include all LEAs that participate in the DRM and the Prosecutor Class, would include prosecuting entities. System Administrators will ensure appropriate users are members of applicable classes. User classes will be used by the DRM to simplify the security access administration of the DRM through providing class specific default authorization, but will also allow for security modification by account to specific transactions, processes, events, etc. where appropriate.

For the notification functionality of the DRM, Northrop Grumman recommends that all mandatory, workflow-related communication between agencies be considered notification management, and that all optional notifications be considered subscriptions. This will allow DPS to differentiate

between the types of communications and will simplify the process of configuring both notifications and subscriptions. State policy will need to dictate the types of communications that should be considered notifications and those that can be instead thought of as subscriptions. Examples of types of notifications and subscriptions that the DRM would handle include the following:

- Subsequent arrest event for an open Disposition Record
- Parole or probation violation events
- Reminders for outstanding dispositions based on defined aging periods
- Consolidation events for an open Disposition Report
- Expungement events for an open Disposition Report
- New charges initiated
- New action taken on a previously closed cycle
- Status information whenever a Disposition Report "changes hands"
- Fingerprints needed for a given cycle

4.4.2 MAINTAIN CODE TABLES

4.4.2.1 Overview

Code tables are sets of allowable values grouped by type that serve to standardize how data is collected and reported. In nearly all communication of criminal justice information with federal entities such as the III, standard sets of codes are used to define data. These codes include values for hair color, eye color, and race, as well as data. The DRM will utilize such standard codes for the storage and communication of data to the ACCH, but it will also provide user-friendly definition of the meanings of the codes for the users of the DRM. This will be accomplished through the use and maintenance of code tables for the storage of both the codes and the descriptions of these codes.

In many cases, additions or modifications to the codes themselves will not be allowed, as these codes may drive functionality within the system or be based upon national sets of data. However, in some instances the system administrator of the DRM will be able to add new codes to the existing code tables. In nearly all cases, the System Administrator will be able to change the description that the users of the DRM see and that are associated to the specific codes.

4.4.2.2 DRM Functionality

The DRM will be required to store data in a consistent means that allows for standardized storage and understanding of that data as well as communication of that data with ACCH. Whenever available, the DRM will utilize standard sets of data already defined by ACJC, such as the codes identified in the Report of the XML Data Dictionary Subcommittee, published in November 2003. The DRM will utilize code tables where standardized data is needed so that the description of the data can be customized by the system administrator, but the data is stored in a manner that is easily searchable and reportable, as well as sharable with other entities.

The DRM will include web screens that can be utilized for the maintenance of code table values. These screens will provide the functionality to query, insert, and update code table values when appropriate.

4.4.2.3 Functional Requirements

The DRM must meet the following functional requirements with respect to code table maintenance:

- Utilization of existing allowable values established by ACJC
- Ability to download ARS code values for Statutes from the ACJC site on a regular basis in order to keep the DRM application current.
- Restriction of the authorization to modify code values to System Administrators, and only to allowable tables
- Validation of new information entering the DRM against code table values to ensure consistency in reporting

4.4.2.4 Recommendations

Northrop Grumman recommends that only certain users, such as the System Administrator, have access to modifying the descriptions of code table data. By restricting this access to only a few individuals, the DRM code table data definitions will remain more static and consistent throughout the system.

4.4.3 MAINTAIN TRANSLATION VALUES AND INTERAGENCY INDEX

4.4.3.1 Overview

Translation of values refers to the process of rendering information from one system into another in a means that allows systems to communicate similar information utilizing dissimilar nomenclature or values. Translation values for the DRM will be used for one of the following two purposes:

- To transform data from interface or contributing systems into values known by the DRM
- To link key values from several systems into a set of indexed values to aid in the searching of data as well as the appropriate communication of data among different entities

An example of the first purpose of translation values is use of disposition codes. If the DRM uses a code of "GLTY" for a guilty disposition, but a court system uses "G", then a translation code table will be necessary to map the "G" in the specific court system to the code of "GLTY" as the transaction is processed.

The other translation that the DRM will perform refers to the incorporation of the Interagency Index as described in the *Arizona ICJIS Strategic Plan*. This is a means of storing agency specific tracking numbers in a common index against information contained in the DRM to support the searching and reporting needs of the agencies. The purpose of such an index is to allow for the collection and cross-referencing of typical agency tracking numbers along with the required DRM tracking numbers. The DRM will include an interagency index that maps, at minimum, the following typical tracking numbers to a criminal history cycle CCID.

- LEA Segment – OCA
- Prosecutor Segment – Case Number
- Court Segment – Docket Number
- Corrections Segment – Corrections Sequence
- AFIS Segment – PCN
- Person – SID

Not only will the interagency index then be able to support query against the specific agency identifiers, but it will also support the appropriate interaction between agencies when they need to communicate with each other on the actions taken on a particular case. For example, if a prosecuting agency needs further information from the law enforcement agency on the original initiated charges, the prosecutor can refer to the specific OCA when requesting the clarification.

4.4.3.2 DRM Functionality

The DRM will maintain a set of code translation tables that consist of interface-specific data values. These code tables will be utilized for the purpose of translating data values that are sent to the DRM from known interfaces to values that the DRM can use. The combination of the interface

agency and code type will dictate where the application will look to translate the values to DRM accepted codes.

The DRM will include a Maintain Translation Web page to support this process. This web page will allow a user from one of the distributed systems to view, insert, update, and delete the mapping of values used by their system to the list of valid values accepted by the DRM.

As new transactions are processed by the DRM, the translation code tables will be consulted to handle automatic conversion of values into codes that can be stored in the DRM.

The DRM will also support translation values in the context of the Interagency Index. As transactions are processed from each agency, specific tracking numbers included in those transactions will be stripped from the transaction and stored against the cycle with the appropriate agency identifying information. The DRM will be able to utilize these agency specific tracking numbers in communications to the contributing agency regarding the cycle. In addition, agencies will be able to query the DRM based on their own unique identifiers.

4.4.3.3 Functional Requirements

The maintenance of translation values is key to both the integration of data from the various sources that will contribute information to the DRM as well as in the communication of cycle events to agencies. The DRM must provide the following functionality to support this requirement:

- Ability to store translation values from all systems that interact with the DRM against DRM-supported values
- Utilization of common GJXDM-defined fields
- Ability for on-line modifications to the translation values used as systems that rely on those values change
- Ability to tie common agency-specific tracking numbers to the criminal history cycle they represent
- Ability to communicate with agencies utilizing the tracking numbers supported by their systems
- Ability to allow queries against DRM data utilizing any of the tracking numbers stored within the interagency index

4.4.4 PROCESS RECORD CONSOLIDATIONS AND CORRECTIONS

Because the DRM will be designed to accept information from any segment of the criminal history cycle in any order, it will be possible to have different

segments of the same cycle recorded in the DRM under different CCIDs. In order to accommodate such cycles, authorized users of the DRM must be provided the functionality to reconcile and combine fingerprint-verified "one-and-the-same" segments into a single criminal history cycle. In addition to the consolidation functions, all submitters of data must have the ability to perform limited, audited corrections to data they have contributed to the DRM to fix errors.

4.4.4.1 Overview

The DRM will be constructed to support the tasks necessary to successfully combine cycle segments that DPS has determined are parts of the same cycle. If an agency discovers two different CCIDs assigned to what is believed to be a single cycle they will notify DPS of the situation. DPS will take the appropriate steps to positively identify the subjects of each cycle in order to verify that the information belongs to the same cycle. If this determination is positive, the staff will choose the CCID that should remain with the cycle, and will provide the direction necessary for the DRM to correctly associate the charges from the cycle segments to one another under a common CCID. The system will then send follow-up notifications to all agencies that have had interaction with either CCID in order to notify them of the consolidation.

In order to fix data-entry mistakes for data that has already been reported to the DRM, agencies will be provided with web access to correct information they reported. Any and all modifications to DRM data must be logged through the logging feature of the system, discussed in section 4.4.5.

4.4.4.2 Functional Requirements

In order to provide the flexibility required to correct DRM information, including duplicate cycles and data entry mistakes, the DRM will support the following functionality:

- Web-based access to cycles to investigate the information that resides within the DRM
- Ability to choose the CCID that will remain with the cycle upon the consolidation of two cycles
- Ability to link charges from combined cycles together
- Ability for agencies to correct data that they submitted to the DRM
- Notification to agencies of consolidations and corrections
- Update to the ACCH to communicate consolidations and corrections.
- Logging of the modifications that have occurred for audit purposes.

4.4.4.3 Recommendations

Only DPS DRM users with appropriate security clearance will have the ability to determine that two cycles should be combined. Northrop Grumman recommends that DPS set policy governing when cycles can be consolidated, and that this process be fairly manual so that DPS has control over how the charges from the cycles are matched in order to ensure that the data is combined correctly.

4.4.5 LOGGING

Logging is the process of tracking changes that have happened within an application as a way of accounting for the data that exists within the system. When logging is performed as an integral part of the system, a user can determine the series of events that have occurred and can thus review those events for reporting or trouble-shooting purposes.

In addition to logging each transaction posted to the system, the system will log specific user information at the time of logon. This information will include the date and time of logon and the IP address of the user. All failed login attempts will be recorded along with the name, password, and IP address of the attempted system user.

4.4.5.1 Overview

In order to provide an audit trail that gives the history of processing within the DRM, the system will track all incoming and outgoing transactions. When a transaction is reported to the DRM, either through a direct interface or through batch mode, the transaction will be parsed. Key information from the transaction itself, its resulting processing status, the date and time the transaction was processed, and the transaction origination information including the sender and the date and time the transaction was received will be recorded into a transaction log table. All transactions will be recorded against the CCID to which they apply, providing a history of events that have occurred within the DRM for a given cycle.

Due to the security requirements of the DRM, logins to the system will also be tracked and logged. The system will track failed logon attempts, and will have the ability to lock out user accounts upon a configurable number of failed login attempts per user. At that point, the user account will be disabled and will need to be reset by a system administrator.

The final requirement of logging is the ability to track specific user information against a record in the DRM. The system will include audit fields within the specification of each table. These fields will track the date and time each record was added to the table, as well as specific user information of the

originator of the record. In addition, the same information about the latest update to the record will also be tracked in the table.

4.4.5.2 Functional Requirements

In order to support logging of transactions as well as both DRM access and record changes, the DRM must provide the following functionality:

- Automatic logging of all transactions that process through the DRM (either into or out of the system)
- Logging of all notifications, including the notification text and destination
- Logging of record state changes to capture what changed and which user made the change
- Logging of failed sign-on attempts
- Automatic password change requirements
- System-defined complexity levels for password creation

4.4.5.3 Recommendations

Because each transaction must be parsed before logging, Northrop Grumman recommends that it be at logging of the transaction when the system will also check for subscription notifications. Should any notifications be necessary following processing of the transaction, these notifications will become part of the overall transaction process, and will be recorded in the transaction log.

4.4.6 TRANSACTION VALIDATION AND MANAGEMENT

Any system that processes incoming transactions must perform a certain amount of validation of these transactions. This validation ranges from ensuring that the transaction is one that the system is aware of, to ensuring that the appropriate data fields are present in the transaction. Whenever any inconsistencies are found, error messages must be sent to communicate the problems with the transaction. This type of processing is referred to as transaction validation and management.

4.4.6.1 Overview

Whenever the DRM receives a transaction, a certain amount of generic processing will occur. The validation process begins with ensuring that the DRM expects the given transaction type, and knows how to processes it. Each transaction that the DRM will support must be documented within the system. A table-driven means to match transactions to the XML Schema Document that they should use for field validation is recommended as a

component to the DRM. Any transaction not defined within this transaction table should be rejected by the DRM.

Another validation process that the DRM must support is ensuring that the originator of the transaction is authorized to submit the specific transaction. The DRM should contain the functionality to ensure that data is received by the appropriate ORIs and that no transactions are processed for unauthorized agencies. This is similar to the purpose code validation that occurs in the submission of NLETS-style inquiry transactions to criminal history repositories.

The next level of validation that the DRM must support is validation of the contents of each transaction. This type of validation should be against a GJXDM compliant XML Schema that tests the validity of both the content model and the specific units of data. Content model validity refers to the order and nesting of tags within an XML document. It ensures that all required fields are present, and that the general structure of the document complies with the rules of the schema against which it is being compared. Validation of the specific units of data refers to the validation of data types and of specific rules for the data, such as that a date must be before the current date.

If a transaction fails any of the above validation points, the DRM must be able to return an error message, specifying the type and nature of the error. In addition to the above validation that may return an error message, if other application-specific errors occur in the processing of a transaction, the DRM must return an error. An example of an application-specific error would be a request to amend a charge, but the given CCID/CTN combination does not match any CCID/CTN combinations within the DRM.

4.4.6.2 Functional Requirements

In the area of transaction validation and management, the DRM must support the following functionality:

- Transaction validation – the submitted transaction must be validated as one that is known to the DRM
- Authorization validation – the submitting agency must be authorized to submit the type of transaction or perform the requested type of query
- Transaction format and content validation – the transaction must meet both content model and data unity validity requirements
- Business-rule specific validation – the transaction must include enough information for the system to accurately complete the transaction request

- Error Messaging – upon error in any of the validation checks, the DRM must support the timely return of error messages, and provide ability to correct the error on-line.

4.4.6.3 Recommendations

In systems that Northrop Grumman has built that contain a transaction-processing interface, Northrop Grumman has had tremendous success with limiting the number of repeat reject messages for a given transaction by performing all error checking possible up front. Therefore, Northrop Grumman recommends that transaction-processing routines for the DRM be built in the same manner, so that all possible error conditions are checked before the transaction is processed, and before any error messages are returned. By doing as much validation as possible on a given transaction, the DRM will be able to eliminate the scenario of multiple attempts to send the same transaction, with the DRM finding another error each time the transaction is submitted.

4.4.7 JAD Recommendations Related to System Requirements

The JAD and *Strategic Plan* recommendations related to general system requirements are listed on the following table. Whether or not these recommendations as presented will actually be implemented can be determined in the detailed design and development of the DRM system.

JAD Requirement Type	JAD/Strategic Plan Recommendation	Relevant DRM System Requirement Section or Sub-section
Access/1	Allow access on mobile terminals	4.3 System Requirements/System Architecture Document
Access/2	Require passwords for access to the system	4.3.1 Create and Maintain User Profiles
Access/3	Provide web access to information and authorized data entry.	4.3.1 Create and Maintain User Profiles
Security/71	Information on Grand Jury indictments must be strictly limited and not available to all users of the system.	4.3.1 Create and Maintain User Profiles
Security/72	Perform only those tasks permitted for their user profile and security level	4.3.1 Create and Maintain User Profiles
Tracking and Accountability/73	Assign missing agency numbers to records where not provided via a system interface or other automated update	4.3.3 Maintain Translation Values
Tracking and Accountability/74	Track all changes made by agencies to correct previous entries.	4.3.6 Logging and Auditing
Tracking and Accountability/79	Identify records that are not associated with fingerprints.	4.3.6 Logging and Auditing
Tracking and Accountability/80	Track record entries and changes by User IDs, so that training and performance issues can be	4.3.6 Logging and Auditing

JAD Requirement Type	JAD/Strategic Plan Recommendation	Relevant DRM System Requirement Section or Sub-section
	addressed.	
Tracking and Accountability/81	Provide tracking to minimize duplicate bookings.	4.3.6 Logging and Auditing
Tracking and Accountability/82	Track charges amended by prosecutors.	4.3.6 Logging and Auditing
Tracking and Accountability/83	Identify the agencies involved in a case so that contacts can be made if further inquiries are needed	4.3.6 Logging and Auditing
Tracking and Accountability/85	Audit the disposition reporting tracking system for edit history, status, user access, and processing history, including printing of Disposition Report form copies	4.3.6 Logging and Auditing

4.5 NON-FUNCTIONAL ISSUES

Some of the issues discussed during the JAD sessions and follow-up interviews concerned "non-functional" recommendations that participants believed should be taken into account in future DRM efforts. For example, there was some discussion during JAD sessions on the level of communications required between agencies participating in an integrated justice system and ways that the system can facilitate that communication and foster the cooperative stance each agency must practice in order to make integrated justice a reality. A few jurisdictions were concerned about the ease of use of the DRM and the amount of training that will be necessary for users of the system. These issues can be explored more fully during the development and implementation of the DRM system.

In addition, the JAD sessions resulted in several non-functional recommendations for the DRM system:

- Consider allowing all incidents to be tracked and processed in DRM; use the DRM functionality to determine which incidents are required to be moved into the ACCH.
- Maintain an on-line glossary of standardized terms to minimize confusion on the meaning and use of terms.
- Standardize processing procedures and common terms.
- Ensure "easy" interface of local systems to DRM.
- Consider interfacing with additional systems such as probation system, Motor Vehicle Department, victim notification.
- Minimize the need for duplicate data entry.

- Allow the original contributor of data to correct their own data.
- Provide training, help features, and procedures on-line.
- Consider adding other tracking needs to the project, such as outstanding warrants and arrests on warrants.
- Add notification capabilities for very specific types of information, such as changes in suspect address.
- Allow access on mobile terminals.

5 DATABASE MODEL

5.1 OVERVIEW

A critical component of the architectural representation of a system is the identification of the structures that will provide persistent data storage and support the business functionality requirements. Typically, a data model is utilized to provide graphical representation of the logical data storage requirements. When modeling a new system, all of the system requirements must be taken into consideration in order to ensure a model that supports the functionality required.

Another consideration that must be made when creating the model includes evaluating the most critical inquires that the model must support, and ensuring that the model supports these queries in the most efficient manner. In addition, the model should reflect the overall purpose of the system: to support a data warehouse and on-line transaction processing for the collection and management of disposition data.

The proposed system component for persistent data storage for the DRM is a relational database. Therefore, the data model suggested for the system includes not only a representation of the required entities but also a definition of the relationships that these entities must have with one another to support the functionality of the system. The sections that follow present a view of the proposed data model for the DRM, as well as providing narrative that describes the intent of the entities and definition of the types of attributes that should be contained within each entity.

5.2 PROPOSED DRM DATABASE MODEL

The database model that follows is a graphical representation of the entities that the DRM would contain, as well as the relationships required between those entities. It is not, however, meant to account for each attribute required within each entity. The attributes provided are intended to be a sampling of the type of attributes that would be found within each entity, and serve to help clarify the model.

In a logical data model, entities represent “things of significance” for a given system. The entities depicted in the proposed DRM data model include those significant objects that the DRM must persist and track to meet the

requirements defined in the Conceptual Design Document. Each of these entities is discussed at a high level in the sections that follow.

5.2.1 CRIMINAL HISTORY CYCLE

The criminal history cycle entity is the crux of the data model. All information that comes into or out of the DRM will be associated somehow to a criminal event or cycle. The CCID is the primary key of this table, and is assigned by the DRM for each new cycle.

5.2.2 INTERAGENCY INDEX

The Interagency Index entity represents the relationship agencies have with a Criminal Cycle. It provides a common storage place for the agency-specific numbers used to uniquely identify cycles within their systems, and as such can be used for notifications and communications between the DRM and agencies.

5.2.3 PERSON SOURCE

Each criminal history cycle is supported by at least one person-source record. The person-source record is the document or transaction that contains details about the cycle from the submitter's point of view. The person source record may be a physical fingerprint card, or it may be a complaint document, or one of a number of other documents. The important thing to note is that it is the person source record where the specific identifiers for a given source are linked to that source. All person source records must be linked to the appropriate criminal history cycle CCID.

5.2.4 PERSON SOURCE TYPES

The Person Source Types code table provides a means to identify the type of document or source of information for the person source record.

5.2.5 IDENTIFICATION

The Identification entity represents the collection of identifiers that can be associated to a person, and that normally are included with a fingerprint card submission. They include date of birth, social security number and any miscellaneous numbers. The type of identification it represents, as shown in this entity's relationship from the identification type code entity, qualifies each identification record.

5.2.6 IDENTIFICATION TYPE CODE

Identification type codes are a set of allowable values representing the types of identifications that can be stored within the identification table. Examples of identification type codes include Date of Birth or Social Security Number.

5.2.7 NAME

The Name entity represents the collection of names that can be associated to a person. This entity must include attributes for the first, last, and middle names, as well as a name suffix.

5.2.8 IDENTIFICATION PERSON SOURCE CROSS-REFERENCE

The Identification Person Source Cross-Reference entity represents the fact that many different instances of a name or identification record could be associated with different instances of a person source. For example, if a single person is arrested multiple times and gives the same date of birth for each arrest event, the distinct date of birth will be stored in the identification entity with the person source attributed to each arrest associated to that date of birth record through this entity. The ARC symbol (curved line) that passes through the relationships on this table represents that a cross-reference record can be associated to either a name record or identification record, but not to both. In other words, the relationship of the cross-reference table with identification and name is mutually exclusive.

5.2.9 CAUTION

The Caution entity captures any cautions information as provided on person source documents and specified in the NIST standards for RAP sheets.

5.2.10 SCARS MARKS TATTOOS

The Scars Marks Tattoos entity captures all scars, marks, and tattoos information submitted to the DRM in conjunction with a person source document such as a fingerprint card. One or more of these records can be created for each person source contributed to the DRM.

5.2.11 DNA SAMPLE

Participants in requirements-gathering focus group sessions expressed a desire for the DRM to include a mechanism to track the receipt and availability of DNA for criminals who have committed felonies. The DNA Sample entity represents the holding place for information identifying that a DNA sample is available. It includes relationships to both the person and the cycle that initiated the acquisition of the sample, as well as the agency responsible for taking that sample.

5.2.12 PERSON

The Person entity is the entity that contains the SID and FBI Number (when available) for a person. When a person source record of type fingerprint card is processed in the DRM, the result is that a criminal cycle is linked to the appropriate Person SID through attaching the person source record created to the appropriate person record. By attaching the SID only to the cycle for

fingerprint-supported person source records, the DRM supports the notion that a SID does not identify a cycle unless there is valid AFIS verification.

5.2.13 STATUTE CODE

The Statute code table is a collection of all Statutes that are appropriate for association to charges in the State of Arizona.

5.2.14 CHARGE

The Charge entity is the location of all distinct charges for a given criminal history cycle. The charges must be associated to an appropriate Statute Code, and to the cycle to which they pertain.

5.2.15 PROSECUTOR ACTION CODE

The Prosecutor Action Codes entity represents all possible prosecutor actions that can be initiated against a charge. Examples of prosecutor action codes include such actions as filed or declined.

5.2.16 CHARGE ACTION CROSS-REFERENCE

Several prosecutor actions may be taken against a single charge, such as first receiving the charge and then filing the charge. The Charge Action Cross-Reference entity allows for the association of charges to prosecutor actions codes, and enables the charges to be associated with more than one different action. Each association is qualified by the date of the association.

5.2.17 DISPOSITION CODE

The code-table entity for Disposition Code is a representation of the distinct types of dispositions that are available for charging decisions, such as Guilty, Not Guilty, or Deferred Dismissed.

5.2.18 DISPOSITION

The Disposition entity can be thought of as a cross-reference table between the charges and the disposition codes. It serves to link each charge to its appropriate final disposition.

5.2.19 COURT SENTENCE TYPE

The Court Sentence Type, another code-table entity, represents the distinct types of court sentences. Examples of court sentence types include such things as fined, incarcerated, work program, and no sentence imposed.

5.2.20 COURT SENTENCE

The Court Sentence entity links the charge with the appropriate sentence type, but also is the location where details about the sentence such as incarceration periods and fine amounts are stored.

5.2.21 COURT SENTENCE CONDITION CODE

Each court sentence imposed upon a person in regard to the disposition of a charge may result in one or more conditions placed upon the person in relationship to the sentence. For example, a condition may be a requirement to report to a probation officer or to remain within the State or to advise of any address changes. The Court Sentence Condition Code entity represents the collection of distinct conditions that may be utilized to qualify a sentence.

5.2.22 SENTENCE CONDITIONS CROSS-REFERENCE

Similar to the charge action cross-reference entity, the Sentence Conditions Cross-Reference entity represents the fact that a given court sentence may have more than one condition associated to it at the same time. This structure allows for the "many-to-many" association between court sentences and court sentence condition codes.

5.2.23 AGENCY

The Agency table is a representation of all distinct agencies that participate in the DRM. The agency is associated to several other entities as the owner or contributor of the data contained in the specific record.

5.2.24 AGENCY - AGENCY CROSS-REFERENCE

In order to capture typical data flow relationships between agencies, the Agency-Agency Cross Reference entity allows agencies to be associated with one another. For example, if a person is arrested by a specific law enforcement agency, this relationship may represent the usual or default prosecuting agency that will receive charges.

5.2.25 ADDRESS

The set of tables for Address will provide the storage place for not only agency addresses, but also for person addresses as reported on given person source documents.

5.2.26 AGENCY JURISDICTION CROSS REFERENCE

The Agency Jurisdiction Cross Reference table will serve to link agencies to one another through association to a jurisdiction. Associating agencies in this manner will support the notification functionality of the DRM, providing

information, for example, on the appropriate prosecuting agency for notification of receipt of a new arrest transaction by a given law enforcement agency.

5.2.27 EVENT TYPE

The Event Type code table is used to categorize each of the events that may occur within the processing of DRM transactions into specific categories.

5.2.28 EVENT

The Event entity is the location of information about every event that may occur within processing of data in the DRM that may require the communication of information with entities in the form of notifications.

5.2.29 SUBSCRIPTION

The Subscription entity is the table that allows agencies to define those DRM events for which they wish to receive notification. It also provides the means for establishment of required notifications to agencies. Each agency may subscribe to notifications for several different DRM types of events.

5.2.30 RECIPIENT

The Recipient entity can be thought of as a notification destination entity. It is within this table that the agency will record specific information regarding the delivery of notifications for each event type for which they have a subscription. More than one recipient may be listed to receive information for a given subscription, and each recipient may be configured to receive the information in a different format or via a different means.

5.2.31 RECIPIENT TYPE

The Recipient Type entity is used to classify recipients of notifications into categories, such as normal delivery recipient or escalation recipient.

5.2.32 DELIVERY FORMAT

By associating an entry from the Delivery Format table with a recipient, the agencies can specify the delivery format and mechanism for notifications that the DRM sends based on subscriptions.

5.2.33 NOTIFY

Whenever an event occurs within the DRM, the DRM will utilize the information in the subscription area of the system to determine the notifications that must be delivered. As the specific notifications are built, information pertaining to the notification is stored in the Notify entity. The

data model supports notification at a person, criminal history cycle or charge level.

5.2.34 NOTIFICATION TYPE CODE

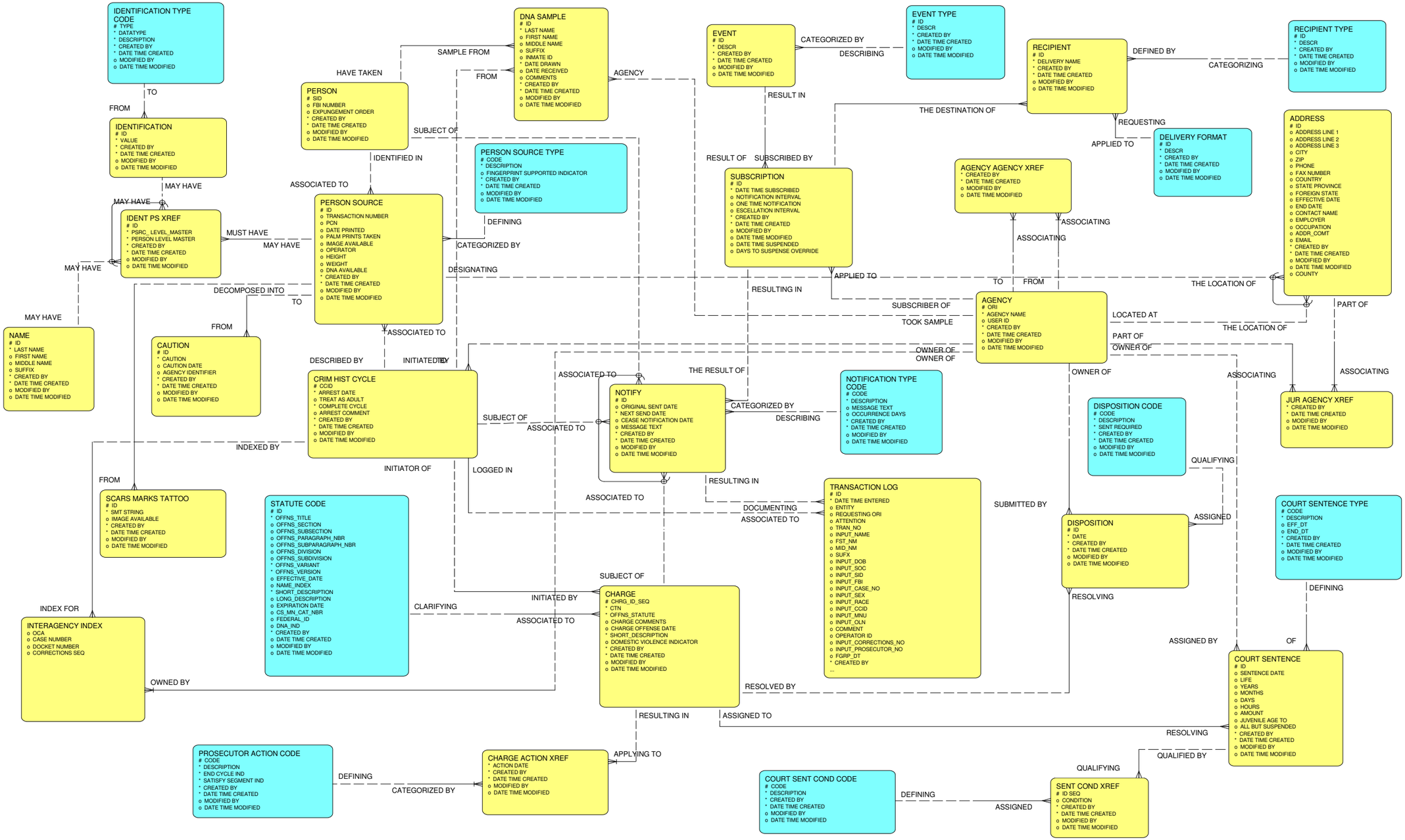
The code table for Notification Type Code is used to classify notifications into categories for reporting purposes. For example, when escalation notifications are sent, the notify record can indicate that the notification is of type escalation.

5.2.35 TRANSACTION LOG

The Transaction Log entity is the place within the DRM where all events that occur within the system are recorded. The records in this log are attached to their applicable criminal history cycles in order to provide a picture of the processing that has occurred for a given CCID over time.

5.3 ENTITY RELATIONSHIP DIAGRAM

The following diagram is a preliminary graphical representation of the proposed data model for the DRM. It illustrates the relationships between entities (the objects for which data is collected) and the interactions between entities. The Entity Relationship Diagram (ERD) is derived from the functional requirements for the DRM.


IDENTIFICATION TYPE CODE
TYPE
* DATATYPE
* DESCRIPTION
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
TO
FROM
IDENTIFICATION
ID
* VALUE
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
MAY HAVE
MAY HAVE
IDENT PS XREF
ID
* PSRC_ LEVEL_MASTER
* PERSON LEVEL MASTER
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
MUST HAVE
MAY HAVE
MAY HAVE
NAME
ID
* LAST NAME
o FIRST NAME
o MIDDLE NAME
o SUFFIX
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
DECOMPOSED INTO
TO
FROM
CAUTION
ID
* CAUTION
o CAUTION DATE
o AGENCY IDENTIFIER
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
SAMPLE FROM
FROM
DNA SAMPLE
ID
* LAST NAME
o FIRST NAME
o MIDDLE NAME
o SUFFIX
o INMATE ID
* DATE DRAWN
o DATE RECEIVED
o COMMENTS
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
AGENCY
HAVE TAKEN
PERSON
SID
o FBI NUMBER
o EXPUNGEMENT ORDER
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
SUBJECT OF
IDENTIFIED IN
ASSOCIATED TO
PERSON SOURCE TYPE
CODE
* DESCRIPTION
o FINGERPRINT SUPPORTED INDICATOR
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
DEFINING
PERSON SOURCE
ID
o TRANSACTION NUMBER
o PCN
o DATE PRINTED
o PALM PRINTS TAKEN
o IMAGE AVAILABLE
o OPERATOR
o HEIGHT
o WEIGHT
o DNA AVAILABLE
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
CATEGORIZED BY
DESIGNATING
ASSOCIATED TO
DESCRIBED BY
INITIATED BY
CRIM HIST CYCLE
CCID
* ARREST DATE
o TREAT AS ADULT
* COMPLETE CYCLE
o ARREST COMMENT
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
INDEXED BY
INITIATOR OF
LOGGED IN
EVENT
ID
* DESCR
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
CATEGORIZED BY
DESCRIBING
EVENT TYPE
ID
* DESCR
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
RESULT IN
RESULT OF
SUBSCRIBED BY
SUBSCRIPTION
ID
* DATE TIME SUBSCRIBED
o NOTIFICATION INTERVAL
o ONE TIME NOTIFICATION
o ESCELLATION INTERVAL
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
o DATE TIME SUSPENDED
o DAYS TO SUSPENSE OVERRIDE
RESULTING IN
APPLIED TO
SUBSCRIBER OF
TOOK SAMPLE
THE RESULT OF
ASSOCIATED TO
NOTIFY
ID
o ORIGINAL SENT DATE
* NEXT SEND DATE
o CEASE NOTIFICATION DATE
o MESSAGE TEXT
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
CATEGORIZED BY
DESCRIBING
NOTIFICATION TYPE CODE
CODE
* DESCRIPTION
o MESSAGE TEXT
o OCCURRENCE DAYS
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
RESULTING IN
ASSOCIATED TO
DOCUMENTING
ASSOCIATED TO
TRANSACTION LOG
ID
* DATE TIME ENTERED
o ENTITY
o REQUESTING ORI
o ATTENTION
o TRAN_NO
o INPUT_NAME
o FST_NM
o MID_NM
o SUFX
o INPUT_DOB
o INPUT_SOC
o INPUT_SID
o INPUT_FBI
o INPUT_CASE_NO
o INPUT_SEX
o INPUT_RACE
o INPUT_CCID
o INPUT_MNU
o INPUT_OLN
o COMMENT
o OPERATOR ID
o INPUT_CORRECTIONS_NO
o INPUT_PROSECUTOR_NO
o FGRP_DT
* CREATED BY
...
SUBMITTED BY
RECIPIENT
ID
* DELIVERY NAME
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
DEFINED BY
CATEGORIZING
THE DESTINATION OF
REQUESTING
APPLIED TO
RECIPIENT TYPE
ID
* DESCR
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
DELIVERY FORMAT
ID
* DESCR
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
AGENCY AGENCY XREF
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
ASSOCIATING
ASSOCIATING
ADDRESS
ID
o ADDRESS LINE 1
o ADDRESS LINE 2
o ADDRESS LINE 3
o CITY
o ZIP
o PHONE
o FAX NUMBER
o COUNTRY
o STATE PROVINCE
o FOREIGN STATE
o EFFECTIVE DATE
o END DATE
o CONTACT NAME
o EMPLOYER
o OCCUPATION
o ADDR_COMT
o EMAIL
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
o COUNTY
TO
FROM
THE LOCATION OF
PART OF
AGENCY
ORI
* AGENCY NAME
o USER ID
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
LOCATED AT
THE LOCATION OF
PART OF
OWNER OF
OWNER OF
OWNER OF
ASSOCIATING
ASSOCIATING
JUR AGENCY XREF
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
DISPOSITION CODE
CODE
* DESCRIPTION
* SENT REQUIRED
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
QUALIFYING
DISPOSITION
ID
* DATE
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
ASSIGNED
RESOLVING
COURT SENTENCE TYPE
CODE
* DESCRIPTION
o EFF_DT
o END_DT
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
DEFINING
ASSIGNED BY
OF
COURT SENTENCE
ID
o SENTENCE DATE
o LIFE
o YEARS
o MONTHS
o DAYS
o HOURS
o AMOUNT
o JUVENILE AGE TO
o ALL BUT SUSPENDED
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
QUALIFIED BY
SCARS MARKS TATTOO
ID
* SMT STRING
o IMAGE AVAILABLE
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
FROM
STATUTE CODE
ID
* OFFNS_TITLE
o OFFNS_SECTION
o OFFNS_SUBSECTION
o OFFNS_PARAGRAPH_NBR
o OFFNS_SUBPARAGRAPH_NBR
o OFFNS_DIVISION
o OFFNS_SUBDIVISION
* OFFNS_VARIANT
* OFFNS_VERSION
o EFFECTIVE_DATE
o NAME_INDEX
* SHORT_DESCRIPTION
o LONG_DESCRIPTION
o EXPIRATION DATE
o CS_MN_CAT_NBR
o FEDERAL_ID
o DNA_IND
* CREATED BY
o DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
INDEX FOR
INTERAGENCY INDEX
o OCA
o CASE NUMBER
o DOCKET NUMBER
o CORRECTIONS SEQ
OWNED BY
CLARIFYING
SUBJECT OF
INITIATED BY
ASSOCIATED TO
CHARGE
CHRG_ID_SEQ
* CTN
* OFFNS_STATUTE
o CHARGE COMMENTS
o CHARGE OFFENSE DATE
* SHORT_DESCRIPTION
o DOMESTIC VIOLENCE INDICATOR
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
RESOLVED BY
RESULTING IN
ASSIGNED TO
PROSECUTOR ACTION CODE
CODE
* DESCRIPTION
* END CYCLE IND
* SATISFY SEGMENT IND
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
DEFINING
CATEGORIZED BY
CHARGE ACTION XREF
* ACTION DATE
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
APPLYING TO
COURT SENT COND CODE
CODE
* DESCRIPTION
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED
DEFINING
ASSIGNED
QUALIFYING
SENT COND XREF
ID SEQ
o CONDITION
* CREATED BY
* DATE TIME CREATED
o MODIFIED BY
o DATE TIME MODIFIED

6 APPENDIX A: JAD MINUTES

This section contains the minutes of the Joint Application Design (JAD) sessions that were held throughout the state. Each set of minutes lists the individuals that participated and the agency they were representing.

JAD sessions were numbered as the date and location were established. JAD VI, held in Yuma, was scheduled last but was actually held two days before JAD V in Phoenix. Therefore, the JAD numbers and corresponding dates appear to be out of sequence.

7 APPENDIX B: DISPOSITION REPORTING INTEGRATION CONCEPTS WHITEPAPER

8 APPENDIX C: CURRENT DISPOSITION REPORT FORM

The following pages contain images of the current Disposition Report form in use throughout the state of Arizona.