BJA Bureau of Justice Assistance

NIJ National Institute of Justice

Standard Functional Specifications for

Law Enforcement Records Management Systems Version II

Developed by the

Law Enforcement Information Technology Standards Council

Acknowledgements

LEITSC Governance

Morris Roberson, Chair
U.S. Postal Inspection Service (retired)
National Organization of Black Law Enforcement Executives (NOBLE)

Paul Fitzgerald, Vice Chair
Sheriff
Story County (IA) Sheriff's Office
National Sheriffs' Association (NSA)

Larry Boyd
Chief of Police
Irving (TX) Police Department
Police Executive Research Forum (PERF)

Greg Browning
Chief of Police
City of Juneau (AK) Police Department
International Association of Chiefs of Police (IACP)

Heather Ruzbasan Cotter
Senior Program Manager
IACP

Joseph Akers
LEITSC Staff Liaison
NOBLE

Dr. Craig Fraser
LEITSC Staff Liaison
PERF

Fred Wilson
LEITSC Staff Liaison
NSA

Meghann Tracy
Project Support Specialist
IACP

LEITSC Functional Standards Committee

LEITSC would like to recognize the law enforcement practitioners, subject matter experts, and industry representatives who volunteered their time to update this document. Specifically:

Steve Barger
Chuck Brady
Tom Dewey
Lt. Scott Edson
Chief Michael Haslip
Steve Hoggard
J.B. Hopkins
Lt. Will Johnson
Bruce Kelling
Lt. David Mulholland
James Slater
Chief Gary Vest
Edward Waigand
Paul Wormeli

Special Recognition

This document is the result of an extraordinary collaboration between many justice practitioners and industry experts. LEITSC would like to recognize the work of Waterhole Software, Inc. for taking on the task of updating this document. In addition, LEITSC would like to identify and express thanks to the law enforcement practitioners, subject matter experts and industry representatives who volunteered their time to develop the *Standard Functional Specifications for Law Enforcement Records Management Systems, Version I,* specifically, Joe Cassa, Mitchell Ray Davis, III, Debbie Fox, Chief Michael Haslip, Linda Hill, J.B. Hopkins, Dina Jones, Bruce Kelling, Deputy Chief Daniel Murray, Beverly Muse, Morris Roberson, James Slater, G. Matthew Snyder, Mark Steigemeier, Darrell True, Chief Gary Vest, Paul Wormeli, and Jennifer Zeunik. We would also like to thank our partners at the IJIS Institue. Finally, we would like to thank the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance for their leadership and continued support of the LEITSC project. Thank you all for your commitment, time, energy, and patience.

This document was prepared with the guidance, leadership, and funding of the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, in collaboration with the Law Enforcement Information Technology Standards Council. This project was supported by Grant No. 2003-MU-BX-0068, awarded by the Bureau of Justice Assistance.

TABLE OF CONTENTS

EXECUTIVE SUMMARY: RECORDS MANAGEMENT SYSTEM

History

With support from the U.S. Department of Justice (DOJ), Office of Justice Programs (OJP), Bureau of Justice Assistance (BJA), the Law Enforcement Information Technology Standards Council (LEITSC) brings together representatives from the International Association of Chiefs of Police (IACP), National Sheriffs' Association (NSA), National Organization of Black Law Enforcement Executives (NOBLE), and Police Executive Research Forum (PERF) to address law enforcement information technology standards issues. The mission of the group is to foster the growth of strategic planning and implementation of integrated justice systems through the development and implementation of information technology standards. With guidance and leadership from BJA, LEITSC allows law enforcement practitioners to speak with a clear and consistent voice in shaping the course of crucial developments in information sharing.

Purpose

In 2003, LEITSC identified the need to develop a set of standard functional specifications for law enforcement Records Management Systems (RMS) to help guide agencies during the request for proposal (RFP) and procurement process. This document was developed with the intent of achieving the following goals:

- Provide a starting point for law enforcement agencies to use when developing RMS requests for proposals (RFP).
- Streamline the process and lower the cost of implementing and maintaining an RMS.
- Promote information sharing and best practices.

With these goals in mind, the LEITSC RMS Functional Standards Committee, composed of law enforcement practitioners and industry experts from around the country, was appointed to develop the Standard Functional Specifications for Law Enforcement RMS. The baseline document was developed from common elements found in the RFPs, technical documentation, and other RMS-related research. The document was then validated by the LEITSC RMS Functional Standards Committee using a computerized modeling tool. Once developed and validated, the specifications were vetted through the law enforcement community via each of the participating associations, as well as through other stakeholder communities, in an effort to gain input from a number of different perspectives.

In June 2006, LEITSC released the Standard Functional Specifications for Law Enforcement RMS, Version I.

Document Scope

This document presents the standard functional specifications for law enforcement RMS. The specifications found in this document are intended to be generic in nature rather than favoring one particular system or approach over another. They are at the functional level in that they define what is to be accomplished versus how it should be accomplished. These specifications were developed to depict the minimal amount of functionality that a new law enforcement RMS should contain. They are not

intended to be substituted for an RFP but should be tailored to fit the specific needs of each agency or group of agencies looking to purchase or upgrade an RMS. These specifications should be used as a starting point to build a fully functional RMS, based on agency needs and open standards, to efficiently interface and share information with other systems both internally and externally.

These specifications are intended to be used in conjunction with technical standards such as the U.S. Department of Justice's (DOJ) Global Justice eXtensible Markup Language (XML) Data Model (GJXDM) and the National Information Exchange Model (NIEM)[1] to streamline the process of sharing information.

LEITSC is responsible for updating and augmenting this document on a regular basis.

Introduction

RMS is an agency-wide system that provides for the storage, retrieval, retention, manipulation, archiving, and viewing of information, records, documents, or files pertaining to law enforcement operations.

RMS covers the entire life span of records development—from the initial generation to its completion. An effective RMS allows single entry of data while supporting multiple reporting mechanisms.

For the purposes of this document, RMS is limited to records directly related to law enforcement operations. Such records include incident and accident reports, arrests, citations, warrants, case management, field contacts, and other operations-oriented records. RMS does not address the general business functions of a law enforcement agency, such as budget, finance, payroll, purchasing, and human resources functions. However, because of operational needs, such as the maintenance of a duty roster, law enforcement personnel records and vehicle fleet maintenance records are included within an RMS.

[1] NIEM, the National Information Exchange Model, is a partnership of the U.S. Department of Justice and the Department of Homeland Security. It is designed to develop, disseminate and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information in emergency situations, as well as support the day-to-day operations of agencies throughout the nation. In 2007, NIEM was released and subsumed JXDM to become one of the many domains incorporated into NIEM. See www.niem.gov for more details.

The following business functions were addressed in Version I of the Standard Functional Specifications for Law Enforcement RMS:

1. General System Requirements
2. Master Indices
3. Calls for Service
4. Incident Reporting
5. Investigative Case Management
6. Property and Evidence Management
7. Warrant
8. Arrest
9. Booking
10. Juvenile Contact
11. Crash Reporting
12. Citation
13. Field Contact
14. Pawn
15. Civil Process
16. Protection Orders and Restraints
17. Permits and Licenses
18. Equipment and Asset Management
19. Fleet Management
20. Personnel
21. Internal Affairs
22. Analytical Support
23. RMS Reports
24. RMS System Administration
25. RMS Interfaces

Version II of the Standard Functional Specifications for Law Enforcement RMS includes all of the above functions and adds the following new features:

1. Language in the General Requirements Section on Service Oriented Architecture (SOA) and the Justice Reference Architecture (JRA), Software as a Service (SaaS), privacy and data quality

2. Change term from Traffic Accident Reporting to Crash Reporting

3. Updates to the Protection Order module

4. Discussion of the Federal Bureau of Investigation, National Data Exchange (N-DEx) exchange program

5. Discussion of the Suspicious Activity Report exchange

6. Discussion of Statutory Registrations

1 General Recommendations

The following are general best practices for an RMS:

Single entry (i.e., data is entered once and then reused by other modules as necessary)

Automatic submission of data to external organizations as defined by the agency

Use of authoritative standardized code tables

Ability to enter and query narrative(s)/text fields

Spell check and formatting capability on narrative(s)/text fields

Ability to access multiple systems from a single RMS workstation

Single database (i.e., virtual or physical)

Validation on data entry (i.e., logical edits, edit checks for all fields)

Some functional specifications need to be addressed at the agency level, such as the identification of specific external agency interfaces. These unique functions are addressed within each applicable business function. For all exchanges generated by an RMS, conformance with DOJ's NIEM standards is required.

Internal and External Databases:

An agency's RMS should provide the capabilities for users to generate inquiries to internal and external data sources—such as the National Crime Information Center (NCIC)—from within each module[2] where such inquiries fit.

In addition, a RMS should provide the user with the ability to reuse and/or import data returned from external sources to eliminate redundant data entry.

An RMS also should provide the capability to electronically transmit RMS data to external data sources, in a non-proprietary format, either automatically (i.e., based on agency rules embedded within the RMS) or upon the user's request.

The above capabilities should be based on existing resources and emerging criminal justice standards, including DOJ's GJXDM[i], NIEM[ii], and those developed by the National Institute of Standards and Technology (NIST)[iii], including the Electronic Fingerprint Transmission Specification (EFTS) and Facial Recognition Collection standards.

Service Oriented Architecture:

Service Oriented Architecture (SOA) defines a mechanism to expose business functionality and provide a particular service to an entire enterprise. For example, a web service might retrieve the subject Master Name Index (MNI) with a query based on name and date of birth from the local MNI. Any module in the RMS package can call that service and request a lookup based on the indicated parameters.

The Global Justice Reference Architecture (JRA)[iv] provides a framework that defines the most relevant aspects of a highly adaptive justice system service oriented architecture. It extends the Organization for the Advancement of Structured Information Standards (OASIS) SOA reference model by adding concepts that are particular to the justice industry. As local, state, tribal, and federal jurisdictions begin to develop their architecture for implementing information exchange, they should consider using the JRA as the basis for their own architecture. Furthermore, RMS vendors should consider the architecture in their own software development efforts to understand where their RMS solutions fit into this bigger picture and how they might expose functionality currently embedded within their RMS to facilitate

[2] A module is an independent portion of an RMS software application which provides specific functionality for a business purpose, e.g., Arrest and Booking.

implementation of a JRA-based architecture in a jurisdiction.

Software as a Service (SaaS)

Until now, most small law enforcement agencies have been limited in their ability to acquire an RMS. The smaller agency not only has difficulty funding the acquisition, installation, and training costs for computer hardware and software, but also generally cannot afford the ongoing hardware and software maintenance and inevitable upgrading that is required to sustain a production system. Furthermore, such agencies do not generally have information technology trained staff to devote to issues of system and network management. SaaS offers the ability for these smaller agencies to reap the benefits of a highly integrated RMS while minimizing up-front costs and eliminating the need for additional technical staff to maintain the system.

SaaS-enabled RMS applications remain on the servers of the RMS vendor. The local agency then connects to these servers through a secured internet connection. The service typically involves a minimal up-front setup fee and an annual subscription fee.

Privacy/Civil Liberties

Privacy deals with ownership and stewardship of Personally Identifiable Information (PII) within an electronic records system. Privacy constraints must be managed to not only limit access to authorized internal users, but also to define dissemination constraints. Key in defining the dissemination constraints is not only the ability to capture these sharing constraints, but also the ability to forward and enforce those restrictions to all other stewards of that data.

A capability to set privacy and dissemination restrictions must be available at several levels:

1. Sensitivity of the record based on levels as described below:

> *Level 1* – All data may be shared
> *Level 2* – Conditional Shared. System should provide the capability for data contributors to indicate specific elements that may be shared.
> *Level 3* – Not shared. Silent hit sends back notice to originating agency that a record exists but record is not shared.

2. Ability to apply privacy constraints at a data element level using either a rules-based engine or manual indication. For example, this rules-based dissemination engine might say "If the case involves a juvenile, then data tagged as PII is not sharable."

Additional functionality that RMS should provide to ensure privacy includes:

- The ability to restrict access to records internally based on user and user groups.
- An audit log indicating all personnel that have accessed a particular record.

A number of references exist for additional information including the Global Privacy guidelines[v], Chapter 8 of the Fusion Center Guidelines[vi] and the srfers.org site that includes useful privacy-related tools.

As new systems are implemented, it is recommended that organizations prepare a privacy impact assessment to document their local and state privacy guidelines and ensure that the system enforces these policies.

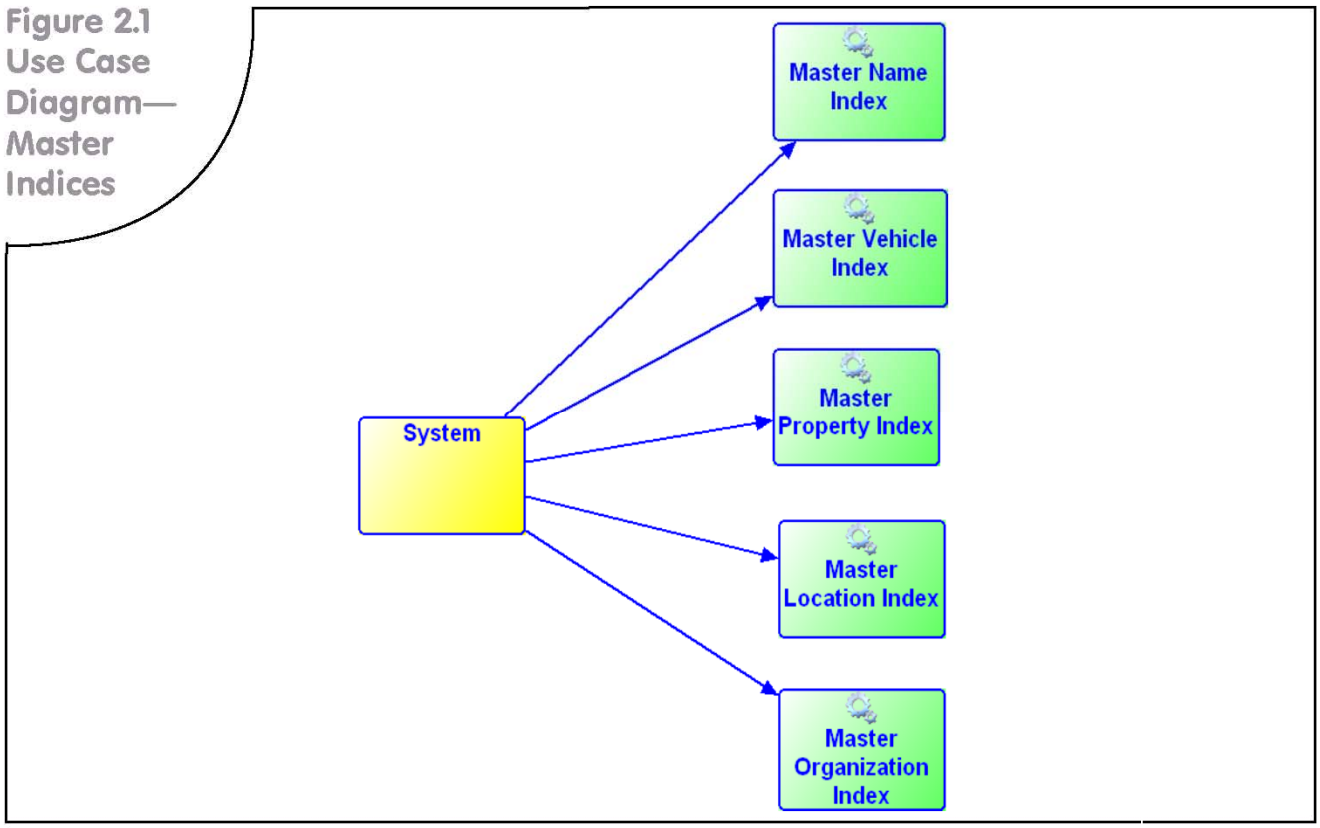
Data Quality

Ensuring data quality within an RMS becomes increasingly important as jurisdictions seek to electronically exchange data between law enforcement and other justice partners. Without strict data quality controls and reviews, inaccurate information entered in the RMS can propagate through justice agencies creating significant issues in the processing of a case. RMS should leverage NCIC standardized code lists to the maximum extent possible. Furthermore, RMS should implement some data quality validation based on context-sensitive business rules. For example, an arrest report might be required to contain an arrest identification, arrest date, and arrest subject information. An interface that allows each vendor to define these business rules should be made available to the client.

An important aspect to improving and maintaining data quality is limiting or eliminating the ability for external tools or software to directly manipulate data stored in the RMS. The RMS should implement strict controls on access to its database to help maintain this quality.

2 Business Function:
Master Indices

Figure 2.1 Use Case Diagram—Master Indices



An agency's RMS should have basic master indices that correlate and aggregate information in the following areas: people, locations, property, vehicles, and organizations (including businesses and gangs). Master indices eliminate redundant data entry by allowing the reuse of previously stored information and the automatic update of the master indices upon the entry of report information.

Master indices information are captured in a variety of ways, including during the input of information into other RMS modules such as incident reporting, crashes, citation, booking, arrest, and juvenile contact. Additionally, master index data can be imported or shared from external sources such as electronic fingerprinting devices and mug shot systems. Prior to accepting an entry, the RMS should automatically give the user the option of determining whether there is a match based on existing data. However, master indices should not allow updates from external systems.

The system should support the validation and linking of addresses, commonplace names, and street intersections.

Linkages among any information contained in the master indices (e.g., people to places or person to person) must be included in RMS.

RMS should include the ability to create an alert that monitors the master name indices, such as vehicle and property indices, and generate an alert based on records matching the specified criteria.

Additionally, an alert can be attached to a specific name, vehicle, or property record so if that record is updated in any other context, an alert is generated.

Standard Outputs:

Query and retrieval by name, vehicle, location, organization, and/or property to produce a comprehensive response displaying all related records in the system

Standard External Data Exchanges:

The master indices serve as an internal or external portal for information sharing

Mobile computing system

Regional, state, and federal information sharing systems and databases (e.g., N-DEx)

NCIC

Standard Internal Data Exchanges:

Existing RMS data

Computer aided dispatch system (CAD)

2.1 Use Case Diagram (see Figure 2.1)

2.2 Use Case: Master Name Index

The RMS Master Name Index (MNI) function links an individual master name record to every event (e.g., incident report, arrest report, field interview, accident report, license and permits) in which the individual was involved or associated. Every person identified within these events is given a master name record. Should that person become involved in another event, the single master name record is linked to all of the other events so that by querying that one name, the system can produce a synopsis of all the RMS records associated with that one person. It also facilitates the linking of additional names to an individual master name record (i.e., alias information and relationship data). In querying an individual MNI record, the user also would be able to view all related records.

When a record or report is added to the RMS, and a person is linked (i.e., indexed) to that event, the system should perform a matching function using a rules-based process defined by the agency. The purpose of this matching function is to either automatically link to an existing MNI record, or to present the user with a list of possible matches to the name so that the user can make the matching decision. The RMS should provide a matching algorithm that will provide the ability to search the name file by a variety of criteria, such as sound-alike searching, phonetic replacement, diminutive first names (e.g., James/Jim/Jimmy, Elizabeth/Beth/Betty, and Jack/John), and other static demographic information, such as age, sex, and race.

Once a list of possible matches is provided, the user can decide whether the information should be linked to an existing master name record or whether a new master name entry should be added. This step is very important in maintaining the quality and integrity of the master name file in the system. In addition to names, the MNI should, at a minimum, capture and maintain information on:

Physical characteristics (e.g., current and past descriptors)

Race and ethnicity

Location history (e.g., current and past residences)

Employer information

Telephone numbers

Known associates

Alias names/monikers

Available mug shot(s) and photographs

Scars, marks, and tattoos

Modus operandi (i.e., unique method of operation for a specific type of crime)

Identification (e.g., social security, driver's license, and local and county identification)

NCIC fingerprint classification

Over time, and depending on the circumstances, this information may change, and new information be made available. Additional information can be added, but older information should be maintained and viewable.

The RMS MNI should also provide maintenance functions that will permit a record or report to be unlinked from one MNI and re-linked to another. Since it is not always possible to ensure that the correct MNI record is linked to an event record, it must be possible to correct it. Functions also should be provided that will allow two or more MNI records to be merged into one record.

2.3 Use Case: Master Vehicle Index

Like individuals, vehicles often are directly or indirectly involved in events. When a vehicle is linked to an event in the RMS, it should be added to the vehicle record in the Master Vehicle Index (MVI), which provides an agency with a detailed, searchable store of information about vehicles.

The RMS should provide the capability to search on:

Vehicle Identification Number (VIN) or Owner Applied Number (OAN)

License plate number

License plate state

License plate year

Registered owner

Description (e.g. make, model, year, color, style, and attributes)

When an inquiry is made on a vehicle, the system should return a list of all events in which the vehicle was involved.

In addition, the RMS MVI may require external interfaces, such as the National Motor Vehicle Title Information System (NMVTIS) and other data networks.

2.4 Use Case: Master Property Index

The Master Property Index (MPI) is the central access point that links all property records entered into the RMS. Each record is catalogued by using unique property characteristics, such as make, model, brand, description, distinguishing characteristics, and serial number. Industry property coding standards, such as NCIC property codes, should be used during the entry of property records into RMS.

In addition, any property records entered throughout the RMS should automatically cross-reference the MPI to find potential matches based on the unique property characteristics outlined above.

2.5 Use Case: Master Location Index

The Master Location Index (MLI) provides a means to aggregate information throughout the RMS based on a specific address, a range of addresses, an area (i.e., as defined in the agency geofile), and/or locations based on latitude/longitude/altitude coordinates. A geofile is the location information base file for emergency 911 CAD systems. The RMS also provides a facility to store information about a specific location that may not be stored elsewhere in the RMS. The MLI should store and provide access to additional premise information, such as occupancy, elevation (e.g., floor), and premise type (e.g., residence versus business). This information should be built up as it is used and not pre-loaded.

All location information being entered in the RMS should be subject to stringent formatting rules. In addition, if the address is within the boundaries of the agency geofile, the actual location should be validated. During the geo-validation process, key identification information, such as latitude/longitude/altitude coordinates and agency-defined reporting areas, should be added to the location information.

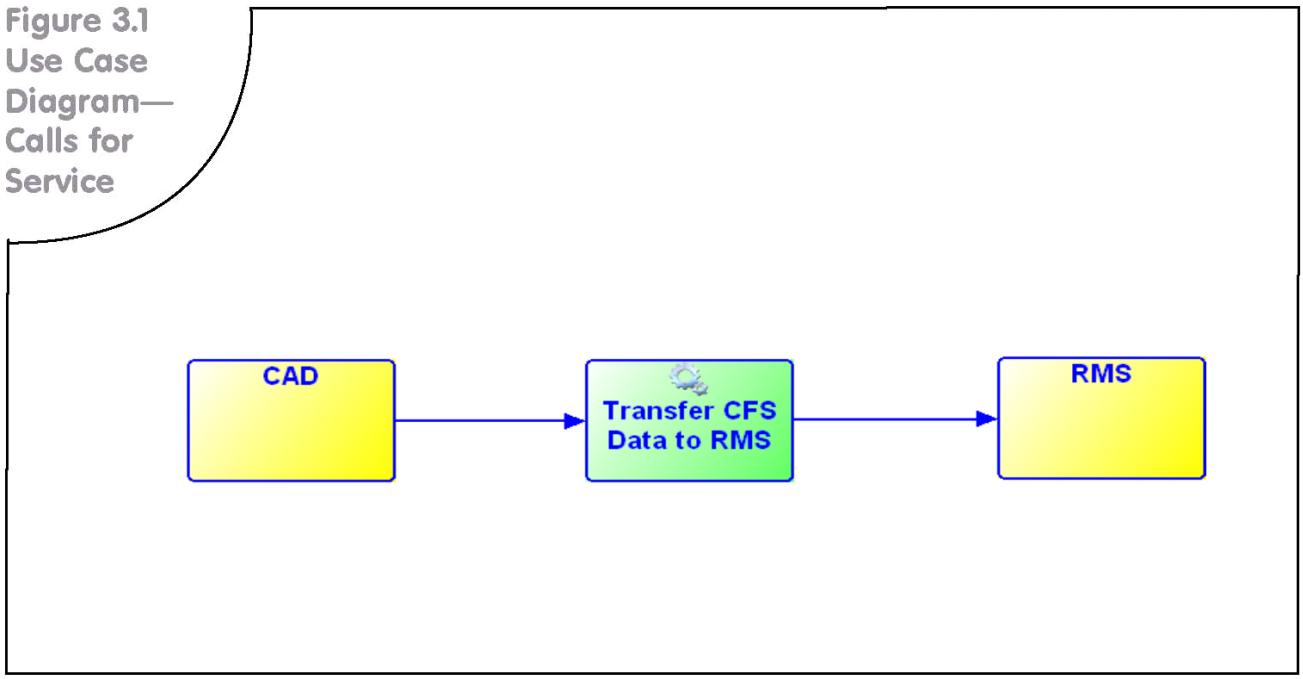
The geo-validation process should allow an address to be accepted, even if it does not appear in the geofile. Unverified addresses should be flagged for possible review. Optionally, either all addresses or only addresses within the jurisdiction are available in MLI.

2.6 Use Case: Master Organization Index

Many events also involve an organization, such as a gang, business, school, or shopping center. Information about these groups entered into the RMS should be contained in a Master Organization Index (MOI). The MOI provides an agency with a detailed, searchable store of information about organizations. An agency should be able to search on a variety of data elements and obtain a listing of all records associated with that organization. Organizations may change location and name, and these changes should be tracked in the RMS. In addition, the MOI also should permit the linking of aliases to organizations (e.g., M&M Associates, doing business as Joe's Pawn Shop).

3 Business Function: Calls for Service

Figure 3.1 Use Case Diagram—Calls for Service



All calls for service (CFS) are recorded in a structured records environment, providing the ability to run reports on these data while also maintaining a historical record on all calls. A multi-jurisdictional RMS must have the capability to associate records with a specific agency.

Typically, data in this module cannot be modified after the call is closed because they serve as a formal audit trail of the information that started the law enforcement activity. If the RMS is not integrated with a CAD system, this function must be able to serve as the initial point of data entry for a CFS. The basic call data (e.g. initial call time, units dispatched, and call disposition) can be available to facilitate the creation of an incident report. The data imported into the incident report can be modified, whether or not the call has been closed, to reflect the latest information known regarding the incident. Basic call data may be transferred at the time an incident number is assigned or at the initial closing of the call, depending on specified call types.

In the event that CFS data are transferred from a CAD system to an RMS, the RMS should receive the call number and associated incident number from the CAD system. If the call does not originate from a CAD system, this CFS module should be capable of generating, or allowing manual entry of, a sequential event number and an associated incident number to link the CFS and incident records.

If the department is dispatched by a CAD system, an interface to the CAD system will be required to transfer the CFS data to the RMS. The CAD workload[3] reports should also be available from the CFS module.

[3] Workload is the metric or metrics which accurately describe the amount of work performed by, or within, a process in a specific period of time. For example, the CFS module contains information about the number of calls received and the length of time needed to process those calls. The data on time and number of calls describes workload. A workload report in an RMS is a compilation of data that provides a user with statistics pertinent to the functions performed by, or recorded within, a module.

Standard Outputs:

Daily log showing all calls received for the prior 24 hours from prior printing of the daily log

Daily log showing all calls received for a specified data and time period

Activity analysis by specified geographical area and time period

CFS summary by specified geographical area and time period

Activity analysis by day of week

Activity analysis by hour of day

Activity analysis by day and hour

Response time analysis by specified geographical area and time period (e.g., receipt of call, dispatch time, on-scene time, and time call cleared)

Response time analysis by call type

Time consumed by call type by hour of day

Workload activity by resource assigned

Workload activity by group assigned

Time consumed by day of the week and hour of the day

Time consumed by specified geographical area and by time period

Calls that should result in the creation of an incident report

Standard External Data Exchanges:

CAD : See CAD to RMS Transfer information exchange package document (NIEM 2.0 IEPD)

Standard Internal Data Exchanges:

MNI

Incident Reporting Module

3.1 Use Case Diagram (see Figure 3.1)

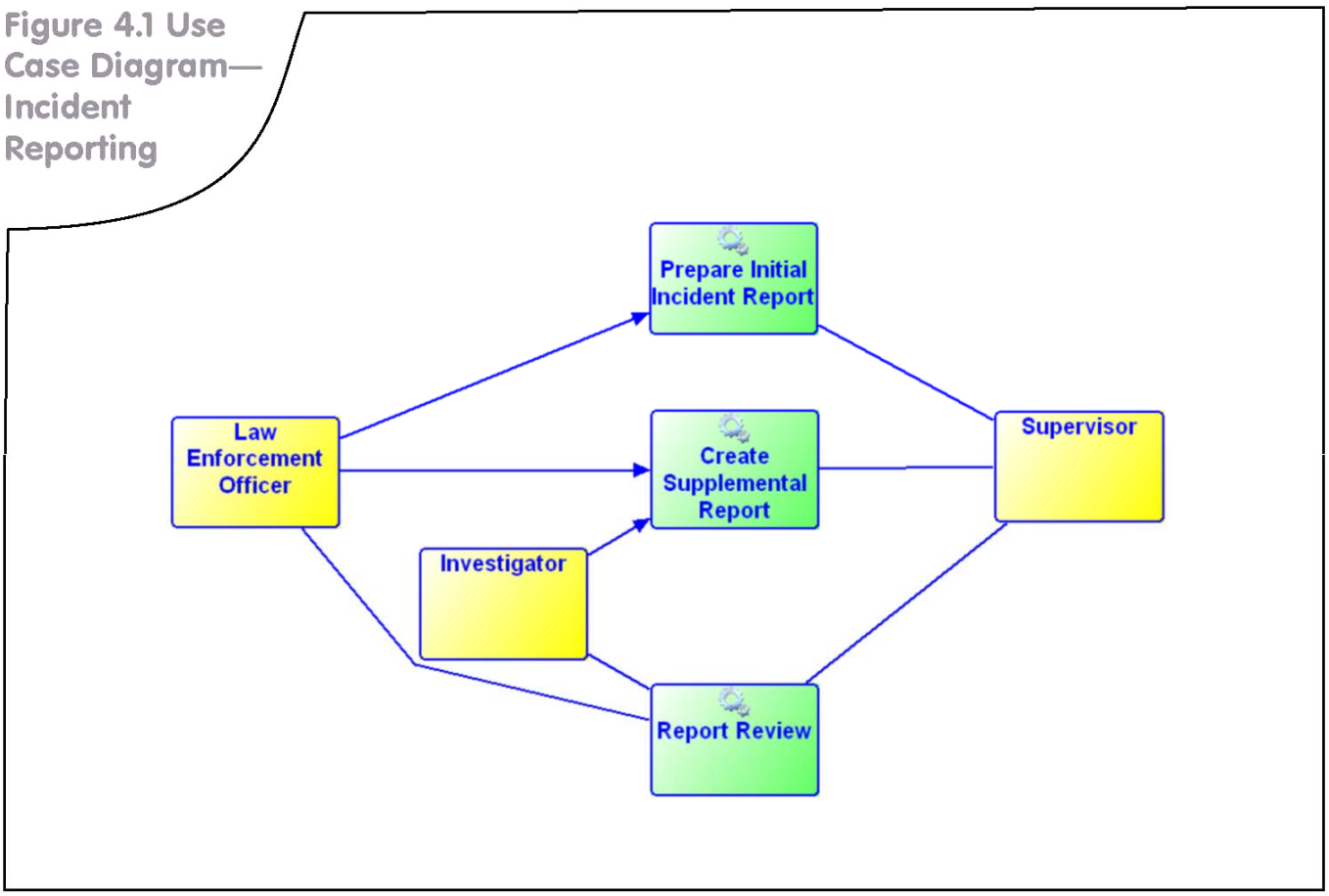
3.2 Use Case: Transfer CFS Data to the RMS

The call data are transferred to the RMS when units are initially dispatched, after an incident number is assigned, or when the call is closed in the CAD system.

.

4 Business Function: Incident Reporting

Figure 4.1 Use Case Diagram—Incident Reporting



Incident reporting is the function of capturing, processing, and storing detailed information on law enforcement-related events handled by the department, including both criminal and non-criminal events. The incident reporting function collects sufficient information to satisfy existing local, tribal, county, or state reporting requirements, as well as the reporting standards of the National Incident-Based Reporting System (NIBRS) program, the Uniform Crime Reporting (UCR) program, and the N-DEx program. Incidents often are initially documented as calls for service in a CAD system. The CFS record in the RMS should be linked to the incident and be easily accessible from the incident report.

Certain types of incident reports must be available to the public. However, items such as witness information, certain victim information, and the names of juveniles who are subjects or victims may need to be redacted for public consumption. The RMS must be able to recognize the age of majority in the jurisdiction in order to determine if certain juvenile-related data can be made available to the public. The system should support the redaction of data prior to printing a public copy or prior to making the report available online to the public.

The data captured in this module must support participation in external information sharing programs, providing the means to electronically submit data to these programs. In addition, the RMS must provide the capability to print a copy of both the full version of the incident report and a redacted version of the incident report.

Standard Outputs:

All UCR reports and NIBRS reports

Full and redacted versions of incident reports

Total incident reports based on period of time, area or beat, and incident type

Location code (e.g., geocode)

Initial call type

Offense type

Summary of incidents by responding officer

Standard External Data Exchanges:

State submission following state and NCIC standards

Prosecutor

Courts

Jail Management System (JMS)

State, regional, and national information sharing systems [e.g., Regional Information Sharing Systems (RISS), N-DEx, Information Sharing Environment (ISE)]

Amber Alert

Mobile computing system

Standard Internal Data Exchanges:

Investigative Case Management module

Property and Evidence Management module

4.1 Use Case Diagram (see Figure 4.1)

4.2 Use Case: Prepare Initial Incident Report

The incident report is prepared as soon as it is practical to do so following the incident and, depending on department procedure, may be updated throughout the initial investigation. Multiple officers may provide input to a single incident report once it is created and an incident number assigned. A primary officer will be assigned with overall responsibility for completing the report. This primary responsibility may shift to other officers during the life of the report. The incident report must contain sufficient information to comply with state and national reporting standards.

Typically, an incident report contains factual information pertaining to the incident, including offense information, suspect information, and case status, as well as information pertaining to perpetrators, witnesses, victims, and complainants. Reporting requirements typically mandate the collection of certain elements of information. In addition, incident reports have free-text fields which allow the collection of an unlimited amount of narrative information. The system should provide the capability to search the narratives for a specific word or phrase.

After completing incident reports, officers may be required to submit them to their supervisors for review.

4.3 Use Case: Create Supplemental Report

A supplemental report is used to add new information to the case after the initial incident report has been submitted and approved. The creation of a supplemental report may result from information gained during additional investigation and also may result in updating the status of the investigation and possibly bringing it to closure.

Investigators are typically the individuals within the law enforcement agency responsible for follow-up investigation and for creating supplemental reports. To that end, they must be able to query and retrieve the initial incident report and use it as a baseline document for the supplemental report. They also must be able to electronically submit the report to a supervisor for review and dissemination.

Multiple officers must be able to simultaneously create and add supplemental reports regarding the same event.

All supplemental reports are linked to the original incident report. The agency should be able to link all associated reports to a common report number. This may be done using the original incident report number, possibly with a suffix indicating the supplemental sequence, or a case number.

4.4 Use Case: Report Review

The incident report must be able to be locked to prevent further edits at a point determined by the agency. This does not prevent the viewing of the document by those with access permissions.

Supervisors are responsible for reviewing incident reports and supplemental reports for accuracy and prior to their permanent, non-editable storage in the local RMS database. The report may subsequently be distributed to the agency records bureau, to other agencies, and to local, state, and federal criminal information repositories.

The RMS must allow supervisors to receive, review, and approve incident reports online and to electronically respond to submitting officers and investigators regarding report quality and accuracy issues. The department's Standard Operating Procedures (SOPs) also may require that the records division complete an accuracy review for compliance to reporting requirements prior to adding the information to the database. The RMS should support all required reviews and corrections prior to locking down the incident report.

5 Business Function: Investigative Case Management

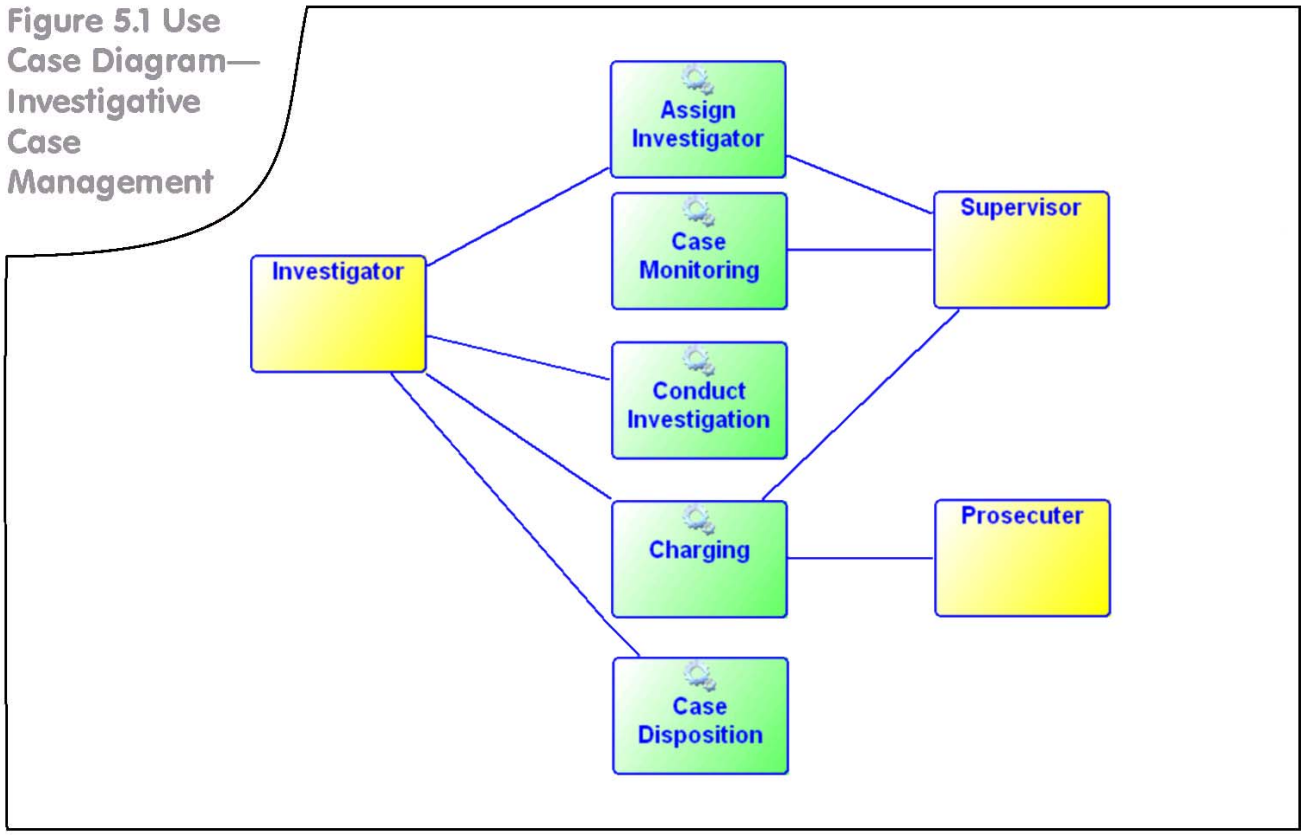


Figure 5.1 Use Case Diagram—Investigative Case Management

Incidents that require further investigation or follow-up may be referred to an investigator before they are closed or submitted to the prosecutor for a charging decision. Depending on the department's size and policies, the assignment may be made to a patrol officer, generally the officer who responded to the original incident, or the department's investigative unit. The system should be able to assign case responsibility and task responsibility.

The assigned officer receives these referrals or cases electronically and records all of the subsequent case management-related activities in the RMS. Case management functions include, but are not limited to, capturing and storing investigation data, requesting a warrant, conducting interviews and photo lineups, and producing supplemental reports. Investigators also may initiate criminal charges and obtain and execute both search and arrest warrants. The department should be able to define its specific activities, including a time allocation for each activity, so the system can generate alerts to both the assigned investigator and the supervisor.

Key products of the process are producing information for the prosecutor, assisting in managing case materials (including evidence), and preparing cases for prosecution.

Standard Outputs:

Cases not assigned for investigation or follow-up

Case summary

Case aging report (list of cases by age range, days, weeks, month, etc.)

Assigned cases (open cases by investigator and current status)

Cases pending assignment

Activity follow-up

Alerts (e.g., overdue, case assignment, and task assignment)

Pending activity (e.g., by investigator, case, and division)

Case disposition (both law enforcement dispositions and court dispositions)

Prosecutor charging documents/Application for Criminal Complaint

Standard External Data Exchanges:

Prosecutor (case submission)

Court (disposition exchanges)

State, regional, and national information sharing systems (e.g., RISSnet, N-DEx, SAR)

Jail Management System (JMS)

Standard Internal Data Exchanges:

Incident Reporting module

Property and Evidence Management module

Warrant module

Other Optional External Data Exchanges:

Financial management system

5.1 Use Case Diagram (see Figure 5.1)

5.2 Use Case: Assign Investigator

The supervisor must be able to access and review unassigned cases. The supervisor will assign case responsibility to a primary investigator. Assignment factors may include the nature of the activity, type of follow-up required, the workload of available investigators, and cases already assigned.

5.3 Use Case: Case Monitoring

Supervisors monitor cases to ensure that progress is being made. The information used in case monitoring includes case status and activities, both pending and overdue, and investigator case workload.

Supervisors must be able to obtain workload information, assess all requests for new investigations, receive deadlines and reminders, and interact with investigators electronically. They must be able to view existing assignments, shift resources, and notify investigators of changes, as required.

5.4 Use Case: Conduct Investigation

Conducting an investigation involves following up on leads and documenting additional facts about the case. The activities associated with the investigation typically include collecting evidence, developing leads, conducting interviews and interrogations, requesting warrants, and writing supplemental reports. Each of these activities must be documented in the RMS to confirm that proper department procedure was followed and that all potential leads were developed. This documentation may include case notes. Each activity during this process may result in an update of the status of the investigation.

During the course of the investigation, the primary investigator may assign tasks to others. The system should be capable of monitoring and tracking at both the case and task levels.

Several of the activities that are a part of conducting an investigation are detailed in other sections of this document. Investigators may need to create a supplemental report as defined in the Incident Reporting module. Warrants may be requested as defined in the Warrant module. Evidence collection and disposition is defined in the Property and Evidence Management module. The arrest process is detailed in the Arrest module.

5.5 Use Case: Charging

In the situation where charges are to be filed, investigators and supervisors must assemble all relevant case information and reports, as well as their charging recommendations, for submission to the prosecutor or court. The system should support the development of charging recommendations and their electronic approval prior to the submission to the prosecutor/court. In some cases, the prosecutor/court may refer the case back for further investigation.

The prosecutor/court may decide to prosecute some, all, or none of the charges recommended by the law enforcement agency or decide to prosecute other charges. The prosecutor's/court's charging decisions should be communicated to the law enforcement agency, and the system should capture the charging decisions.

In integrated justice systems, much of the communication between the prosecutor/court and the law enforcement agency happens electronically. If no interface is available, the data must be entered manually into the RMS.

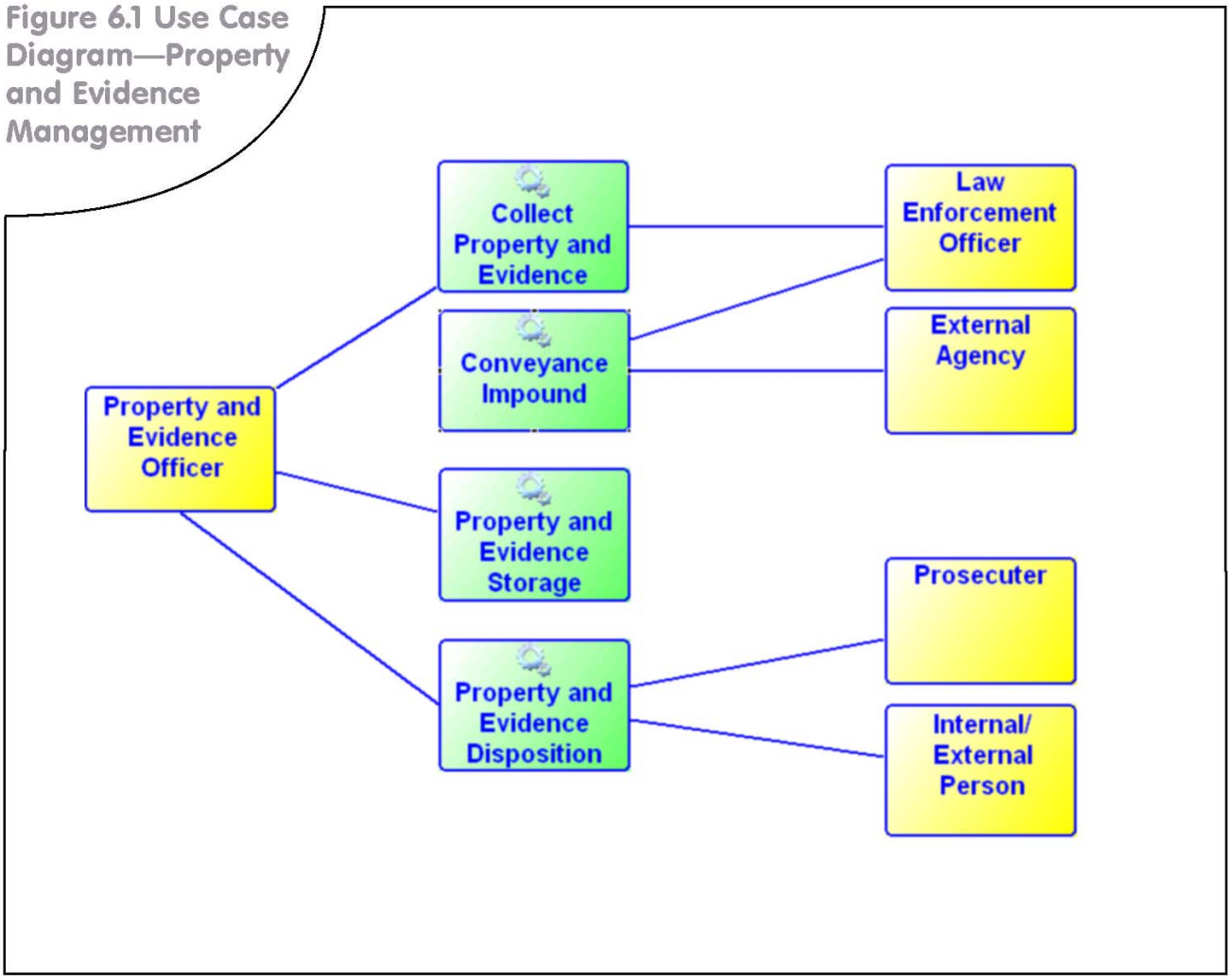
5.6 Use Case: Case Disposition

When the case is completed, a Law Enforcement Case Disposition is captured. This disposition is in addition to a case status. At this point, any property may be eligible for release to the owner as defined in the Property and Evidence Management module.

A court disposition (per person arrested and per charge) also should be included in the record as the court case is completed. Within an integrated justice system, the disposition can be exchanged electronically. The system should support the ability to reopen a case, if necessary, based on new evidence.

6 Business Function: Property and Evidence Management

Figure 6.1 Use Case Diagram—Property and Evidence Management



Property refers to any tangible item that can be owned, consumed, or otherwise used (e.g., stolen or recovered items, currency, narcotics, vehicles, animals, and evidence of any form) that is to be tracked by the agency. Property owned for use by the agency (e.g., department equipment) is typically not included in this module. Law enforcement agencies can take custody of property during the investigation of cases and preserve it for possible use at trial. Agencies also will receive property turned over by the public in which ownership is unknown or where the circumstances of receiving the property are unknown or unrelated to an event or incident.

A property custodian is responsible for receiving property for the agency. Information about the property, including its source, is collected and recorded in the RMS.

Law enforcement personnel can access property data to view detailed information about the item and historical information about the custody and control of the item, including the current status and location. Personnel also can follow links to related property items tracked in the system. The system provides the ability to accurately track all property items and verify that the evidentiary chain-of-custody requirements are met. The system also will track property that has been impounded or stored in remote facilities. Information about property and evidence must be linked to either a case file or a report that describes the circumstances under which the property was received by the department.

The disposition of property is managed by the system, with timed events to notify property custodians when property items can be released, destroyed, or sold at auction. The disposition history may be maintained for a specified time period or may be retained indefinitely for future investigative purposes.

Many jurisdictions are using stand-alone software programs to support the property and evidence function. The RMS must provide standards-based interfaces to these systems as well as the capability to import data from these external systems using standard file formats. Links to appropriate RMS records should be made at the time the property record is uploaded.

Standard Outputs:

Chain of custody

Other Optional External Data Exchanges:

Bar-code/radio-frequency identification (RFID) system

Third-party property management systems, including laboratory evidence processing systems

Pawn shops

Property summary report

Property item detail

Released property report

Property inventory report

Property disposition reports

Form letter to inform the property owner of the pending disposition of property with instructions for filing a claim

Vehicle impound forfeiture report

Case closed evidence report

Evidence location summary report

.

Audit report

Standard External Data Exchanges:

State, regional, and federal information sharing systems (e.g., RISSnet, N-DEx, ISE) based on state and national standards such as GJXDM, NIEM, and NCIC

Prosecutor

Courts

Standard Internal Data Exchanges:

Incident Reporting module

Fleet Management module

6.1 Use Case Diagram (see Figure 6.1)

6.2 Use Case: Collect Property and Evidence

Property and evidence items are collected and processed into a physical location with established process and security controls. This is the point of entry into the system where descriptors and tracking identifiers (e.g., date/time received, contributing and receiving officers, and location) are recorded for both inventory control and chain-of-custody purposes. The property will be checked against internal and external databases for matches. The RMS will link property/evidence information with the case report, if any.

6.3 Use Case: Vehicle Impound

The law enforcement agency will impound vehicles in the normal course of operations. Vehicles might include boats, cars, motorcycles, airplanes, and other items used for transportation. The system should support the entry of all identifying information for each of these vehicle types. A vehicle may be impounded as evidence in an ongoing investigation or because the driver was driving under the influence. A vehicle may also be impounded because it has been abandoned or because it was parked in a prohibited location.

The officer who initiates the impound records the reason behind the impoundment and information about the vehicle, including the VIN, description, license number, and the condition of the vehicle, as well as information about the owner and driver

The vehicle should first be checked against the MVI in the RMS and then automatically queried against both the state and federal repositories.

The officer enters his estimate of when the vehicle will be available for release and, if appropriate, includes the name of the tow company that will be moving the vehicle to the impound lot. An interface with a mobile computing system enables the information to be captured at the scene and made available at the time the vehicle arrives at the impound lot.

At the impound facility, the owner and driver information, as well as vehicle identification and description information, are validated or entered, and the specific location within the facility is added to the record. Information related to the tow-and-impound process also is captured. An initial estimate of the vehicle's value may be entered. A general inventory is conducted to document items that may potentially be removed from the vehicle, including personal items, spare tires, gas caps, batteries, weapons, etc. This module should support a quick and easy way to capture that information.

If the vehicle has evidentiary value, it will be subject to the rules for chain of custody and should be protected and tracked by the system like other tangible evidence. The RMS can treat the vehicle and most of its contents as one piece of evidence. However, if additional evidence is found during the impoundment process, it can be processed as a stand-alone piece of evidence.

6.4 Use Case: Property and Evidence Storage

Movement of property and evidence, regardless of how minor, is recorded to ensure that an accurate log of the activity is captured and that all policies and chain-of-custody rules are followed. Bar-codes and/or RFID may be applied to the property to facilitate this process. Updating the RMS during the check-in, checkout, and movement of the property will improve the accuracy of the chain-of-custody information in the system.

6.5 Use Case: Property and Evidence Disposition

Final disposition of property is essential to maintaining manageable storage capacities for the agency and for allowing certain owners to have their property returned in a timely fashion. The disposition process documents the disposition action and includes safeguards to ensure that procedures and laws governing the release, sale, or destruction of the item are followed. The system will use timed events by using system messages or providing access to lists of eligible property items to notify the property custodian when property can be lawfully disposed of.

The prosecutor's approval may be required before the disposition of property with evidentiary value can proceed. The system should provide a means to store images of the item prior to the disposition. The system may include an interface or exchange capability with the prosecutor that affords officials an efficient and accurate means to review and grant or deny approval of disposition requests sent by the law enforcement agency.

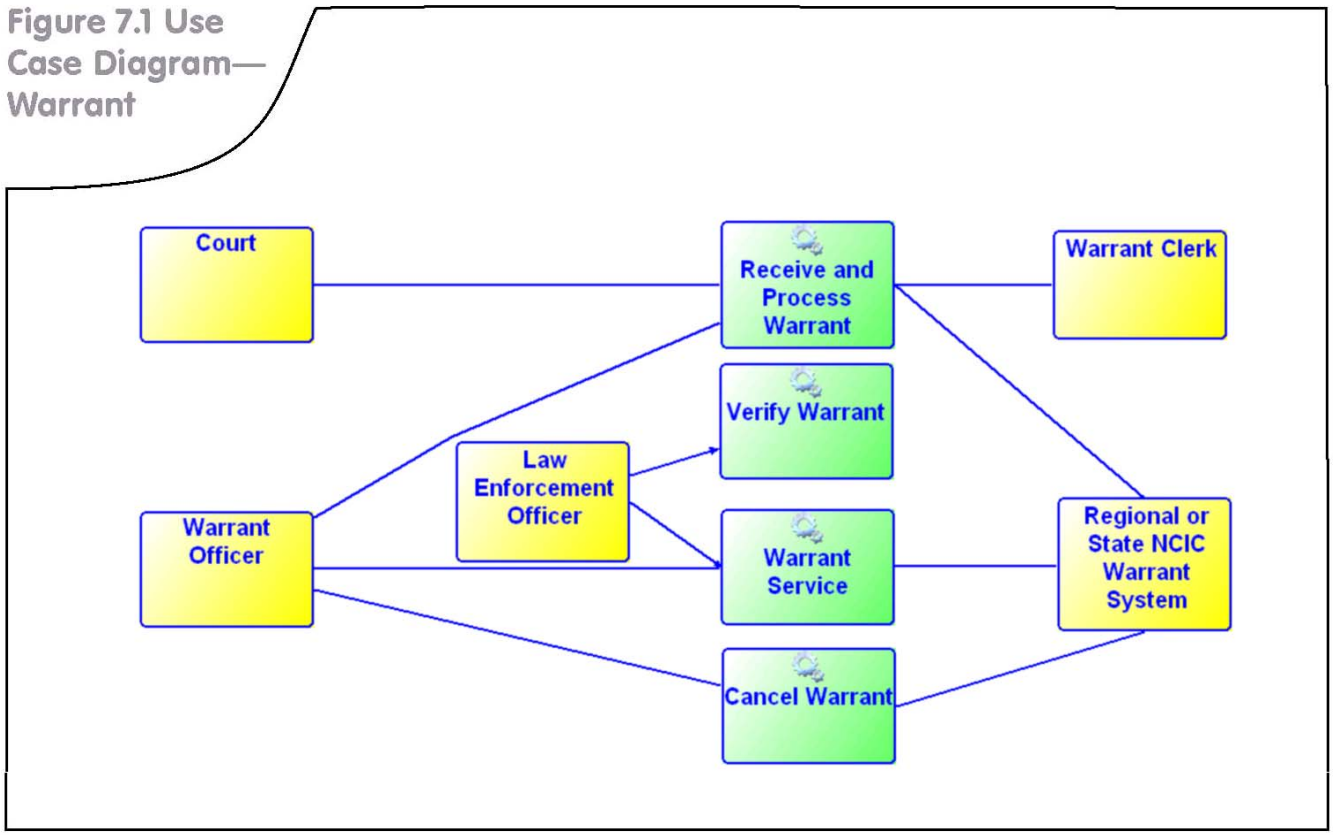
Appropriate identification is required to verify the identity of the individual claim a piece of property, and a search of information sources may be conducted where warranted. For example, if a person comes in to claim a weapon, a check of records should be conducted to ensure he or she can lawfully possess a weapon. An additional check against property databases (e.g., NCIC) should be conducted to determine if the property has been reported as being stolen. The RMS should automate these queries and document that they were completed prior to the release of property.

After a prescribed period of time, property is eligible for sale or destruction. Only lawful property can be returned to the owner or sold at public sale. Any property deemed illegal for an individual to possess will be properly destroyed.

The system should generate automatic alerts when property is eligible for release, sale, or destruction.

7 Business Function:
Warrant

Figure 7.1 Use Case Diagram—Warrant



A warrant is an order from the court that directs a law enforcement officer to take specific action, such as arresting a person and bringing them before the court. A warrant may be issued for a variety of reasons. For example, a warrant may be issued for a person charged with a crime, a person convicted of a crime who failed to appear for sentencing, a person owing a fine, or a person that the judge has ruled to be in contempt of court.

The Warrant module is designed to track warrants that the law enforcement agency will be serving and indicate the physical location of the warrant. It also tracks and records any warrant-related activity or status changes. The documentation of each activity includes the type of activity, contact with the subject (if any), the date of the activity, and the result of the activity.

In many departments, other documents (e.g., criminal summons) may be tracked and stored using the same process identified in the Warrant module.

The Warrant module should be able to create a warrant affidavit requesting that the court issue a warrant.

Standard Outputs:

Warrants issued

Warrants served or cancelled

Warrant summary based on varying search criteria

Attempts to serve by date or date range

Warrant aging report

Warrant affidavit

Complaint

Standard External Data Exchanges:

Courts

Prosecutor (for extradition determination)

Regional, state, and federal warrant repositories following NCIC standards

State, regional, and federal information sharing systems (e.g., RISSnet, N-DEx, ISE)

Jail Management System (JMS)

Corrections

Mobile computing systems

Standard Internal Data Exchanges:

Booking

MNI

MVI

MPI

7.1 Use Case Diagram (see Figure 7.1)

7.2 Use Case: Receive and Process Warrant

Upon receipt of a warrant from the court, the warrant clerk enters the information into the Warrant module. An interface with the court system will reduce data entry. Entry into the local warrant system will update the appropriate regional and/or state warrant systems. The warrant clerk reviews the warrant for completeness and ensures the subject information is up to date.

7.3 Use Case: Verify Warrant

Immediately prior to warrant service, the officer must verify that the warrant is still valid before the actual service takes place. This is especially important in serving an arrest warrant. This warrant verification process is also important in determining whether the wanting agency is willing to extradite the subject if the warrant is served.

If available, the verification can be done using a mobile data computer that has the appropriate interface. As an alternative, the officer can contact dispatch or another department facility to have the warrant verified.

7.4 Use Case: Warrant Service

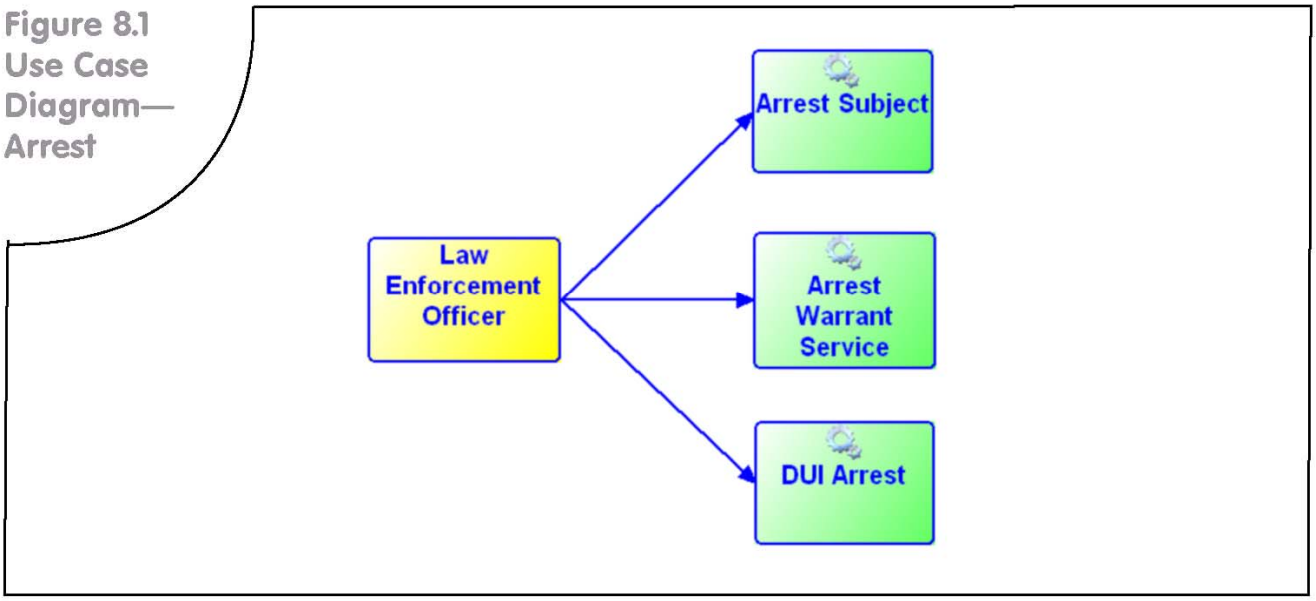
The process for warrant service will depend on the type of warrant. The Warrant module tracks and records any warrant-related activity or status changes. The documentation of each activity includes the type of activity, contact with the subject (if any), the date of the activity, and the result of the activity. Once the warrant is served, the module is updated and the warrant is cancelled in other appropriate warrant systems.

7.5 Use Case: Cancel Warrant

The court has the ability to cancel a warrant. The reason for the cancellation must be recorded in the Warrant module. Other appropriate warrant systems also must be updated to reflect that the warrant has been cancelled.

8 Business Function:
Arrest

Figure 8.1 Use Case Diagram—Arrest



Law enforcement agencies arrest subjects suspected of having committed a crime. Arrest actions must be supported by either probable cause rules or a court warrant commanding the arrest of a subject. It is essential that the arresting officer follow well-defined procedures that include accurately documenting and recording every step in the arrest process. Both scenarios follow the same procedure when the person is arrested.

The Arrest module provides a place to document all of the steps taken in an arrest. This complete documentation may be used to defend the legality of an arrest.

The data entered into the Arrest module can then be used by the Booking module, the JMS, the prosecutor, and the court.

Standard Outputs:

Daily arrests, by day and time, and date range

Arrest report and/or affidavit

Arrests by location

Arrest log

Standard External Data Exchanges:

JMS

Court

Prosecutor

State criminal history system

State, regional, and federal information sharing systems (e.g., RISSnet, N-DEx, ISE)

Mobile computing systems

Standard Internal Data Exchanges:

Incident Reporting module

Booking module

MNI

MVI

MPI

Property and Evidence Management module

8.1 Use Case Diagram (see Figure 8.1)

8.2 Use Case: Arrest Subject

When a law enforcement officer has control of a subject, the officer will take the subject into custody if the circumstances support maintaining control of the individual to maintain public safety and peace.

A probable cause or on-view arrest is based on the immediate circumstances of an incident, where sufficient evidence supports the actions of the law enforcement officer. Examples include traffic violations and incidents when the officer witnesses the commission of a crime. In some cases, the arrest may trigger the detention process and booking.

The law enforcement officer must make every reasonable effort to confirm the identity of a subject prior to the person's being taken into custody. The Arrest module must allow the officer to capture the method of identification that was used. It also must capture the completion of other steps such as the issuing of the Miranda warning.

The RMS must provide the capability to print the arrest report after all of the data have been entered into the system.

An arrest report will be required when the law enforcement officer takes the final step in the arrest process of transporting the person to jail. The RMS should facilitate and document the agency's arrest report review process.

An interface with the appropriate booking and/or JMS is desirable.

8.3 Use Case: Arrest Warrant Service

There are two situations that may trigger an arrest based on the serving of a warrant. The law enforcement officer may serve an arrest warrant that was issued as a result of an ongoing investigation. Certain charges will have been approved by the prosecutor or court prior to the warrant being issued. These charges may or may not be updated prior to the service of the warrant. The arrest now follows the same process as a probable cause arrest.

The second trigger of a warrant arrest is when a law enforcement officer conducts a warrant check during a traffic stop or some other activity and finds that there is an active warrant on file for the person involved.

Prior to the warrant service, the officer must verify that the warrant is still valid. If the warrant was issued by another jurisdiction, the law enforcement officer must first confirm that the issuing agency is willing to extradite. This warrant verification process can be done using a mobile data computer that has the appropriate interface. Some agencies do not require an arrest report to be written if the warrant was issued by another jurisdiction.

After the warrant has been served, it is necessary to remove the warrant from all of the appropriate warrant systems.

8.4 Use Case: DUI Arrest

Driving under the influence (DUI) of drugs or alcohol, or while impaired in some other way, is considered one of the most serious issues for traffic enforcement. Additional steps are required prior to the beginning of a DUI arrest.

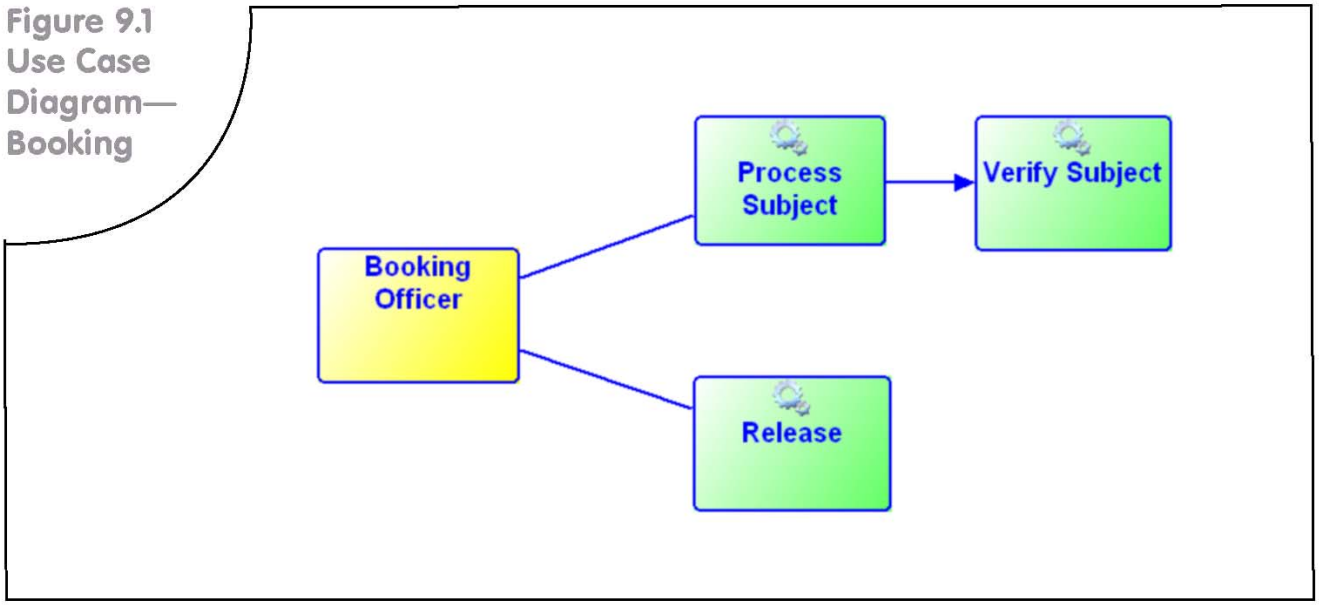
This process may be initiated as part of a traffic stop or in response to an accident. If the law enforcement officer suspects that the driver was using drugs or alcohol, a chemical test will be conducted either in the field or under more stringent controls. The law enforcement officer will ask the subject if he or she is willing to submit to a chemical test. The response should be captured in the RMS. When fatalities are involved, the law enforcement officer may be required to obtain chemical tests without the consent of the subject. All relevant information regarding the results from tests are gathered and recorded to supplement the report in the RMS.

Based on the test results, the department's SOP for handling DUI arrests will be followed, and each step will be documented in the RMS.

Evidence may be obtained from these types of incidents, which require property handling and tracking.

9 Business Function: Booking

Figure 9.1 Use Case Diagram—Booking



Booking data captured in a law enforcement RMS are ultimately linked to the arrest report. The data to be captured include the personal information of the subject.

The personal identification information provided by the subject will be checked against the MNI to create a link to this booking and avoid unnecessary or redundant data entry. Personal information includes the subject's name and any known aliases; a physical description, including tattoos and other identifying marks; address and other contact information; date of birth; and identification data, such as a driver's license number or social security number. The subject's fingerprints will be taken as part of the booking process. A photo image also will be taken of the subject and may include images of any identifying attributes, such as tattoos and scars. The RMS will provide the capability to store the images in the database linked to the booking record.

Standard Outputs:

Booking form

Booking summary, based on varying search criteria

Daily court list by court and time

Property received receipt

Property released receipt

Booking activity (e.g., intakes, releases, and transfers)

Standard External Data Exchanges:

JMS

Arrest

Regional and state warrant and criminal history repositories, following NCIC standards

State, regional, and federal information sharing systems (e.g., RISSnet, N-DEx, ISE)

Automated fingerprint identification system

Mug-shot system

Standard Internal Data Exchanges:

MNI

MVI

MPI

Property and Evidence Management module

Arrest module

9.1 Use Case Diagram (see Figure 9.1)

9.2 Use Case: Process Subject

The booking process includes collecting all relevant information on the subject and his or her arrest details, verifying the subject's identity, and addressing obvious physical and mental health needs.

This information may be obtained from the arrest report record within the RMS. If the arrest report is available in the RMS, a link should be established between the arrest report and the booking record.

If the booking record precedes the arrest record, the data from the booking record should pre-populate the arrest record. The MNI acts as the link between the arrest record and the booking record.

Information about the arrest of the subject will be entered into the Booking module.

Agency officials perform an assessment during the course of the arrest and booking processes. Generally, the assessment may follow a checklist of questions, the answers to which are captured in the RMS. Special attention is given to medical needs and security risks. In an integrated environment, this information should be forwarded to appropriate external systems, including the JMS.

Property in the possession of the subject will be inventoried and stored in a secured area while the subject is in custody. If it is determined that the property will not be released to the subject at the time of his or her release, then the property should be handled following department procedures for property and evidence management.

The subject will be assigned to an appropriate facility and bed, based on gender, assessment needs, and space availability. Temporary holding areas may be used in cases where long-term accommodations are unavailable or where the subject's assessment warrants the assignment, such as when medical needs exist or intoxication is a factor.

9.3 Use Case: Verify Subject

Personal information obtained from the subject will be used to obtain verification information from one or more sources to affirm or disaffirm the subject's identity. The personal information obtained from or about the subject will exist in many forms, including descriptive text, fingerprints, Deoxyribonucleic Acid (DNA), and photographic images. In most instances, the verification process will affirm or disaffirm the subject's identity electronically, but in some instances, a visual comparison will be necessary to make a determination. Fingerprints may be sent to an Automated Fingerprint Identification System (AFIS) and FBI Integrated Automated Fingerprint Identification System (IAFIS).

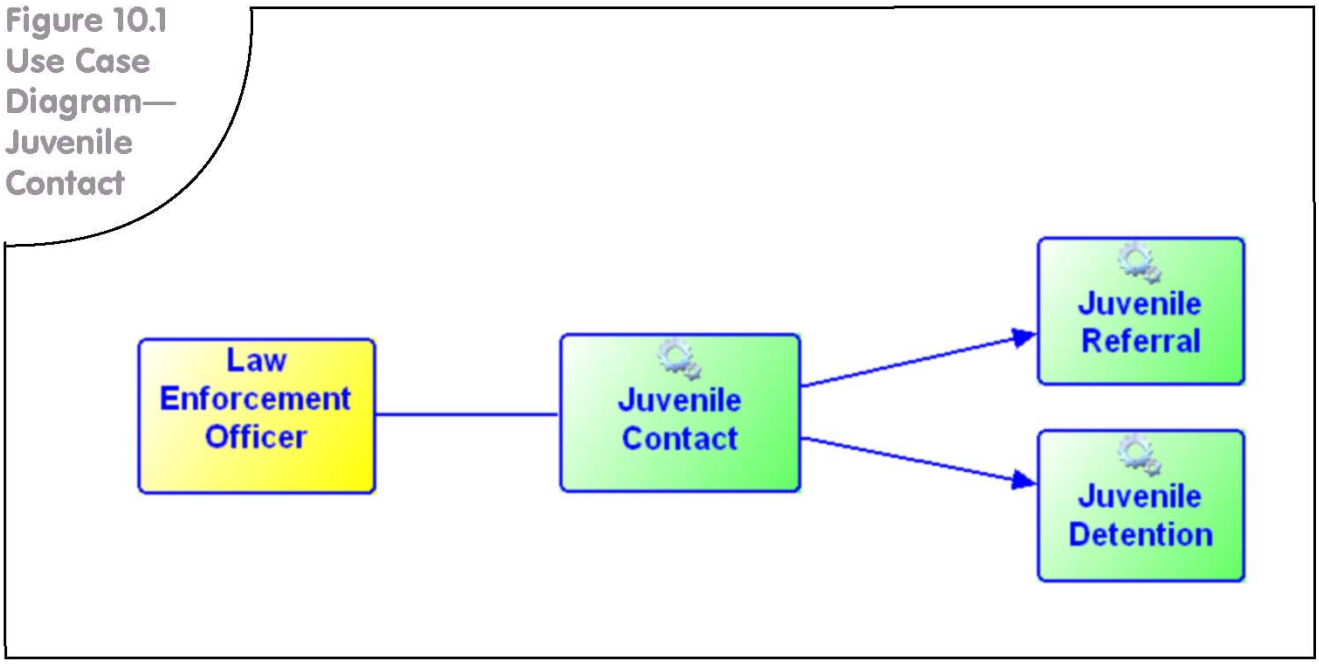
The system should check the MNI plus state, regional, and federal databases for any information. The State Identification Number (SID), FBI number, and any other information returned from AFIS/IAFIS will be added to the report as they are received.

9.4 Use Case: Release

When a subject is released from custody, bond money will be collected, if required, and a check will be made to determine if the subject has any active warrants. Prior to release, subjects may have their personal property returned to them. The booking record will be updated, where applicable, to record all relevant information supporting the release of the subject from custody, including the reason, effective date, and time of release.

10 Business Function: Juvenile Contact

Figure 10.1 Use Case Diagram—Juvenile Contact



The juvenile justice system requires special handling of information about juveniles. Paramount in this is the handling of their records, which must conform to legal requirements that specifically define privacy protections.

The RMS must accommodate the need to access juvenile data distinctly from adult information.

As with all cases, information about juveniles disseminated externally also requires information entered into the system to be expunged from the system when ordered by the court or statute as per SOP. Access must be restricted to authorized law enforcement personnel with special privileges.

In some jurisdictions, the juvenile court is actively involved in juvenile intake and assessment activities. There may be an interface between the court case management system and the RMS. Juvenile RMS modules also may provide notifications to external agencies, such as social services organizations and schools, based on certain activities involving juveniles.

The RMS should have the ability to automatically archive juvenile information when either a requisite amount of time (as governed by state law) has passed since the entry or when the subject reaches the age of majority (whichever occurs first).

Standard Outputs:

Juvenile custody

Juvenile contact report

Name listing for juveniles separate from adults, based on varying search criteria

Standard External Data Exchanges:

Prosecutor

Juvenile assessment center

Juvenile detention center

JMS

Mobile computing system

Standard Internal Data Exchanges:

MNI

MVI

Other Optional External Data Exchanges:

Social services

Court

Schools

10.1 Use Case Diagram (see Figure 10.1)

10.2 Use Case: Juvenile Contact

Contact with a juvenile should be documented in the RMS. The contact may result in a citation, referral, or detention. Taking the juvenile into custody allows the law enforcement officer to have the juvenile assessed and to ensure the juvenile is not in danger. The law enforcement officer will gather information from the juvenile about the incident to determine whether an offense (or status offense) occurred and whether to sanction the juvenile in any way.

In some jurisdictions, the law enforcement officer taking the juvenile into custody will take them to a juvenile intake center for an assessment. In other cases, qualified personnel at the law enforcement agency will make the assessment. Once the law enforcement officer has determined that the circumstances merit a more serious response than admonishment, they will determine the appropriate recourse or referral. This evaluation is based on a number of factors such as the nature of the incident, whether weapons were involved or narcotics were present, and the number of past contacts with law enforcement and victims. In many jurisdictions, referral to juvenile intake is mandated if the juvenile has a pattern of delinquency over a period of time as defined by law.

The juvenile may be released to a parent or guardian, a hospital, or other non-judicial authority. Informal diversion might include requiring the juvenile to perform specific community service. The RMS has a mechanism that allows for timed alert notices if follow-up contact or information is necessary.

The RMS will support these activities by documenting the contact with the youth in a juvenile contact record. It also will guide the law enforcement officer to the appropriate remedy, sanction, or referral, depending on the circumstances.

In handling a juvenile contact, law enforcement officers must communicate with both the professionals conducting the assessment and the juvenile's parents or guardian. The RMS must document these contacts as well as other information about the juvenile. The youth's full name, age, address, contact (i.e., family) information, physical description, sex, and name of the school they attend, as well as information about the incident are examples of information that may be entered into RMS.

The RMS should have the ability to automatically archive juvenile contacts after a requisite period of time (as governed by state law) has passed since the entry or when the subject has reached the age of majority (whichever occurs first).

10.3 Use Case: Juvenile Detention

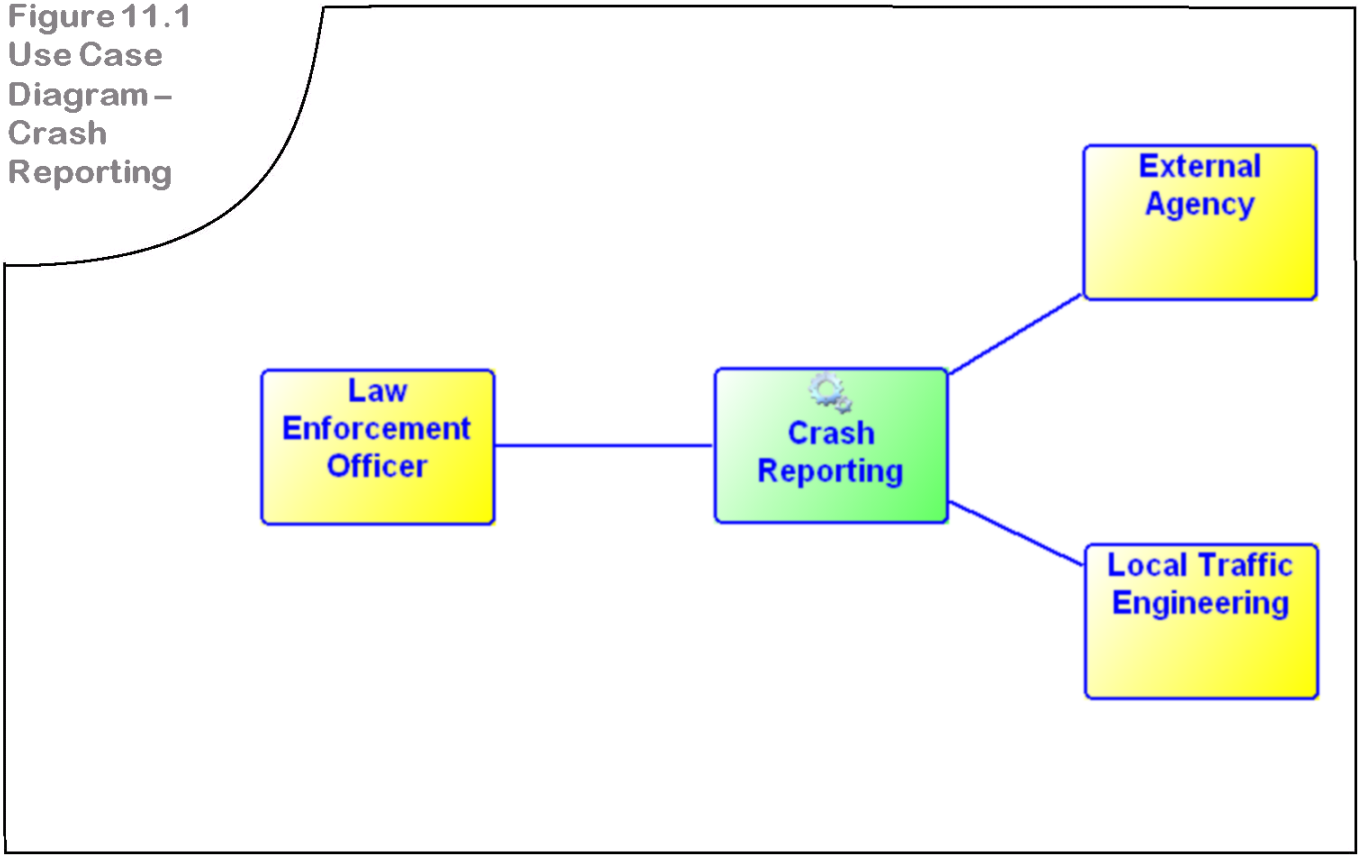
The juvenile is placed into the care of a custodial facility. The RMS must send appropriate notifications to the court, the prosecutor, and all appropriate social services agencies involved.

10.4 Use Case: Juvenile Referral

Formal charges may be brought against the juvenile. The juvenile may be released to a parent or guardian, a hospital, or other non-judicial authority. Informal diversion may include assigning required community services. The RMS has a mechanism that allows for timed alert notices if follow-up contact or information is necessary.

11 Business Function: Crash Reporting

Figure 11.1 Use Case Diagram – Crash Reporting



Crash reporting involves the documentation of facts surrounding an accident. Typically, these are incidents that involve one or more motor vehicles but also may include pedestrians, cyclists, animals, or other objects. Crash reporting also may be referred to by the terms "collision" or "traffic accident."

Most states require law enforcement to provide uniform documentation and reporting on all crashes. The information compiled in crash reports is used by the public, insurance companies, traffic analysts, and prosecutors. The accident data can also assist in identifying necessary road improvements and the elimination of traffic safety hazards.

Typically, Crash reporting is a module within the agency RMS. The information is typically captured at the location of the incident, transcribed into electronic forms (e.g., in the field or office), transferred to and used by the RMS for local analysis, and, in many jurisdictions, transmitted to the state transportation department. In some jurisdictions, crash reporting is performed using a separate software system which may be provided by the state transportation agency.

The module also should allow the officer to collect data on the demographics of the people involved for statistical reporting in bias-based policing programs.

Standard Outputs:

State crash report

Crashes by location

Crashes by time of day and day of week

Crashes by violation

Crashes by severity

Crashes by driver demographic

Statistical summary by intersection

Statistics by area (e.g., beat, precinct), day, and time

Standard External Data Exchanges:

State motor vehicle division

Local, regional, and state transportation departments, using U.S. Department of Transportation (DOT) standards

Traffic engineering using DOT standards

Community development

Mobile computing system

State, regional, and federal information sharing systems (e.g., RISSnet, N-DEx, ISE)

Standard Internal Data Exchanges:

Citation module

MNI

MVI

MPI

Arrest module

Booking module

Property and Evidence Management module

Fleet Management module

11.1 Use Case Diagram (see Figure 11.1)

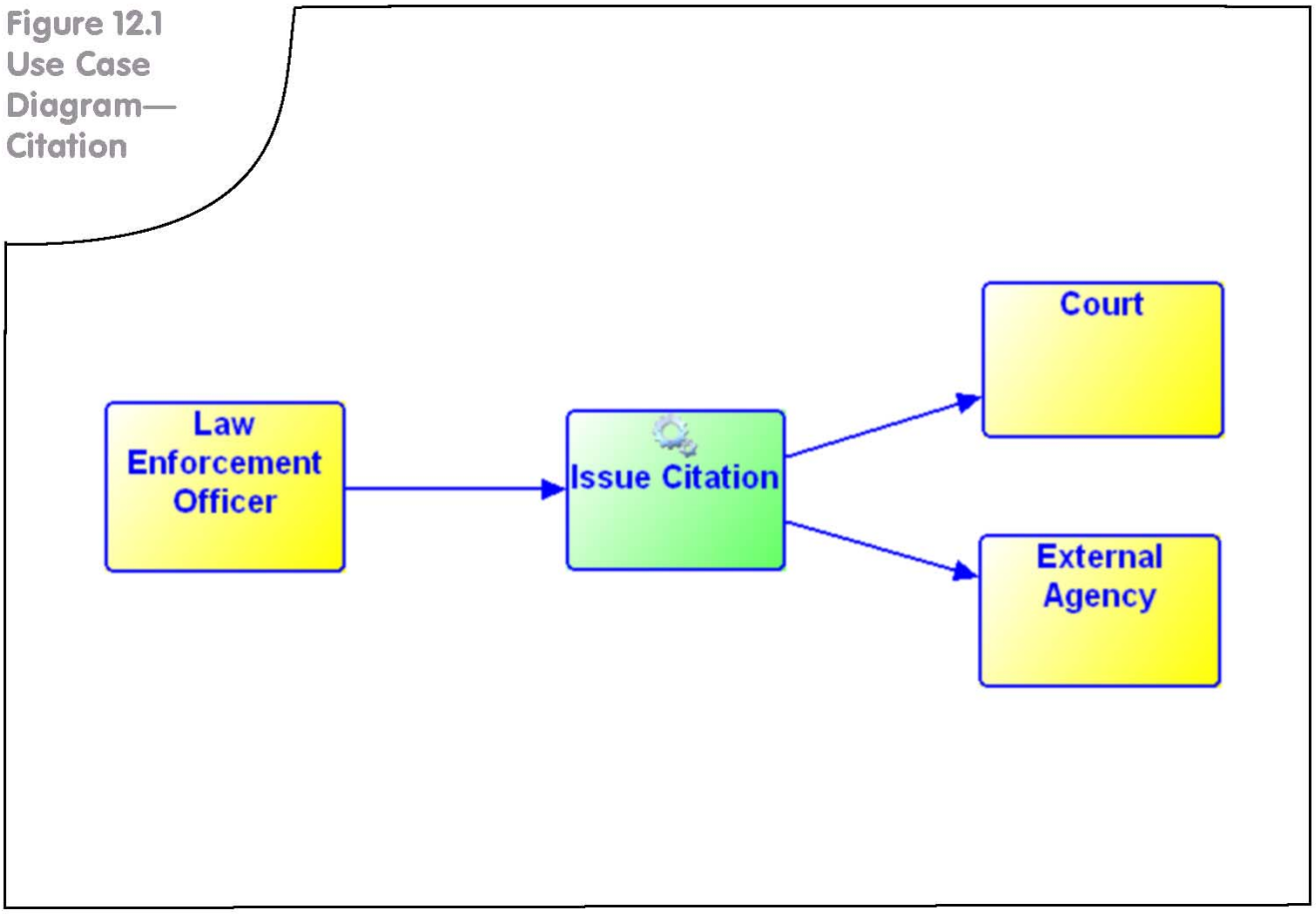
11.2 Use Case: Crash Reporting

Crash reporting requirements differ from general criminal incident reports in that they emphasize the cause of the crash, weather conditions, visibility, road surface conditions at the time of the crash, and location information. Therefore, crash reporting systems usually include drawing or diagramming tools to assist in accurately capturing crash scene and location information.

The system should support the ability to attach diagrams and photographs to the crash report. If a citation is issued as a result of the crash, the citation should be linked to the crash report.

12 Business Function: Citation

Figure 12.1 Use Case Diagram—Citation



Individuals or organizations charged with minor offenses often are issued a citation or ticket, which requires them to pay a fine, post a bail amount, and/or appear in court on a specified date. Citations are commonly used in traffic and misdemeanor law enforcement.

The offender is given a copy of the citation that may contain a pre-assigned court appearance date. When the citation data are entered or uploaded into the RMS, the appropriate links should be made to the master index records. The court clerk is notified of the charges, either by receiving a paper copy of the citation or an electronic copy of the citation data. Often, the offender can pay a fine or forfeit a bail amount to satisfy the fine. In the event that the court date is not assigned when the citation is issued, it is assigned at a later date. The Citation module should capture court data such as case number and date and record the court's disposition of the citation.

In many jurisdictions, a uniform citation form is used by all law enforcement agencies. The software that supports the creation of the citation may be a module of the RMS or a third-party solution designed for the creation of citations in the field.

If the subject is not issued a citation from a citation book, the application must be able to print the citation.

Standard Outputs:

Citation and warnings summary based on varying search criteria

Citation by location

Citations and warnings by demographic data

Citation audit (e.g., missing/voided numbers)

Citations and warnings

Standard External Data Exchanges:

Courts

JMS

Warrant module

Prosecutor

Department of Motor Vehicles (DMV)

State, regional, and federal information sharing systems (e.g., RISSnet, N-DEx, ISE)

Mobile computing system

Standard Internal Data Exchanges:

Crash Reporting module

Incident Reporting module (e.g., misdemeanor citations)

MNI

MVI

MPI

Arrest module

Booking module

Juvenile Contact module

12.1 Use Case Diagram (see Figure 12.1)

12.2 Use Case: Issue Citation

Citation information is stored and tracked in the RMS. Officers will document information about the violation(s) or charge(s), as well as relevant court information. The citation information will then be sent to the court, either electronically, if the appropriate interface is in place, or manually.

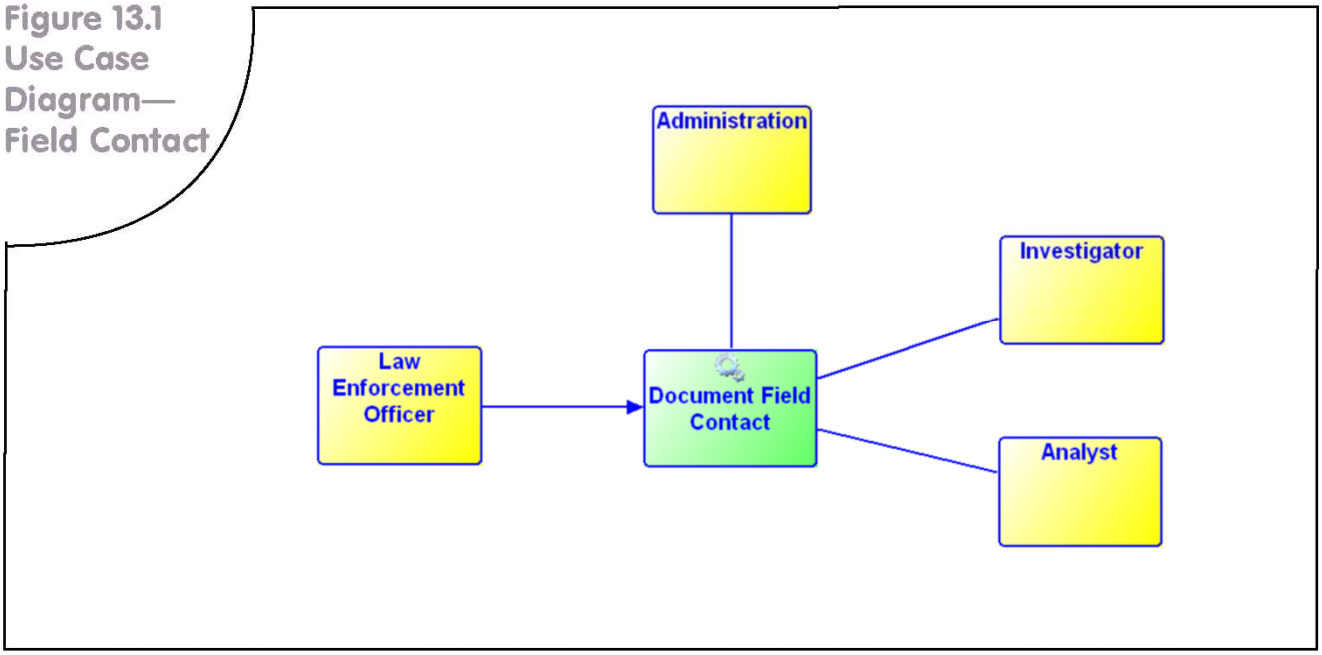
The officer issuing the citation needs to query state and local databases that contain information regarding previously issued citations and warnings. The query also should check for any outstanding warrants or alerts.

A law enforcement officer may decide to issue a warning instead of a citation. The RMS must track warnings as well as citations. Both must be linked to the subject's master name record.

The module also should allow the law enforcement officer to collect data on the demographics of the people involved for statistical reporting in bias-based policing programs.

13 Business Function: Field Contact

Figure 13.1 Use Case Diagram—Field Contact



A field contact record is created by a law enforcement officer based on the department's SOP. Typically, this process is triggered by unusual or suspicious circumstances or any activity that is considered by the law enforcement officer to be of interest but would not otherwise be documented in the RMS (see the Incident Reporting module for more details). The data in the Field Contact module are available for analytical support (crime analysis). It also can be searched by investigators to develop leads.

Field contacts are not subject to the same stringent review and approval process as incident reports.

The module should allow the officer to collect data on the demographics of the people involved for statistical reporting in bias-based policing programs.

The module should allow the system to automatically transmit information based on the Suspicious Activity Reporting (SAR) standard to the ISE. See section 25.6.

Standard Outputs:

Field contact summary, based on varying search criteria

Standard External Data Exchanges:

State, regional, and national information sharing systems (e.g., RISSnet, N-DEx, ISE)

Mug shot repository

Electronic Fingerprinting Device

Mobile computing system

Standard Internal Data Exchanges:

MNI

MPI

MVI

Arrest module

Booking module

Warrant module

Case Management module

13.1 Use Case Diagram (see Figure 13.1)

13.2 Use Case: Document Field Contact

A field contact is documented, usually at the discretion of the law enforcement officer, based on an observation or information indicating suspicious or unusual activity or circumstances, such as the following:

A parked car in an area and at a time normally vacant of cars

One or more people in an area and at a time normally vacant of people

One or more people loitering in a vulnerable area

People and vehicles that appear to be out of place for any particular reason

Specific areas may be targeted for field contact based on departmental policy. Such targeting may be for high-crime areas or in potentially sensitive areas, such as areas near schools and religious institutions.

The information collected includes:

Location and time

General circumstances

Names and descriptions of persons

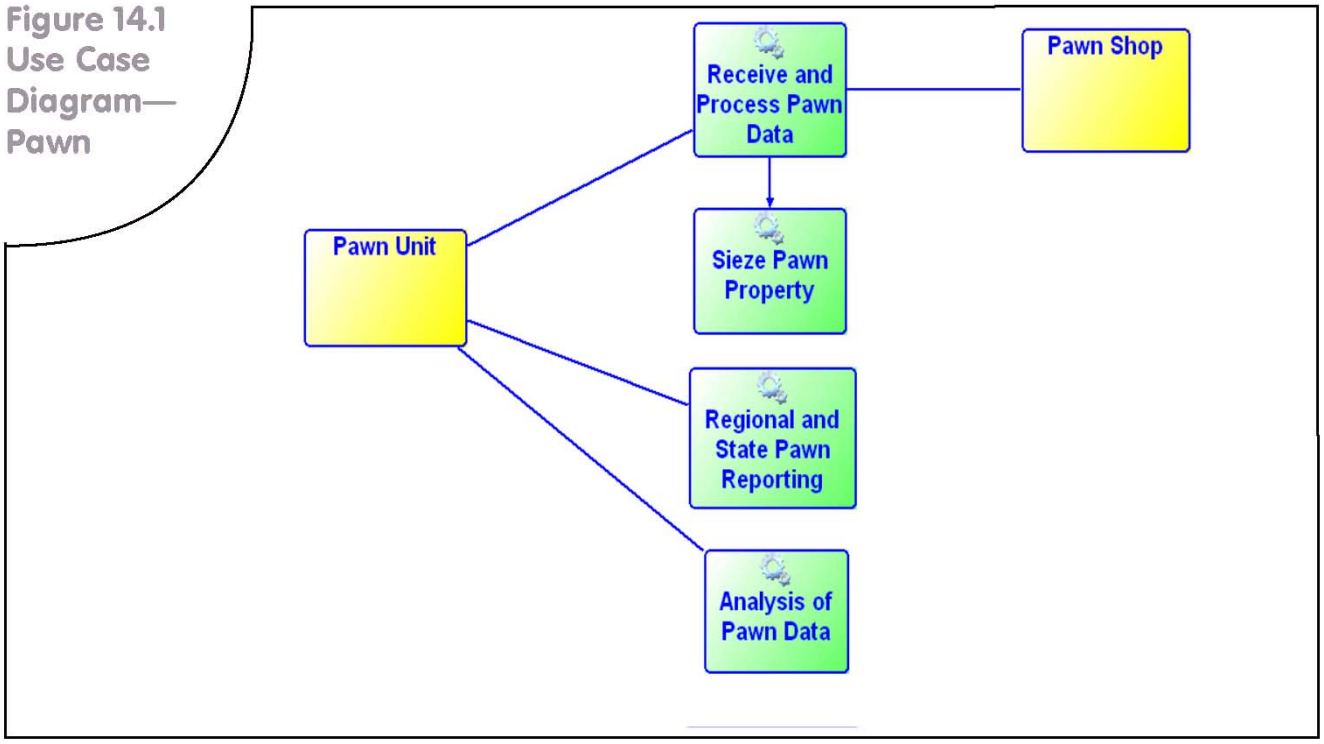
Identifying information on vehicles or other property

Field contact information serves as a key input to analytical support (crime analysis) and other investigative processes. It helps to establish links between persons, vehicles, and crime events. Because of this, field contact information should be consistent with data standards used in the analytical support/crime analysis process.

Field contact reports, unlike incident reports, are normally not subject to a stringent supervisor review and approval process. They are, however, reviewed to ensure the quality and adequacy of reporting and consistency with departmental policy and statute.

14 Business Function: Pawn

Figure 14.1 Use Case Diagram—Pawn



Pawn modules in RMS help law enforcement representatives identify and recover personal property that has been reported stolen. Many jurisdictions require pawnshops to register the items they receive and sell to facilitate this tracking process.

Specific functionality of the Pawn module includes:

Collecting, storing, and tracking pawn data

Comparing pawn data with lost or stolen property

Supporting the investigative process for matches or patterns

Running inquiries to external regional, state, and federal systems

Providing data necessary to serve the needs of state pawn systems

Standard Outputs:

Pawn summary based on varying search criteria (e.g., date, time of sale, and property type)

Frequent pawner list

Standard External Data Exchanges:

State and regional pawn systems following NCIC property standards

State and national stolen property files

Local pawnshop computer systems following NCIC property standards

Standard Internal Data Exchanges:

Permits and Licenses module

MPI

Property and Evidence Management module

14.1 Use Case Diagram (see Figure 14.1)

14.2 Use Case: Receive and Process Pawn Data

The pawn shop must submit pawn tickets to the law enforcement agency—either electronically or by paper. This information is then entered into the Pawn module. In the event the property record has a unique identifier such as a serial number, inquiries may be made to local and external systems. In addition, the name of the person pawning the item and personal identifying information (e.g., driver's license number) should be included. Depending on the type of property being pawned, name inquiries may be made to state and national systems.

As new items are added to the stolen property database, the pawn database should be automatically queried to determine if the item was previously reported as being pawned.

Any positive hits that return from these external inquiries require follow-up on the part of the pawn unit. This follow-up could include seizing property or further investigation.

14.3 Use Case: Seize Pawn Property

When the pawn unit has identified pawned property that was reported stolen, the pawn record is updated to reflect that the article had been reported stolen and then seized. The pawn unit will take action to seize the property for evidentiary or safekeeping purposes. The property is then checked into the RMS using the Property and Evidence Management module and, at this point, becomes part of an investigation.

14.4 Use Case: Analysis of Pawn Data

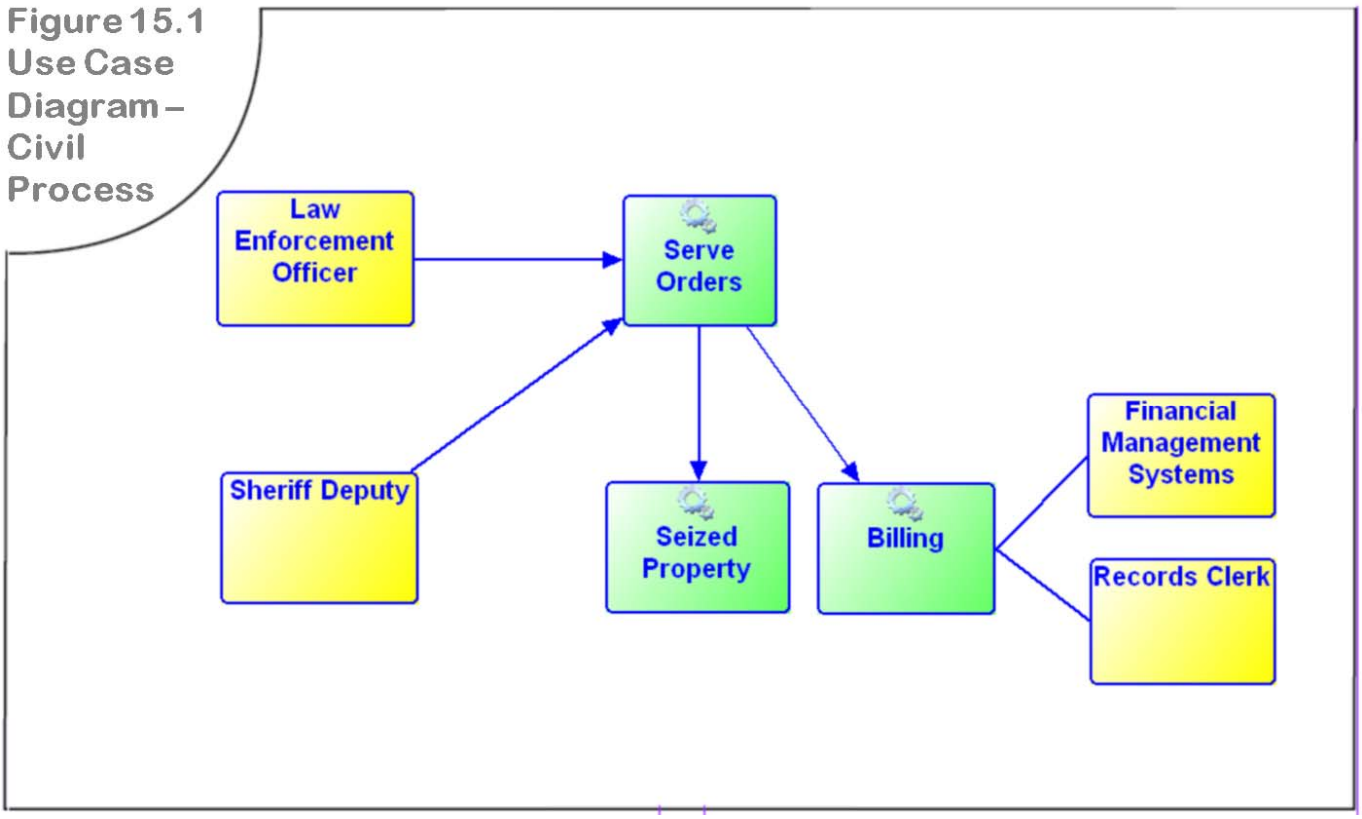
The Pawn module will analyze pawn data versus stolen data to identify trends and patterns. Examples of analysis include frequent pawn activity by location, person, type, etc. The module must create reports to support the analysis.

14.5 Use Case: Regional and State Pawn Reporting

If an external repository maintains pawn data, information from local Pawn modules may be transmitted to these systems electronically.

15 Business Function: Civil Process

Figure 15.1 Use Case Diagram – Civil Process



Civil process describes the law enforcement agency responsibility to serve legal papers and execute legal processes as required to facilitate due process through the judicial system. These functions are commonly performed by the county sheriff and may be entitled to compensation by private parties for such service. RMS modules should allow the data entry of civil papers to be served, and allow tracking, of those papers. There may be a data exchange with a billing or accounting system.

The agency may be required by statute to serve these court documents as prescribed and within specified time limits. These documents may include writs, summonses, subpoenas, warrants, judgment orders, and civil protection orders. The RMS will provide the ability to record the disposition of all actions required by the order, including court-ordered eviction, the seizure of property, and collection of court-ordered fees.

Standard Outputs:

Active civil papers (e.g., by age, jurisdiction, and server)

Served/returned civil papers

Civil paper/civil paper jacket

Expired civil papers

Notice generation

Letter generation

General financial

Civil summary (e.g., paper summary, assignments, and attempts to serve)

Affidavit of service

Standard External Data Exchanges:

Accounting system

Court

Jail Management System (JMS)

Standard Internal Data Exchanges:

MNI

MVI

MLI

MPI

MOI

Warrant module

15.1 Use Case Diagram (see Figure 15.1)

15.2 Use Case: Serve Orders

The service of orders to individuals or organizations is based on court orders or subpoenas. Service of orders also includes evictions. There will be a good faith effort to serve the order as many times as necessary up to the expiration date. The service attempts and circumstances will be documented. The system should generate an affidavit of service to the court on successful service or expiration of the order.

15.3 Use Case: Seized Property

Seized property describes the process and action of seizing personal property, based on a court order presented to a law enforcement officer. The individual or organization is served the order to voluntarily relinquish the property. On failure to relinquish property on a designated date, a property seizure will be scheduled and executed. All service attempts, as well as the order execution, will be documented in the RMS.

15.4 Use Case: Billing

An agency's RMS should collect the information pertaining to any fees associated with an order service and should transfer billing data to the financial system for billing, collection, and distribution of funds. Billing information includes whom and when to invoice, billing amounts, and the allocation and disbursement of fees.

16 Business Function: Protection Orders and Restraints

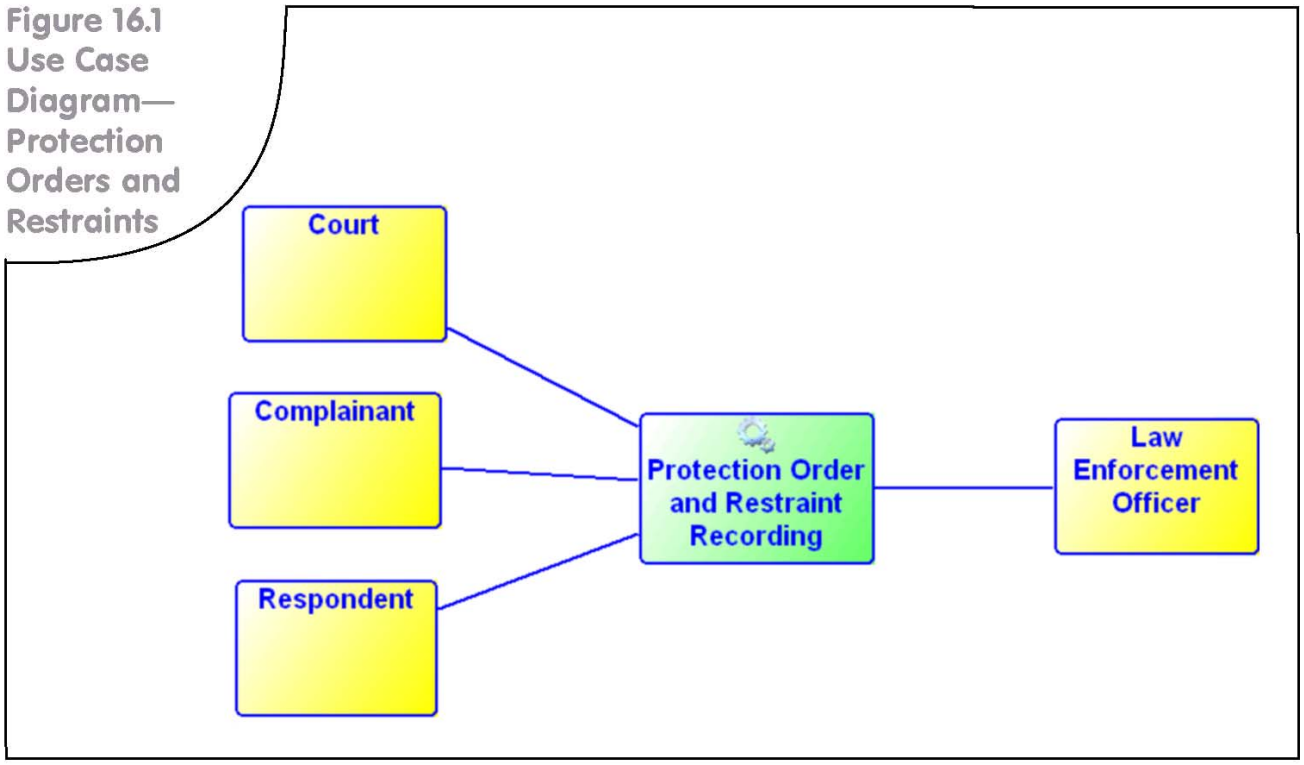


Figure 16.1 Use Case Diagram—Protection Orders and Restraints

Law enforcement agencies receive court orders for protection directly from the court or the protected party. This module is used to record protection orders and restraints, including anti-harassment orders and no-contact orders. All parties named in the orders and their relationship to the order must be stored in the system. The conditions of the order are stored as well. The conditions should include information such as the issuing authority, effective time period, location, distance, restrictions, and type of contact prohibited. This information must be readily available by name and location of the parties and also may be cross-referenced by vehicle.

Standard Outputs:

Expired/soon-to-expire orders

Active orders

Orders that have been served

Orders received, by source

Cancelled orders

No trespass orders

Standard External Data Exchanges:

CAD

Court

State, regional, and National Protection Order Registry

JMS

Standard Internal Data Exchanges:

MNI

MLI

MVI

MOI

MPI

16.1 Use Case Diagram (see Figure 16.1)

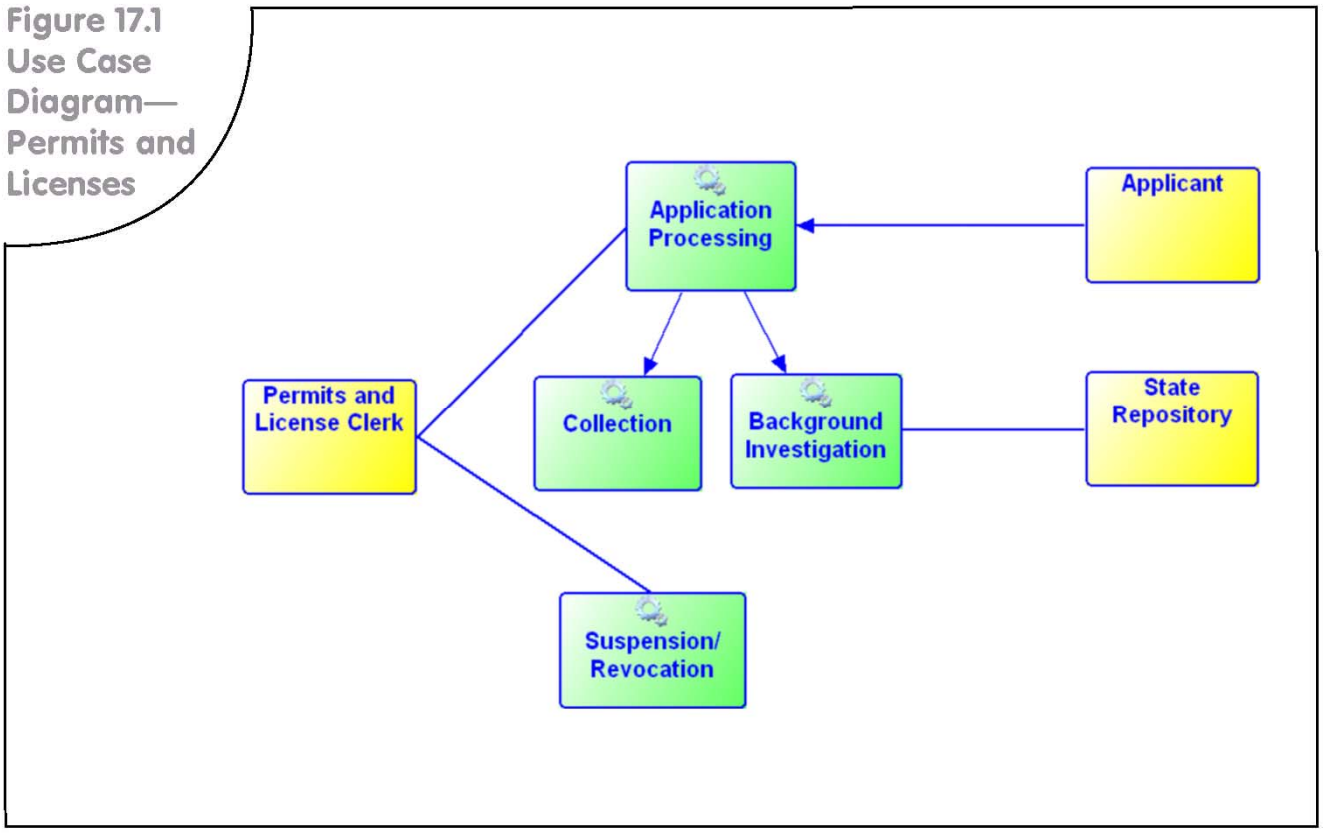
16.2 Use Case: Protection Order and Restraint Recording

The NCIC 2000 Protection Order File is a national registry that allows courts to add, update, and clear orders of protection that have been issued by a civil or criminal court. As of the end of 2006, 46 states or territories were actively submitting data into the system. An RMS should have the capability to query the Protection Order File using the specified NCIC 2000 Protection Order File query format. At a minimum the query should require the subject or protected person's exact name and must be combined with any number of other query criteria such as exact date of birth, FBI number, social security numbers, etc.

Protection Orders that have been entered into the NCIC Protection Order File must be verified based on a specified validation schedule. The RMS should notify the appropriate user when a Protection Order record requires validation.

17 Business Function: Permits and Licenses

Figure 17.1 Use Case Diagram—Permits and Licenses



The Permits and Licenses module records and tracks the issuance of permits and licenses by the department. Examples of devices and activities that may require a license include but are not limited to electronic alarms, firearm ownership, and operating massage parlors. Examples of permits include parade, race, or demonstration permits. Generally, licenses provide authority for an extended period of time, while permits provide authority for a shorter and specific period of time.

The status of licenses and permits including application, granting, denial, revocation, and expiration is tracked in the RMS. A change of status or an upcoming expiration date generates appropriate alerts and notifications.

As part of the processing, applicant names may be checked against the system MNI. Depending on the type of license or permit, a history of criminal behavior or other background information may preclude the applicant from obtaining the license.

Once a license is issued, if the licensee is arrested or is issued a traffic violation, the system will generate an alert and notify the permit and license group to determine whether the license should be revoked.

The system also must track the payments associated with the issuance of licenses and permits or link with a financial system to determine payment status.

Standard Outputs:

Permit and license applications granted based on varying search criteria

Permit and license applications denied with reason

False alarm responses (for billing purposes)

Expiration notices

Permits and licenses

Standard External Data Exchanges:

CAD (e.g., call data from alarms)

Standard Internal Data Exchanges:

MNI

MOI

Other Optional External Data Exchanges:

Financial management system

17.1 Use Case Diagram (see Figure 17.1)

17.2 Use Case: Application Processing

The application process includes reviewing the application to ensure all requirements are met. The review will result in either an approval or denial. The decision will be recorded in the RMS, and a notification will be generated by the system and sent to the applicant.

Guidelines for approval may include successful completion of specific training and/or passing a background check to verify the absence of relevant criminal history information. There may be fees associated with the application process.

17.3 Use Case: Collection

The system will either receive notification of payment receipt from the financial system or record payment for the application. This module merely associates the payment with the application; it does not include cash drawer accounting.

17.4 Use Case: Background Investigation

The purpose of the background investigation is to determine whether the individual is eligible for the license or permit. The type of permit or license may require differing investigative steps and procedures, such as collecting fingerprints, performing criminal history checks, and other inquiries.

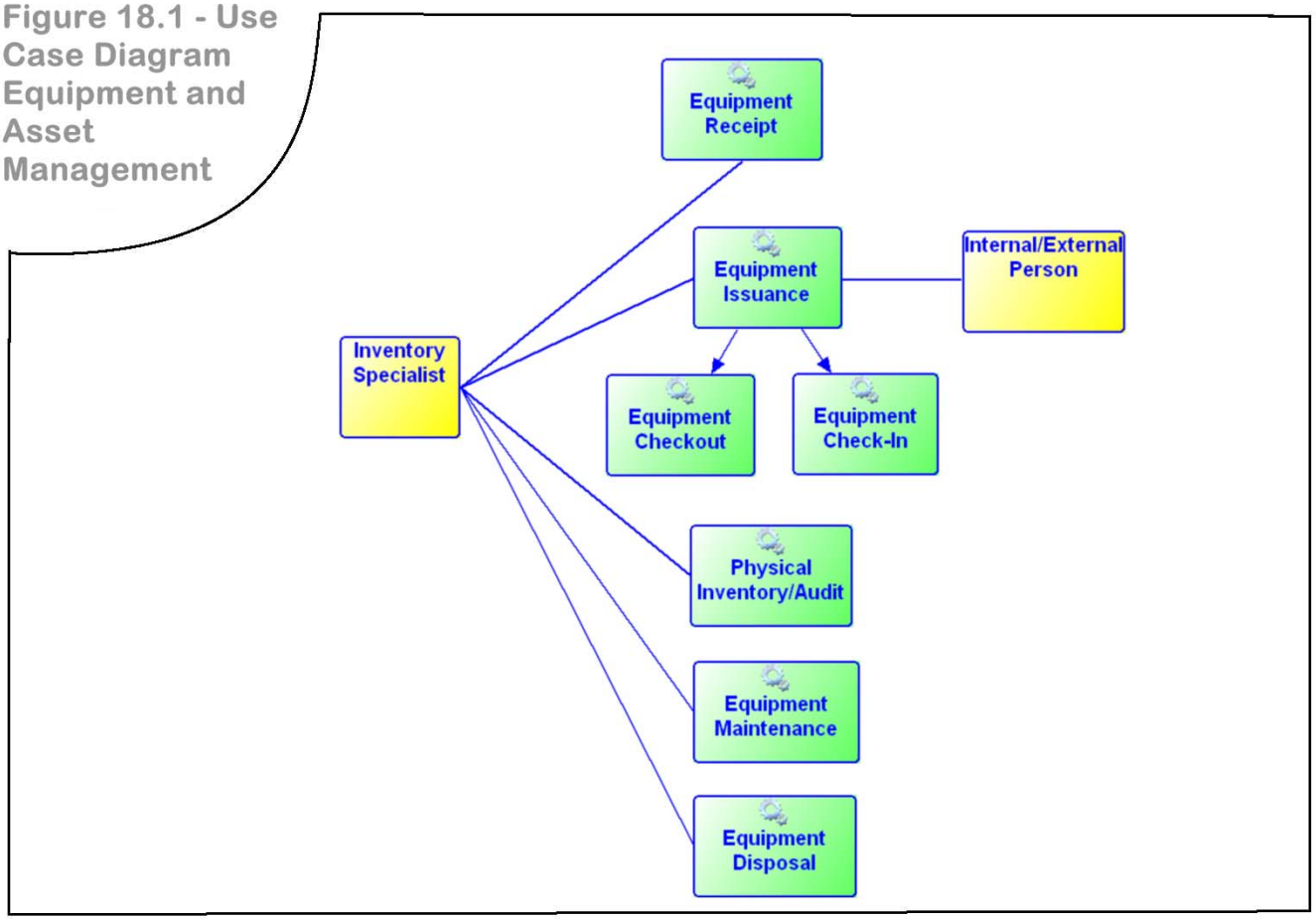
17.5. Use Case: Suspension-Revocation

Once the license has been issued, if a licensee is arrested or has qualifying traffic violations, the system will generate an alert to notify the permit and license group to determine whether the license should be revoked.

The above situation can result in the generation of a notification letter to the licensee.

18 Business Function: Equipment and Asset Management

Figure 18.1 - Use Case Diagram Equipment and Asset Management



Equipment management describes the processes that the law enforcement agency uses to:

Record the receipt of equipment

Record the source of the equipment

Issue equipment to an organizational element or individual

Track equipment check-in or checkout

Management and tracking of equipment may be facilitated by the integration of bar coding equipment, RFID, etc. The system should have the ability to store photographs of the equipment.

The Equipment and Asset Management module should generate reports to support physical inventory and audits, which will assist in managing the repair, disposal, and maintenance of agency equipment.

In some agencies, the inventory and control of agency property are regulated by authorities outside the law enforcement agency. If this is regulated by an outside agency, an interface between the two systems may minimize duplicate data entry.

Standard Outputs:

Physical inventory report, based on varying search criteria (e.g., category, age, unit, and location)

Physical inventory exception report

Check-in/checkout log

Equipment history

Bar Code Labels

Receipts

Standard External Data Exchanges:

Regulating authority (e.g., general services, facility services)

Bar Coding System

Inventory Control System

Other Optional External Exchanges:

Financial management system

Purchasing

18.1 Use Case Diagram (see Figure 18.1)

18.2 Use Case: Equipment Receipt

The Equipment and Asset Management module will allow the capture of descriptive characteristics of the equipment, associated identifiers on the equipment, and any agency-specific unique identifier, such as an inventory control number.

18.3 Use Case: Equipment Issuance

Equipment may be assigned to an organizational element (e.g., unit, division, or group) of the agency, a physical location, or an individual. In addition, equipment may be assigned on a check-in/checkout basis (e.g., daily basis, for patrol). The system must maintain a log of all activity.

Equipment may be authorized but not issued (e.g., a personally owned weapon). The authorization to carry that equipment must be captured.

18.4 Use Case: Equipment Checkout

When equipment is checked out to a unit or authorized person, information about the checkout (e.g., individual receiving equipment, date and time of equipment checkout, and condition of equipment) is recorded for tracking purposes.

This process may be facilitated by the use of bar-code or RFID equipment.

18.5 Use Case: Equipment Check-In

The return of equipment will include an evaluation of the condition of the item, performance of maintenance procedures, disposition of equipment deemed unfit for service, and the return of functional equipment.

The system must support the generation of reports for overdue, lost, stolen, or destroyed equipment.

The system must be capable of printing receipts.

18.6 Use Case: Physical Inventory/Audit

This function of the system must be able to generate reports about the physical whereabouts of agency equipment. A physical inventory will result in the identification of missing equipment, as well as equipment recommended for repair, replacement, or disposal. This process may determine that the location of the equipment has changed. All information gathered during the physical inventory is used to update the system.

18.7 Use Case: Equipment Maintenance

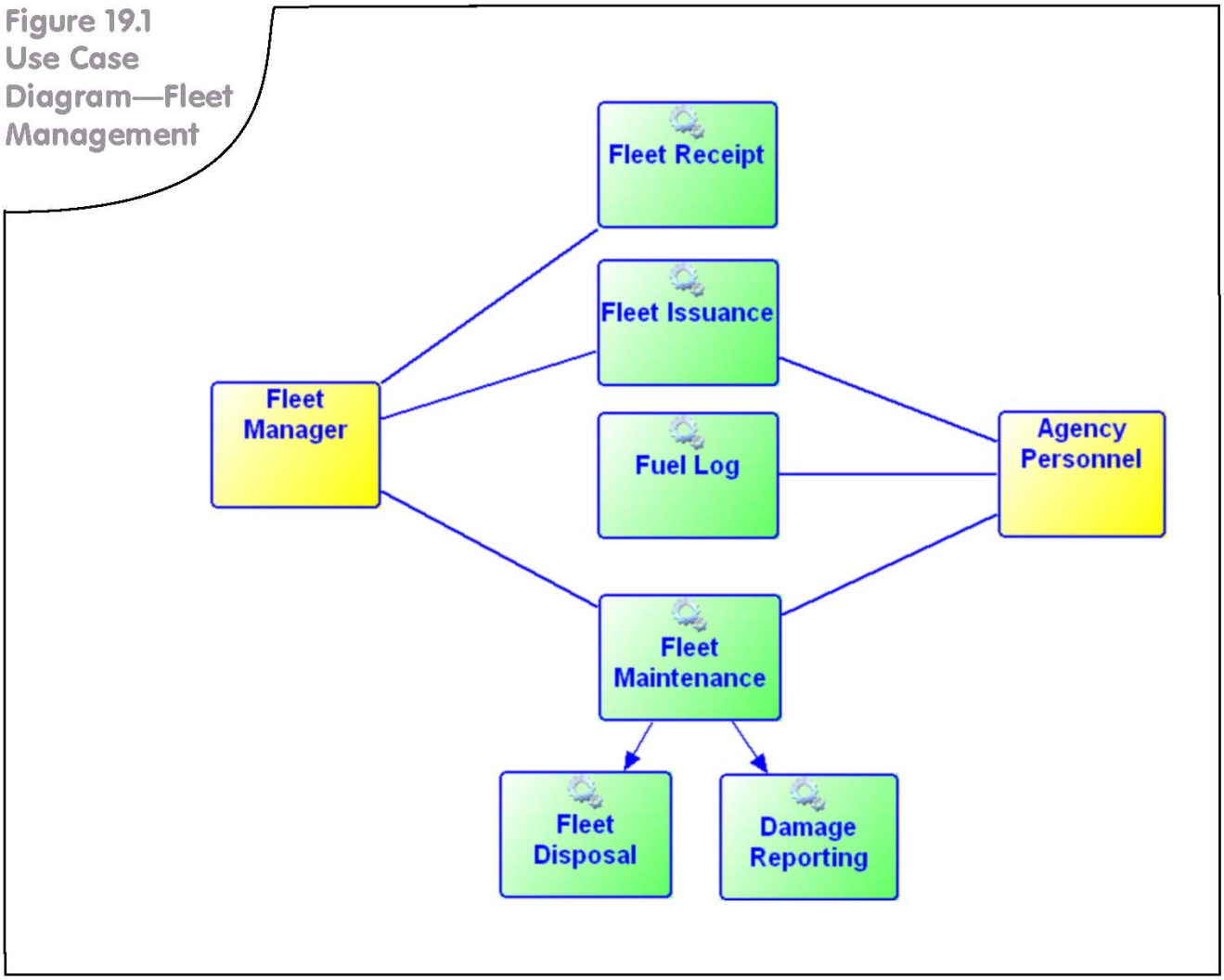
The system shall record information about equipment condition and maintenance. The information recorded in this module includes reason for repair, cost of repair, date of repair, maintenance location, date expected back in service, date returned to service, and date of next scheduled maintenance.

18.8 Use Case: Equipment Disposal

This is the process associated with taking a piece of equipment out of service and disposing of it. The system changes the equipment status but will not delete or remove historical records associated with that item.

19 Business Function: Fleet Management

Figure 19.1 Use Case Diagram—Fleet Management



Fleet management includes all vehicle types (e.g., car, motorcycle, boat, and aircraft) and generally encompasses:

Tracking and issuance of fleet assets

Tracking service and maintenance schedules and history

Parts inventory and warranties

Fuel and oil inventory and usage

Vehicle disposal

When maintenance or repair work is performed by a contractor, the Fleet Management module may include functions to track vendors and the services they provide.

Equipment assigned to vehicles may be associated with the identifiers issued by the Equipment and Asset Management module.

Standard Outputs:

Fleet inventory

Maintenance schedule

Fleet repair log

Fluid consumption/cost

Vehicle repair cost

Fleet equipment list

External Data Exchanges:

CAD (e.g., for mileage and use information)

Other Optional External Data Exchanges:

External fleet management system managed by city, county, or agency

Fuel card system

Personnel module (for tracking vehicle and related damage/accidents)

19.1 Use Case Diagram (see Figure 19.1)

19.2 Use Case: Fleet Receipt

The Fleet Management module will allow the capture of:

Descriptive characteristics of the vehicle (e.g., color, make, and model)

Date the vehicle was deployed

Starting mileage

Identifiers (e.g., VIN and license plate number)

Any agency-specific unique identifier

This module also will establish the service schedule for activities such as tune-ups and oil changes.

19.3 Use Case: Fleet Issuance

Fleet issuance refers to tracking events related to fleet asset issuance and where fleet is assigned. Vehicles are assigned to a particular organizational element or individual. The system should allow the ability to track the issuance history of the vehicle.

19.4 Use Case: Fuel Log

The Fleet Management module records the date, price, and amount of fuel purchased at each fill-up, as well as the vehicle's mileage at the time of fill-up. This assists the agency in tracking fuel-related costs.

If the agency uses a fuel card system, there may be an interface between it and the Fleet Management module to import the fill-up data directly.

19.5 Use Case: Fleet Maintenance

The system can be used to record information about vehicle maintenance and service. The information recorded in this module includes:

Projected and actual maintenance schedule

Fluid servicing

Vendor providing service

Repair schedule

Repair and maintenance costs

In addition to periodic scheduled maintenance, a vehicle can enter this process if it is determined to be in need of unexpected repair.

19.6 Use Case: Damage Reporting

Agency personnel and the fleet manager will periodically assess the condition of the vehicle and record any damage.

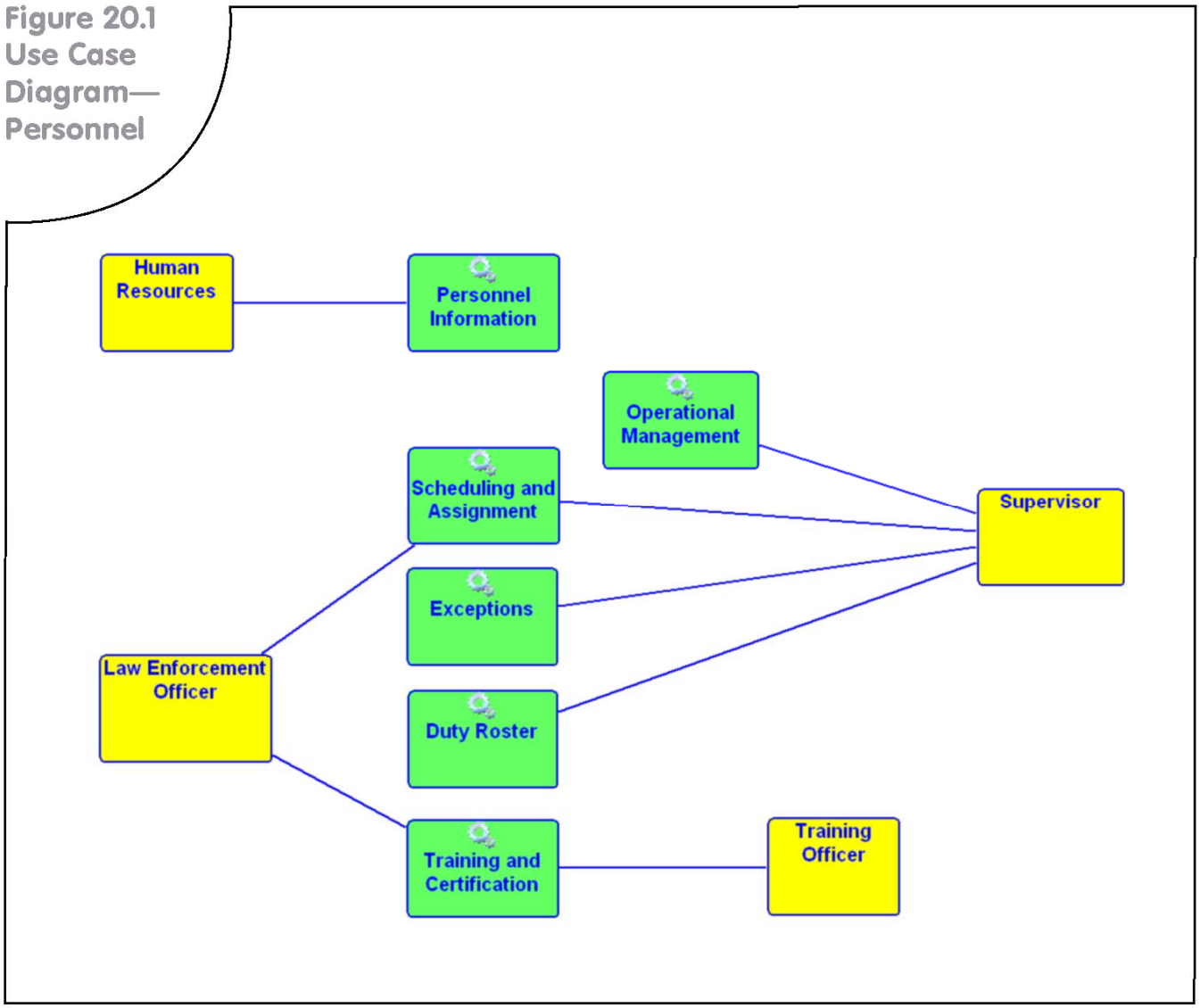
This may or may not lead to a repair or maintenance activity. It also may lead to an assessment of officer performance.

19.7 Use Case: Fleet Disposal

This process is associated with taking a vehicle out of service and disposing of it. The system changes the vehicle status but will not delete or remove historical records associated with that item.

20 Business Function: Personnel

Figure 20.1 Use Case Diagram—Personnel



The Personnel module allows law enforcement managers to capture and maintain information on the individuals in their department, including volunteers. It also may include information on people outside the department who have received training from the department (e.g., people attending a citizen's academy). This information typically includes the person's basic information, such as emergency contacts, current and past assignments, education, training history, and certifications.

In most locations, information about the employee also is maintained in an external human resource system. To avoid duplicate data entry, an interface should be established between the human resources system and the law enforcement RMS personnel module.

This module addresses those functions that are unique to a law enforcement agency and/or are typically not found in a stand-alone human resources software program.

The regulations under the Health Insurance Portability and Privacy Act (HIPPA) apply to those agencies that provide health care. To determine whether your system falls under the purview of HIPAA, look at http://www.hhs.gov/ocr/hipaa/.

Standard Outputs:

Personnel summary, based on varying search criteria

Personnel detail

Duty roster

Training and certification scheduling

Pending certification and skill expiration

Issued equipment based on varying search criteria

Health maintenance requirements for duty status

Paid detail or detail scheduling

Standard External Data Exchanges:

Human resources system

Staffing deployment system

CAD

Standard Internal Data Exchanges:

Equipment and Asset Management module

Fleet Management module

20.1 Use Case Diagram (see Figure 20.1)

20.2 Use Case: Operational Management

The RMS should be able to draw on RMS data to identify potential personnel and organizational issues. The information includes biased-based policing, uses of force, vehicle pursuits, vehicle crashes, employee injuries, citation data, field contact reports, citizen complaints, and civil and criminal actions.

Management should be able to conduct analyses, as well as ad hoc reporting on these parameters. Management should have the ability to define thresholds on data elements of interest and be notified when certain values, either above or below the thresholds, have been reached.

20.3 Use Case: Personnel Information

The system must allow for the gathering and maintenance of basic information for all personnel working for the department. Information may include names and addresses, physical characteristics, assigned equipment, emergency contact information, special skills, classifications (e.g. sworn/non-sworn), and rank histories.

Health maintenance is important to agency productivity, and some aspects of protecting employee health are mandated by law. The Personnel module will support the tracking of required vaccinations and medical baselines, such as titer tests for tuberculosis exposure. An agency-specific table should maintain information on vaccinations required by law or recommended by the agency and each vaccination's duration of efficacy. The Personnel module will collect information on date, type, and expiration date of vaccinations employees receive. Reports generated to supervisors will alert the agency to upcoming expirations and needed vaccinations. Similarly, the module will collect information on current health-related duty restrictions affecting employees, produce supervisor reports to ensure employee duties are assigned appropriately to prevent injury, and permit longitudinal tracking and analysis of medical limitations for risk management.

20.4 Use Case: Scheduling and Assignment

The scheduling portion allows for the creation and maintenance of schedule patterns (e.g., days on, days off, and assigned hours). The assignment portion records the officer assignment, shift, and location and associates the officer with a particular pattern. As assignments change, the personnel record is updated to reflect the new assignment. All exceptions to the officer assignment must be recorded.

The system creates the duty roster, which is based on the assignment, schedule, and exceptions to the schedule. To be able to generate past and future rosters, a complete history of assignments, patterns, and exceptions are maintained.

If the department uses an external manpower deployment system, the system can be used for defining and finalizing changes in the overall plan for resource utilization, and changes in the assignment can be updated in the Personnel module. These automated updates will require an interface between the two systems.

20.5 Use Case: Exceptions

After schedules and assignments have been generated, it will then be necessary to document all conflicts with previously created work schedules. The exception can include any other duty or assignment outside the scheduled or assigned pattern (e.g., training, vacation, or sick leave).

20.6 Use Case: Duty Roster

From the scheduling rotation, assignment, and exception information, the system generates the duty roster for a particular time period (e.g., past, present, or future) the supervisor selects.

20.7 Use Case: Training and Certification

The Personnel module tracks training history and the certification process. The certification process includes officer certification status, deadlines for maintaining certifications, necessary hours of training, and student performance.

21 Business Function: Internal Affairs

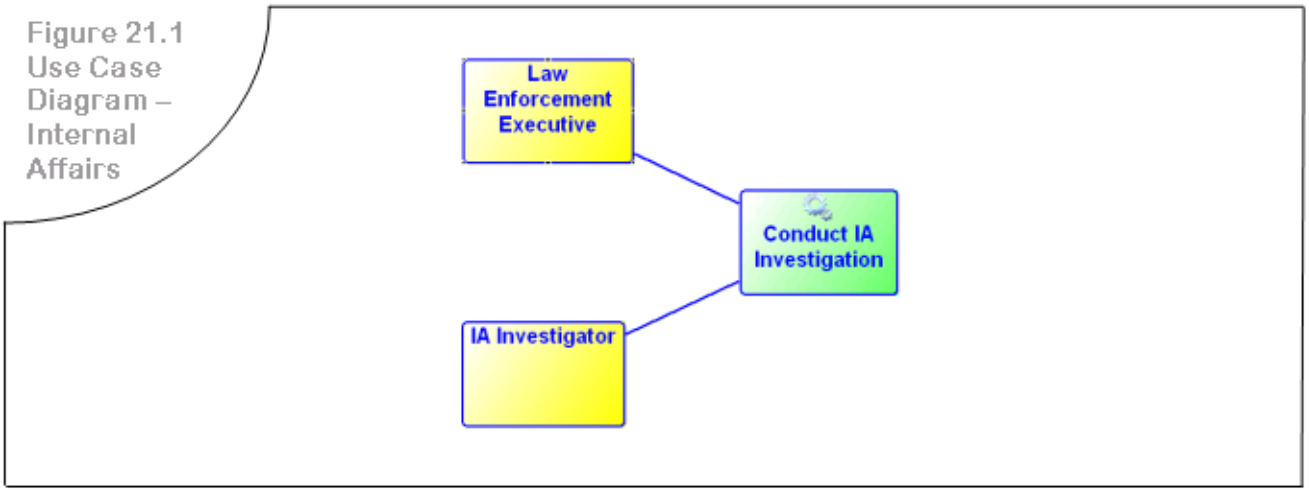


Figure 21.1 Use Case Diagram – Internal Affairs

A law enforcement agency's internal affairs (IA) Division investigates allegations of misconduct on the part of employees of the department.

There are several common administrative requirements that help isolate the IA investigation information. The IA system must have multiple levels of security for the application itself, for individual records or groups of records, and for individual or groups of fields. Due to the sensitivity of the information collected in IA functions, the data should be encrypted.

The RMS will store all information related to the IA investigation.

21.1 Use Case Diagram (see Figure 21.1)

21.2 Use Case: Conduct IA Investigation

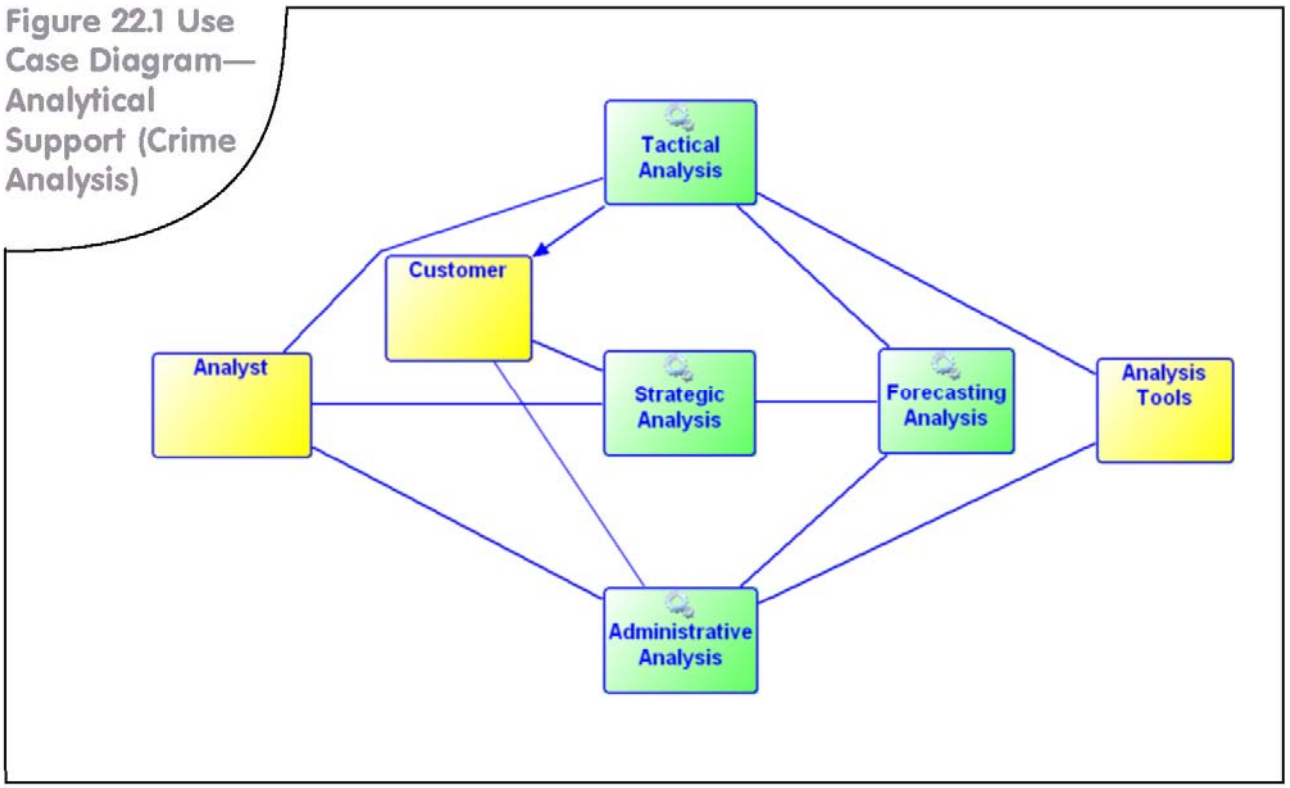
The purpose of an IA investigation is to ensure that department policy and procedures are followed and that agency standards of professionalism are adhered to by all department employees.

In many ways, IA investigations are conducted in a manner similar to criminal investigations. Subjects, witnesses, and complainants are interviewed and that information, along with the facts of the case, is recorded in the Internal Affairs module.

Security levels within the Internal Affairs module will limit the availability of information accessible through other RMS modules and indices. An agency-designated recipient will receive an alert whenever a party to an investigation is the subject of a query or if any other RMS activity occurs regarding that party.

22 Business Function: Analytical Support (Crime Analysis)

Figure 22.1 Use Case Diagram—Analytical Support (Crime Analysis)



Analytical support is the systematic process of collecting, collating, analyzing, and disseminating timely, accurate, and useful information that describes patterns, trends, problems, and potential suspects in criminal activity. The RMS should support the tools used by the analyst in this work. Analytical support can be subdivided into four main types:

Tactical Analysis: Provides information to assist operations personnel in the identification of specific policing problems and the arrest of criminal offenders.

Strategic Analysis: Provides information concerning long-range crime problems. Strategic crime analysis provides information concerning crime rate variations and provides geographic, economic, social, and/or other types of general information to administrators.

Administrative Analysis: Provides information to support administrative decisions related to resource allocation and to support budget requests and decisions.

Forecasting Analysis: A combination of tactical, strategic, and administrative analysis, merging multiple sets of data.

In addition to being able to query and produce ad hoc reports on any number of indicators, analytical support also includes standardized reporting functionality. One example of a standardized report is crime statistics. Crime statistics are essentially comparative statistics on the community crime rate, which can be disaggregated by specified timeframes, offenses, and complaints by beat or zone.

The RMS must interface with analytical support tools, such as crime-mapping software and link-analysis, data mining, spatial, and temporal tools. The results of these

analyses should be stored in the RMS for a time determined by the jurisdiction's SOP and can be used to assess agency performance and to provide support for administrative decisions. The RMS should have a variety of reporting functions attached to its Analytical Support modules and allow presentation of information in a variety of formats, such as bar graphs, pie charts, and line graphs.

The RMS should support the ability to aggregate data on the various indicators, such as:

Current period vs. previous period

Current period vs. historical average

Percentage of total crimes for period by:

- Reporting districts
- Areas/beats/zones
- Teams/shifts

Percentage change from prior periods (i.e., trend)

The RMS should contain the ability to conduct crime distribution analysis based on a number of criteria, including:

By area/beat or reporting district (i.e., ZIP codes)

By time, date, and day of week

Frequency of occurrence

Citation

Crime/incident report number

Field interview data

Search warrant data

Vehicle information

Type of offense (e.g., residential, auto, or business)

The system also should include standardized reports, such as general offense activity, offense activity by day of week, and offense activity by beat. Every field of operational data in the RMS (i.e., data entered by the user in any form, not configuration or system control data) should be searchable, including narrative (e.g., text or memo) fields. This can be done by using query interfaces that are part of the application or, at a minimum, using third-party tools that can access the operational database.

The RMS should include an alert function related to analytical support to provide for the immediate transmission of information to law enforcement officers in the field.

The RMS should support a quality control process on incoming reports to ensure that data are correctly and completely entered.

The RMS should contain complete data elements that relate to time, such as the day, time of day, week, date, month, and year. It also should include a locally determined and previously validated geographic reference.

The RMS should support crime/suspect correlations to show a relationship between a suspect and an offense. The correlations may be made by using any number of selected criteria in which unique and distinguishing characteristics, physical identifiers, modus operandi, and various other common traits of offenders are known. These identifiers may be captured as a part of multiple different RMS functions, including the Incident Reporting module, the Field Contact module, the Arrest module, the Crash Reporting module, the Citation module, the MNI, the MVI, the MLI, and the MOI.

Standard Output:

Crime distribution analysis reports using the criteria listed above

Standard External Data Exchanges:

Third-party mapping, analysis, and graphing tools

State, regional, and national information sharing systems (e.g., RISSnet, N-DEx)

22.1 Use Case Diagram (see Figure 22.1)

22.2 Use Case: Tactical Analysis

Tactical analysis provides information to assist personnel in the identification of specific, immediate crime or disorder problems and the arrest of criminal offenders. Tactical analysis provides information to assist personnel (e.g., patrol and investigative officers) in preventing and disrupting criminal behavior, identifying specific and immediate crime problems, and arresting criminal offenders. Analytical data are used to promote a quick response to field situations.

22.3 Use Case: Strategic Analysis

The purpose of strategic analysis is to provide information concerning long-range problems. Strategic analysis is primarily concerned with solutions to ongoing problems. It results in the ability to accomplish the agency mission more effectively and efficiently.

22.4 Use Case: Forecasting Analysis

The purpose of forecasting analysis is to prevent crime by analyzing information collected in the RMS and correlating it with external sources. It can involve the application of advanced analytical methods to forecast the occurrence of specific crimes or trends.

The RMS should support the ability of the analyst to generate the Forecasting Analysis report. The report's format should be tailored to meet the particular requirements of the customers who receive the information, whether they are patrol, investigative, or administrative personnel.

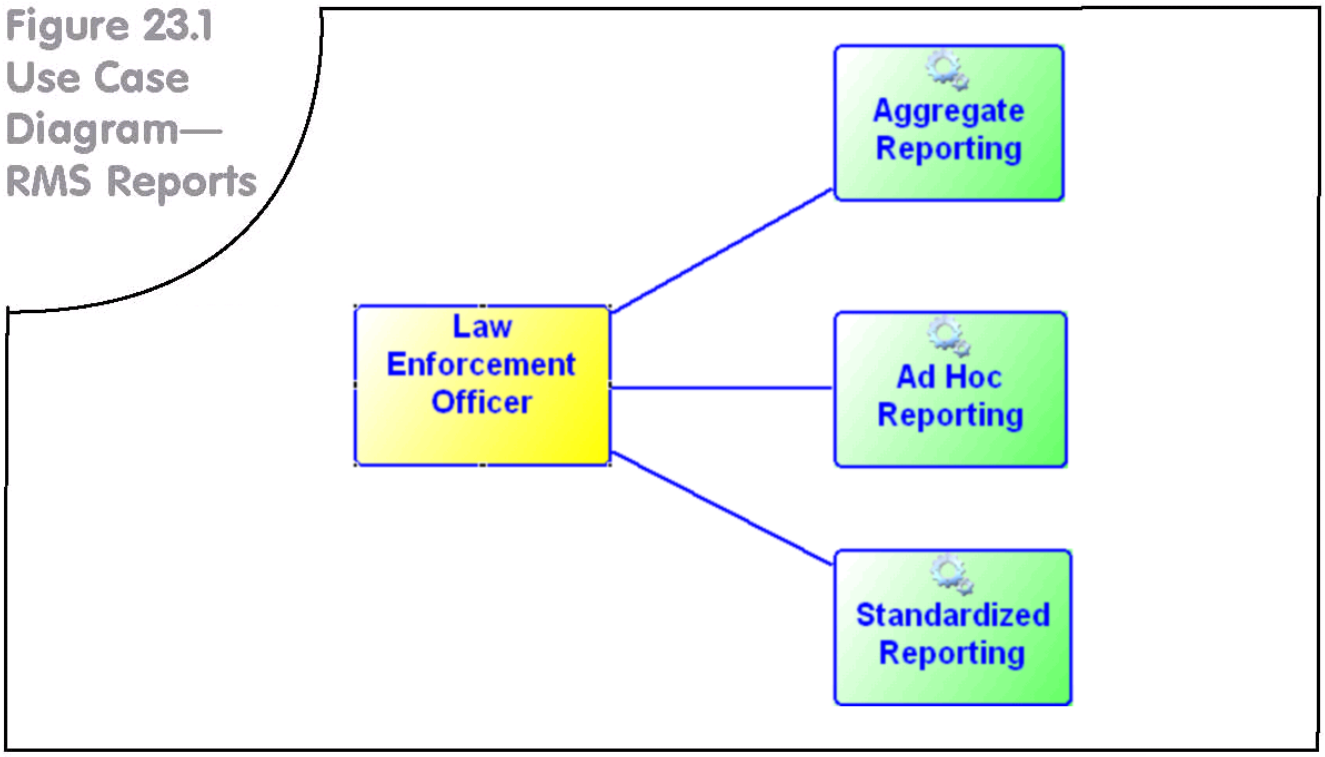
22.5 Use Case: Administrative Analysis

Administrative analysis develops long-range (e.g., quarterly, semiannually, or annually), strategic comparisons and reports them externally. Examples of administrative crime analysis tasks may include providing economic, geographic, and law enforcement information to law enforcement management, neighborhood/citizen groups, other appropriate agencies, and the public.

Where required by the agency's SOP, the RMS should support the ability to generate statistical reports on all law enforcement activities within that agency, allocate costs to those activities, and track performance measures as defined by the agency.

23 Business Function: RMS Reports

Figure 23.1 Use Case Diagram—RMS Reports



The RMS Reports module documents officer and agency-wide activity or performance in a given area. Many reports are created over the course of conducting policing business (e.g., arrest report and incident report). Aggregated reports are conducted by line and supervisory staff and reviewed by law enforcement executives. Role-based security should restrict access to some reports.

Law enforcement personnel must be able to generate standardized reports and aggregate reports, as well as query the RMS to produce ad hoc reports from the RMS Reports module.

Examples of standardized reports from the RMS business functions are:

Incident reports

Crash reports

Property/evidence reports

Citation reports

Field interview reports

Uniform Crime Reporting (UCR)/National Incident-Based Reporting System (NIBRS) reports

Case management reports

Billing reports

Summary reports for warrants, citations, CFS, accidents, and employees

Typically, third-party products are used for ad hoc queries and reports.

23.1 Use Case Diagram (see Figure 23.1)

23.2 Use Case: Aggregate Reporting

Aggregate, agency-wide reporting allows law enforcement personnel to associate information in a variety of ways and among a number of different tables or fields, including CFS, warrants, incident reports, crash data, property data, and weapons data.

Managers must be able to query, retrieve, and display information in a variety of ways. They must be able to query on indicators, such as date of the incident, case type, and assigned officer. They should be able to produce reports from a list of standardized reports or on an ad hoc basis.

The query and data retrieval system must be integrated with the RMS security system so that the department can designate search and query types and depths by password or groups of passwords or by role.

23.3 Use Case: Standardized Reporting

Each module includes its own set of standardized reports, which also are available through the RMS Reporting module.

23.4 Use Case: Ad Hoc Reporting

The agency may need operational reports and analysis that are not provided by standard RMS reports and queries. Ad hoc reporting will allow a user to define and create these additional custom reports. Once created, these custom reports can be saved and run as standard reports.

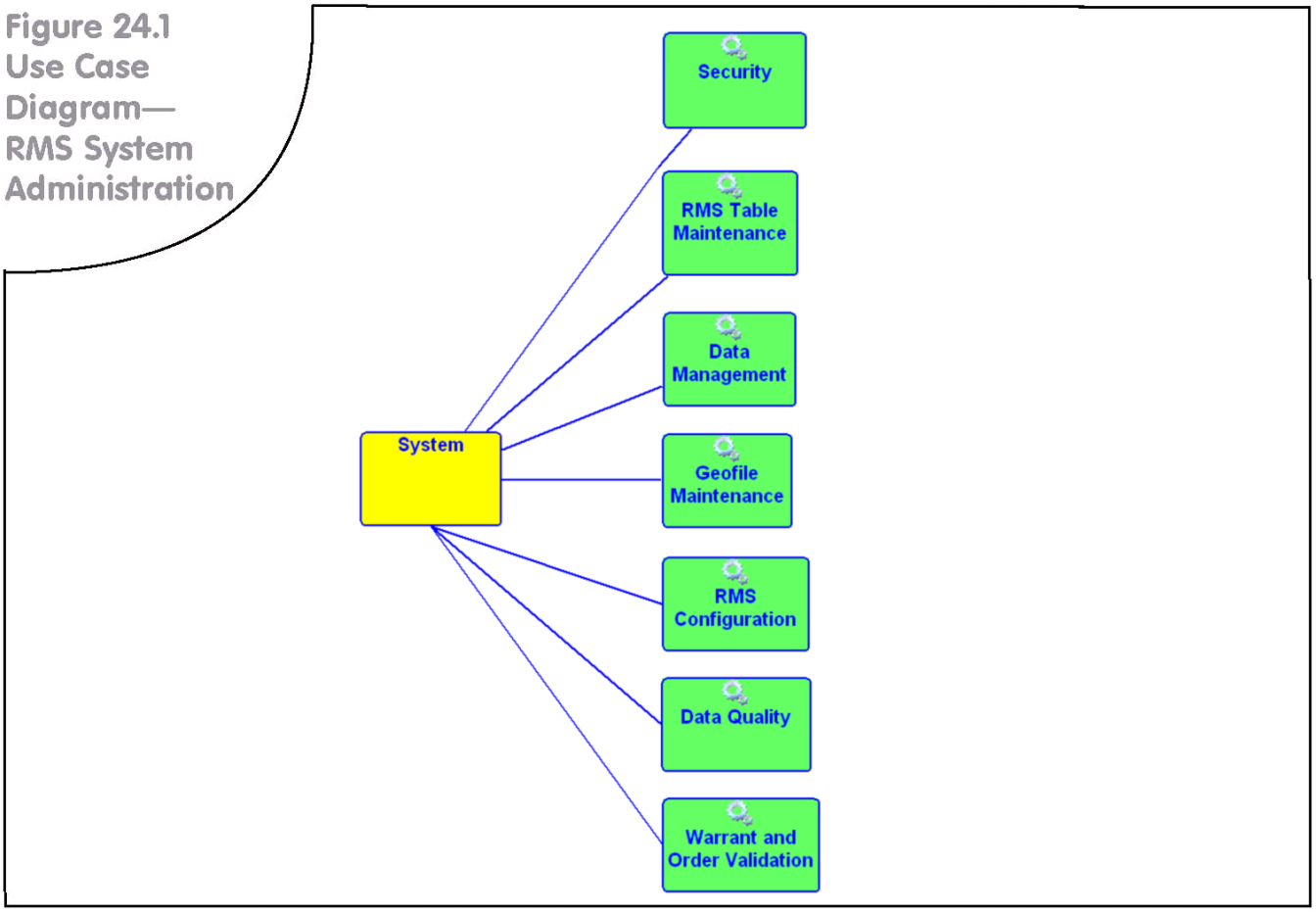
The RMS should provide a tool or mechanism that can be used to produce any number of ad hoc reports.

This ad hoc reporting tool or mechanism may be provided using a third-party solution. This solution may be embedded in the application or run as a stand-alone function. Ad hoc reporting functions that are embedded into the RMS solution may use existing RMS security controls. Stand-alone, ad hoc applications open the potential to bypass the RMS security controls (e.g., juvenile data, sealed records, and redacted records). On the other hand, the stand-alone approach may allow an agency to have more ad-hoc reporting capabilities. Any stand-alone or third party tools provided as part of this business function should be integrated with the RMS security mechanism.

Another approach is to extract data, excluding secured information, into files or data warehouses. That way, stand-alone, ad hoc tools can be used to access the data without compromising RMS security controls and performance.

24 Business Function: RMS System Administration

Figure 24.1 Use Case Diagram—RMS System Administration



Many aspects of an RMS should be configurable so that they can be used to meet specific agency requirements. The RMS administration functions address the configurable aspects of an RMS.

System administration encompasses a wide array of general functions that law enforcement agencies need in an RMS to be able to create and query information effectively; to ensure appropriate access to information and system security; and to ensure effective departmental information.

Examples of administrative functions include:

RMS table maintenance

RMS configurations (e.g., parameters, defaults)

Security (e.g., user role, jurisdiction)

Geofile maintenance

Data management (e.g., data dictionary, archive and purge)

Standard Outputs:

Report on users, sortable by names, access level, password age, and machine used

Report on RMS use, sortable by user log-in, frequency, total time in system, number of concurrent log-ins, machine used, and duration time-outs

Report on failed log-ins, sortable by log-in name, number of attempts, date/time of attempt, and machine used

Report on subsystem security violations

Alerts; agency-definable security violations, which generate an external message to predefined locations

E-mail system for alerts

Standard Internal Data Exchanges:

Agency network operating system

24.1 Use Case Diagram (see Figure 24.1)

24.2 Use Case: Security

Systems should allow tiered access to information, based on passwords and other authentication and non-repudiation practices. Role-based authentication and authorization must be a part of the RMS. Other standards current exist for identification technologies such as biometrics, identification cards, and security tokens.

Systems should apply appropriate edits to all entered data to ensure data integrity and maintain activity logs and audit trails.

The security mechanism must also take into account local, county, state, and national security policies and requirements (e.g., NCIC Security Policy)

24.3 Use Case: RMS Table Maintenance

The RMS should include the ability for the user agency to define and maintain code lists and associated literals (i.e., plain English translation) for as many data elements as possible. The literals should be stored in the database, as appropriate.

Where available and applicable, the RMS should use the authoritative code tables referenced in GJXDM, NIEM, and NCIC.

24.4 Use Case: Data Management

Data management includes the following:

Record expungement, sealing, and purging

Data redaction

Data dictionary

These topics are further described in the following paragraphs.

Record Expungement, Sealing, and Purging

The RMS must be able to support expungement, sealing, and purging of whole records and partial records. To support this function, the system must be able to flag a record, to flag data elements within a record, and to delete a record. The RMS should also allow the agency to indicate why the record or data element is restricted.

Data Redaction

Redaction is the process of editing report information to filter sensitive or confidential information before the report is released to the public or for general use outside the department. The type of information that is edited includes victims' names in certain types of cases, juvenile information, information that is considered by the agency to be sensitive to an investigation, and information whose release is prohibited or restricted by local, county, state, or federal law or policy.

In the case of formatted and structured data, report output programs can produce a redacted version of specific report data. In the case of narrative or otherwise unstructured information, the redaction process requires a manual step to produce a public version of the report.

Generalized report tools, if employed to produce reports for public consumption, should be used only on data that have already been redacted.

Data Dictionary

The RMS must provide a capability to display and/or print the database structures to allow the end user to access the database tables through third-party, ad hoc inquiry tools/utilities.

The data dictionary may contain the following information for each field description:

Field name (e.g., external representation)

Database column name (e.g., internal representation)

Data type (e.g., numeric, alpha, or date)

Field size

Field format (i.e., output format)

Edit or validation criteria

Associated code table

Default value

Description

24.5 Use Case: Geofile Maintenance

The geofile is used to validate and standardize location and address information. It also is used to cross-reference addresses and locations with law enforcement-defined reporting areas, latitude/longitude/altitude coordinates, ZIP codes, and other identifiers. The geofile contains sufficient information to ensure that an address is valid. Furthermore, it provides cross-references to addresses and locations using commonplace names (e.g., business names, parks, hospitals, and schools) and street aliases. It includes information such as direction of travel on particular streets and can identify the side of a street for a specific address. It is assumed that all addresses in the RMS are validated using the system geofile.

The reporting area defined above should be used to define beats, sectors, command areas, neighborhoods, communities, etc.

The geofile contains the geographic information that is the basis for many decisions in a communications center. The system needs to provide the ability for an agency to enter and update all geofile data, including the physical address and the latitude/longitude/altitude coordinates.

The creation of a comprehensive geofile is a significant undertaking. The system should support the creation and maintenance of the geofile using an available mapping/Geographical Information System (GIS) database. Geofile information in the CAD and the RMS should be synchronized, based on established parameters.

24.6 Use Case: RMS Configuration

Some parameters of the RMS should be configurable by the system administrator. For example, the system administrator should be able to modify parameters, such as agency and chief's name, Originating Agency Identifier (ORI), address, and phone number. Changes to parameters, such as juvenile majority age, latitude/longitude/altitude or state plane geography coordinates, and name match rules, should be allowed.

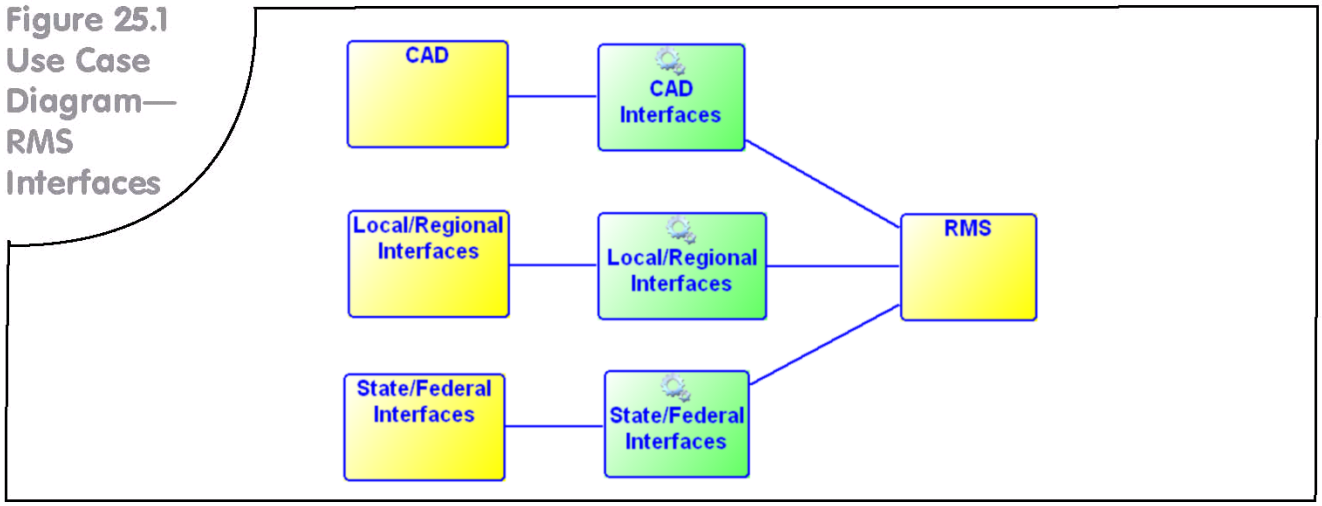
The system administrator also must have the ability to define the conditions under which an alert or notification is issued.

In a multi-jurisdictional RMS, the system administrator should be able to change the parameters for each participating agency.

Any configuration changes that could affect system integrity must be properly flagged with adequate warning to prevent inadvertent damage to the system.

25 Business Function: RMS Interfaces

Figure 25.1 Use Case Diagram—RMS Interfaces



The RMS requires functionality to exchange data with other systems. The exact nature of those exchanges will, in large part, be determined by local business practices and local agency work flows. All interfaces need to comply with national standards. Each business function includes examples of data exchanges.

Sections 25.2 – 25.4 describe exchanges between local and State or Federal Interfaces. Section 25.5 – 25.7 describe particular exchanges in greater detail.

25.1 Use Case Diagram (see Figure 25.1)

25.2 Use Case: CAD Interfaces

Information may be transferred from a CAD system to the RMS when units are initially dispatched, an incident number is assigned, and/or the call is closed in the CAD system.

CAD users require the ability to retrieve information from the RMS based on name, location, and vehicle descriptors.

25.3 Use Case: Local/Regional Interfaces

RMS users need to access and possibly update a variety of local and regional systems. Examples include court systems, prosecutor systems, financial systems, JMS, human resources systems, and multi-jurisdictional information systems. Data exchanges with many of these systems are identified in the specific business functions in this document.

These interfaces should be based on national standards, such as GJXDM, NIEM, and NCIC.

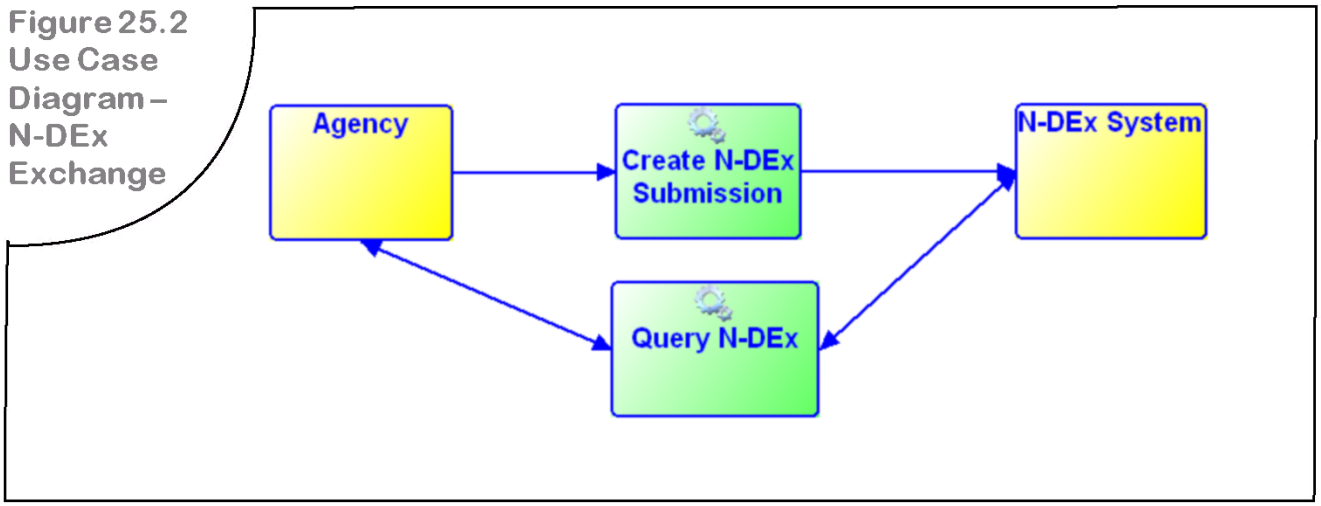
25.4 Use Case: State/Federal Interfaces

The RMS needs to query, add, or modify information stored in state and federal systems. Examples include updates for wanted people, missing people, stolen vehicles/property, and state sex offender registries.

In addition, the RMS needs to interface to state, regional, and federal information sharing systems (e.g., RISSnet, N-DEx, ISE). These interfaces should be based on national standards, such as GJXDM, NIEM, and NCIC.

25.5 N-DEx Exchange

Figure 25.2 Use Case Diagram – N-DEx Exchange



The N-DEx system will provide law enforcement agencies with a new investigative tool to search, link, analyze and share criminal justice information (e.g. incident and case reports) on a national basis. Figure 25.2 describes the general flow of information between the local agency and the N-DEx system. The incident, arrest, or booking report would be eligible for transmission following report approval by a supervisor. The particular type of report that is transmitted is based on the event that triggered the exchange. For example, submitting a booking report would trigger a process that would culminate with transmission of that report to the State Fusion Center or the ISE.

Participating local jurisdictions will be able to query this system using an extensive variety of investigative factors and receive responses to their queries. The RMS must provide the ability to not only create an N-DEx submission but also to query the system from within the RMS and return results into a view that is native to that RMS.

The RMS must be able to connect to the N-DEx system to establish recurring N-DEx queries that will automatically notify the user in the event that N-DEx records are added or updated and match those criteria. It is expected that the agency will use its local network to transmit and receive the N-DEx messages, when possible. For the majority of implementations, it is anticipated that the exchange of information will be one way and there is no need to expose RMS records to a federated query from a state or federal system.

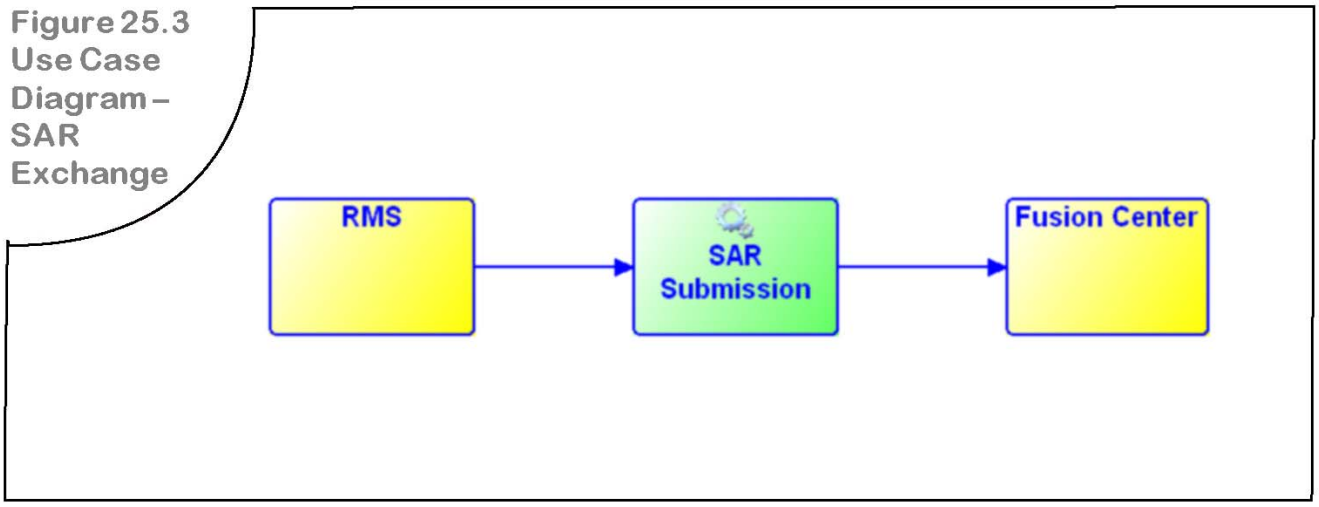
Submission of N-DEx data may be real-time or batch.

All submissions, whether to the state/regional system or N-DEx, must conform to the N-DEx IEPD. The actual content of the submission depends on the event that triggered the submission. For example, if triggered by an incident, an incident report becomes the payload; likewise, if triggered by a booking, the booking report is used.

The RMS must have the ability to query the N-DEx system based on any number of factors (e.g. person, modus operandi, etc.). Credentials for application access must be passed from the RMS to N-DEx. The user can be automatically notified for similar queries or new entries or repeating queries. A query may return data or simply link to additional data.

25.6 Suspicious Activity Report (SAR) Exchange

Figure 25.3 Use Case Diagram – SAR Exchange



The Suspicious Activity Report (SAR) exchange is designed to support the sharing of suspicious activity, incident, or behavior information throughout the ISE and between Fusion Centers and their law enforcement or intelligence information sharing partners at the federal, state, local, and tribal levels. Figure 25.3 describes the exchange between local agencies and their respective regional or state fusion center. These SARs will provide for the discovery of patterns, trends, or nationally suspicious activities beyond what would be recognized within a single jurisdiction, state, or territory.

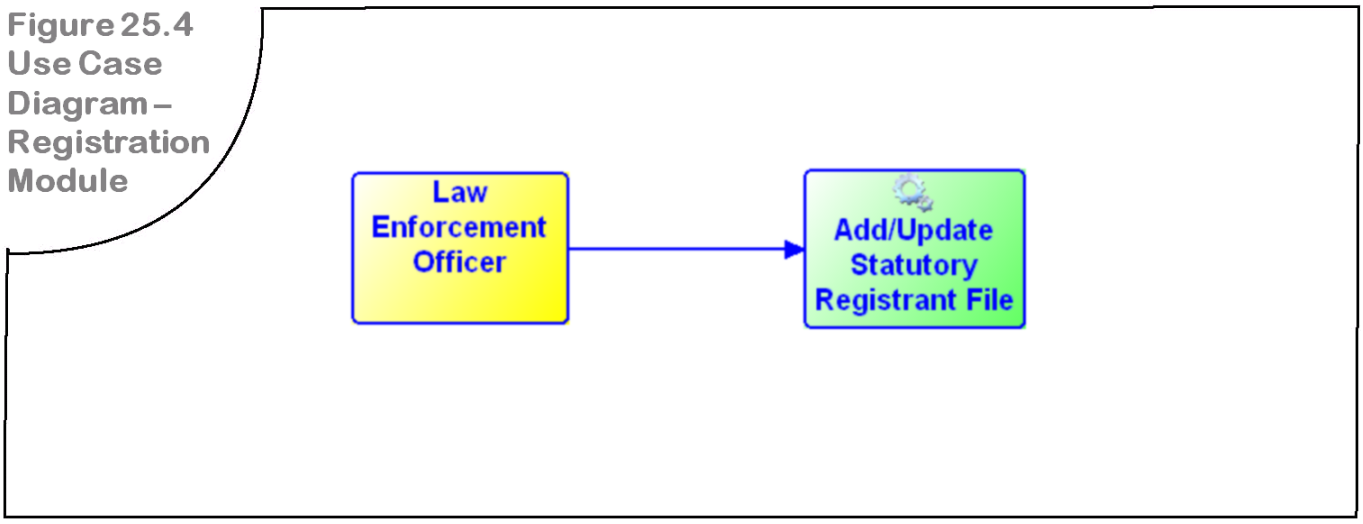
Standardized and consistent sharing of suspicious activity information with the state-designated Fusion Centers is deemed vital to assessing, deterring, preventing, and or prosecuting those planning terrorist activities. The SAR IEPD has been designed to incorporate key elements for terrorist related activities as well as all other crimes.

To use the SAR exchange, RMS Systems should allow officers to tag a report as being eligible for transmission to the state fusion center. The criteria for what constitutes a suspicious activity will need to be further refined and training implemented to assure a successful implementation of SAR.

Like N-DEx, the SAR specification has been developed based on the LEISP Exchange Specification (LEXS). This means that RMS service providers should be able to reuse much of the software written for N-DEx. This constitutes additional functionality that should be embedded as part of the Field Contact Modules (Module 13).

25.7 Registration Module

Figure 25.4 Use Case Diagram – Registration Module



Increasingly, local, state, tribal, and federal governments are passing statutes that require registration of convicted offenders. Figure 25.4 describes the flow of information between the officer and the registration module. These statutes require offenders that have been charged or convicted of a wide variety of statutes including sex crimes, gang membership, and other felonies to register with the authorized authority. These registrations place an increasing demand on organizations that have been mandated to manage and maintain these databases typically law enforcement.

The RMS should provide a mechanism to add and update any type of mandatory registration. Because many of these registrations must be updated on a regular basis, the RMS should automatically alert law enforcement personnel if registrants fail to comply with the recurring registration requirement. The RMS should also automatically perform a cross-check of the current residence of the registrant with the list of restricted addresses such as schools, day care facilities, etc.

Using These Functional Specifications For RMS

The Standard Functional Specifications for Law Enforcement RMS, Version II, are meant to describe the minimal amount of functionality that an RMS for law enforcement should contain. These specifications should be used as a starting point for law enforcement agencies to build a fully functional RMS, based on agency needs and open standards, to efficiently interface and share information with other systems, both internally and externally. They are designed to serve as a guiding tool and should be tailored to fit the specific needs of each agency or group of agencies looking to upgrade or purchase a new RMS. Although the Standard Functional Specifications for Law Enforcement RMS, Version II, were not developed to substitute for an RFP, they can be used to supplement an RFP.

The business functions described in this document are intended to be generic in nature and do not favor one particular system or approach over another. They are at the functional level, meaning that they define what is to be accomplished versus how it should be accomplished.

The Standard Functional Specifications for Law Enforcement RMS, Version II, were developed by the LEITSC RMS Functional Standards Committee, composed of law enforcement practitioners and industry experts, and are now available to all law enforcement agencies.

For questions, inquiries, training, and technical assistance, please visit www.leitsc.org or contact us at leitsc@theiacp.org.

Appendixes

List of Acronyms

AFIS	Automated Fingerprint Identification System
BJA	Bureau of Justice Assistance
CAD	Computer Aided Dispatch system
CFS	Call For Service
DMV	Department of Motor Vehicles
DNA	Deoxyribonucleic Acid
DOJ	United States Department of Justice
DOT	United States Department of Transportation
DUI	Driving Under the Influence
EFTS	Electronic Fingerprint Transmission System
FBI	Federal Bureau of Investigation
GIS	Geographical Information System
GJXDM	Global Justice XML Data Model
HIPPA	Health Insurance Privacy and Portability Act
IA	Internal Affairs
IACP	International Association of Chiefs of Police
IAFIS	Integrated Automated Fingerprint Identification System, an FBI system
IEPD	Information Exchange Package Document
ISE	Information Sharing Environment
IJIS	Integrated Justice Information Systems Institute
JDBC	Java Data Base Connectivity
JMS	Jail Management System
JRA	Justice Reference Architecture
LEITSC	Law Enforcement Information Technology Standards Council
LEO	Law Enforcement Online, an FBI system
MLI	Master Location Index
MNI	Master Name Index
MOI	Master Organization Index
MPI	Master Property Index
MVI	Master Vehicle Index
N-DEx	National Data Exchange, an FBI System
NCIC	National Crime Information Center
NIBRS	National Incident-Based Reporting System
NIEM	National Information Exchange Model
NIJ	National Institute of Justice
NIST	National Institute of Standards and Technology
NMVTIS	National Motor Vehicle Title Information System
NOBLE	National Organization of Black Law Enforcement Executives
NSA	National Sheriffs' Association
OAN	Owner Applied Number
OASIS	Organization for the Advancement of Structured Information Standards
ODBC	Open Data Base Connectivity
OJP	Office of Justice Programs
ORI	Originating Agency Identifier

PERF	Police Executive Research Forum
PII	Personally Identifiable Information
RFID	Radio Frequency Identification
RFP	Request for Proposal
RISS	Regional Information Sharing Systems
RMS	Records Management System
SaaS	Software as a Service
SAR	Suspicious Activity Report
SID	State Identification Number
SOA	Service Oriented Architecture
SOP	Standard Operating Procedure
UCR	Uniform Crime Reporting
VIN	Vehicle Identification Number
XML	eXtensible Markup Language

Glossary

Crash Reporting: Module within RMS. Emphasizes the cause of the crash; weather, visibility, road surface conditions at time of incident, and location.

Ad Hoc Reporting: Custom analysis and operational reports that are created when not provided by the RMS standard system.

Administrative Analysis: Provides information to support administrative decisions related to resource allocation and to support budget requests and decisions.

Aggregate Reporting: A sum of all reporting that allows law enforcement personnel to associate information in a variety of ways.

Analytical Support: The systematic process of collecting, collating, analyzing, and disseminating timely, accurate, and useful information that describes patterns, trends, problems, and potential suspects.

Arrest: To take someone into custody.

Assignment: Portion of module that records the officer assignment, shift, location, and associates with a particular pattern.

Automated Fingerprint Identification System (AFIS): A system to match unknown fingerprints against a database of known fingerprints. Used in many countries for multiple reasons.

Background Investigation: Investigation into an individual's background to authenticate information given and to verify eligibility for permit, license, system, etc.

Billing: Total amount of the cost for fees, goods, and services (etc.) to an individual or organization.

Booking: Collecting all relevant information on the subject and their arrest details, verifying the subject's identity, and addressing obvious physical or mental health needs.

Bureau of Justice Assistance (BJA): A component of the Office of Justice Programs, U.S. Department of Justice, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. BJA provides leadership and services in grant administration and criminal justice policy development to support local, state, and tribal justice strategies to achieve safer communities.

CAD Interfaces: Functionality to exchange and transfer data from CAD to RMS or other systems.

Call for Service (CFS): Call for service from an internal or external source.

Cancel Warrant: The ability of the court to cancel a warrant.

Case Disposition: The point at which a case has been completed and any property may be eligible for release to the owner.

Certification: Part of the personnel module that includes officer certification status; deadlines for maintaining certifications, including necessary hours of training (etc.), and student performance.

Charging: The process by which formal accusations are brought against a person or organization.

Citation: Individuals or organizations charged with minor offenses often are issued a citation or ticket, which requires them to pay a fine, post a bail, and/or appear in court on a specified date. Commonly used in traffic and misdemeanor law enforcement.

Civil Process: The law enforcement agency responsibility to serve legal papers and execute legal process as required to facilitate due process through the judicial system.

Computer Aided Dispatch (CAD): A computer system that assists 911 operators and dispatch personnel in handling and prioritizing calls.

Damage Reporting: Record of vehicle condition and damage.

Data Management: Involves record expungement and sealing, data redaction, data dictionary.

Driving Under the Influence (DUI): The act of operating a motor vehicle after having consumed alcohol or other drugs, to the degree that mental and motor skills are impaired.

DUI Arrest: An arrest for driving under the influence of drugs or alcohol.

Duty Roster: A list based on scheduling rotation, assignment, and exception information generated for a particular time period of duty.

Electronic Fingerprint Transmission Specification: A standard developed by the FBI in conjunction with the National Institute of Standards and Technology (NIST) for electronically encoding and transmitting fingerprint images.

Equipment and Asset Management: The processes that a law enforcement agency uses to record the receipt of equipment, record the source of the equipment, issue equipment to an organizational element of individual, and track equipment check-in or checkout.

Evidence: Things which help form conclusions or proves or disproves something.

Evidence Disposition: Procedures for the release of evidence from the system.

Evidence Storage: Movement of property that is recorded to ensure that an accurate log of the activity is captured and all policies and chain-of-custody rules are followed.

eXtensible Markup Language (XML): A free, open standard, general purpose mark-up language to facilitate the exchange of information between information systems.

External Exchange: An information exchange with other organization outside of the law enforcement agency. *See Internal Exchange.*

Federal Interfaces: Functionality that allows an RMS to query, add, or modify information stored in federal systems (e.g., updates for wanted persons, missing persons, and stolen vehicles/property).

Field Contact: Record created by a law enforcement officer based on the department's standard operating procedure – typically triggered by unusual or suspicious circumstances or any activity that is considered by the law enforcement officer to be of interest but would not otherwise be documented in the RMS.

Fleet Disposal: RMS module that deals with the process associated with taking a vehicle out of service and disposing of it.

Fleet Issuance: Tracking events related to fleet asset issuance and where the fleet is assigned.

Fleet Maintenance: RMS module that records information about vehicle maintenance and service.

Fleet Management: Encompasses tracking and issuance of fleet assets, tracking service and maintenance schedules and history, parts inventory and warranties, fuel and oil inventories and usage, and vehicle disposition.

Fleet Receipt: RMS module that captures vehicle information (such as descriptive physical characteristics, date vehicle was deployed, starting mileage, and identifiers such as the VIN and license plate number as well as any agency-specific unique identifier) and establishes the service schedule.

Forecasting Analysis: A combination of tactical, strategic, and administrative analysis; merging multiple sets of data.

Fuel Log: Records the date, price, and amount of fuel purchased at each fill-up, as well as the vehicle's mileage at the time of fill-up.

Geofile Maintenance: Ensuring that the geofile is current and that all functions remain in proper working order.

Geographic Information System (GIS): A system that captures, stores, analyzes, and manages data and its associated attributes which are spatially referenced to the earth.

Global Justice XML Data Model (Global JXDM): Data reference model for the exchange of information within the justice and public safety communities (http://www.it.ojp.gov/jxdm/). The GJXDM has been replaced by the National Information Exchange Model (NIEM).

Internal Affairs Investigation: Conducted in a similar manner to criminal investigations.

Incident Reporting: The function of capturing, processing, and storing detailed information on all law enforcement-related events handled by the department, including both criminal and noncriminal events.

Information Exchange Package Documentation (IEPD): A set of documents and technical artifacts based on NIEM that defines how information that is exchanged between multiple systems will be organized.

Initial Incident Report: A report prepared soon after an incident and contains factual information pertaining to the incident as well as narrative information.

Integrated Automated Fingerprint Identification System (IAFIS): A database managed by the FBI of all fingerprint sets (ten prints) collected in the U.S.

Internal Affairs: Ensures that department policy and procedures are followed and that agency standards of professionalism are adhered to by all department employees.

Internal Exchange: These exchanges occur within a law enforcement organization either between the modules of an RMS or between the RMS and other departmental systems. *See External Exchange.*

Investigative Case Management: RMS function that maintains all information in investigations and includes capturing and storing investigative data, warrant requests, conducting photo lineups and interviews, and producing supplemental reports.

Issue Citation Module: Allows an officer issuing a citation to query state and local databases that contain information regarding previously issued citations and warnings.

Jail Management System: A software system designed to collect, store, and retrieve essential information on individual inmates incarcerated in a jail.

Juvenile Contact: Law enforcement contact with a person under the age of adulthood as defined by the state.

Juvenile Detention: Custodial facility exclusively for juveniles.

Juvenile Referral: Recourse of action if circumstances warrant more than an admonishment as decided by the law enforcement officer or mandated by law.

Law Enforcement Information Technology Standards Council (LEITSC): Consisting of the four most prominent law enforcement organizations, the International Association of Chiefs of Police, National Organization of Black Law Enforcement Executives, National Sheriffs' Association, and the Police Executive Research Forum; together, participants from these organizations represent the law enforcement community as a whole on technology standards-related issues.

Licenses: An official governmental, written order (writ, certificate, tag, etc.) granting permission, generally for an extended period of time.

Local Interfaces: Functionality that allows RMS users to access and update a variety of local systems (e.g. courts, prosecutor, financial systems, Jail Management Systems, human resources systems, and multi-jurisdictional information systems).

Mobile Data Computer: A mobile computer that allows law enforcement officials to interface with department systems while in the field, usually found in law enforcement vehicles.

Master Location Index (MLI): Provides a means to aggregate information throughout the RMS based on a specific address, a range of addresses, an area (i.e., as define in the agency geofile), and/or other locations based on latitude/longitude/altitude coordinates.

Master Name Index (MNI): Links an individual master name record to every event in which the individual was involved or associated.

Master Organization Index (MOI): A detailed, searchable store of information about organizations (e.g., gangs, business, school, shopping centers).

Master Property Index (MPI): Links all property records entered into the RMS.

Master Vehicle Index (MVI): A detailed, searchable store of information about vehicles involved directly or indirectly with events.

Module: An independent portion of an RMS software application which provides specific functionality, e.g., Arrest and Booking. Each module performs those procedures related to a specific process within a software package. Modules are normally separately compiled and linked together to build a software system. Single modules within the application can normally be modified without requiring change to other modules so long as requisite inputs and outputs of the modified module are maintained.

National Crime Information Center (NCIC): A nationwide, computerized information system established as a service to all criminal justice agencies, local, state, and federal.

National Data Exchange (N-DEx): An incident- and case-based information sharing system managed by the FBI for local, state, tribal, and federal law enforcement agencies. It securely collects and processes crime data in support of the investigative and analytical process and will provide law enforcement agencies with strategic and tactical capabilities on a national scale. www.fbi.gov

National Incident-Based Reporting System (NIBRS): NIBRS is an incident-based reporting system that collects data on each single incident and arrest within the 22 offense categories that are made up of 46 specific crimes called Group A offenses and arrest date for Group B. (UCR Handbook, NIBRS Edition, pp. 1-2).

National Information Exchange Model (NIEM): A common vocabulary that can be used by software developers to facilitate communication between information systems. www.niem.gov.

National Protection Order Registry (NPOR): A registry of protection and restraining orders within the NCIC that all states can access.

Open Database Connectivity (ODBC): Provides a standard software application programming interface (API) method for database management systems making them independent of programming languages, database, and operating systems.

Operations Management: Organization and management of basic and essential business functions.

Originating Agency Identifier (ORI): An identifier that allows uniquely identifies an agency and allows them to access information.

Pawn: Something that has been given as a security for a loan, a pledge of guarantee or as a deposit.

Permits: An official, written order granting permission, generally for a shorter and specific period of time.

Personnel: All employed persons within a place of work.

Personnel Information: A person's basic information (e.g., emergency contacts, address and contact information, training history, certifications, education, etc.)

Property: Refers to any tangible item that can be owned, consumed, or otherwise used (e.g., stolen or recovered items, currency, vehicles, narcotics, animals, and evidence of any form) that is to be tracked by the agency.

Property Disposition: Procedures for the release of property from the system.

Property Storage: Movement of property that is recorded to ensure that an accurate log of the activity is captured and all policies and chain-of-custody rules are followed.

Protection and Restraining Orders: A civil order issued by the court to order a person to cease contact with a person, to stay away, or to stop harming (etc.).

Query: A query occurs when search criteria is transmitted to an external source and search results are returned to the system originating the query. Note that these are not considered exchanges because information from the query is not used to update the RMS database.

Radio Frequency Identification Device (RFID): Tags or transponders that can be attached to or inserted into anything and automatically identify the item or subject by remotely receiving stored data.

Records Management System (RMS): Stores computerized records of crime incident reports and other data.

Regional Information Sharing System (RISS): A national network comprised of six multi-state centers.

Regional Interfaces: Functionality that allows RMS users to access and update a variety of regional systems (e.g. courts, prosecutor, financial systems, Jail Management Systems, human resources systems and multi-jurisdictional information systems).

Regional Pawn Reporting: An external repository maintaining pawn data to which local pawn modules may be transmitted electronically.

Release: When a subject is released from custody and bond money collect.

Reporting Area: The smallest unit of geographical aggregation, agencies generally try to not have division lines that segment these. Typically, an agency will aggregate these into reporting sectors.

Request for Proposal (RFP): A bidding process where an invitation is given to service providers to submit a proposal on a specific product or service.

RMS Administration: Encompasses a wide array of general functions that law enforcement agencies need from their RMS to be able to create and query information effectively, ensure appropriate access, and ensure effective departmental information, image and document management.

RMS Configuration: Ensuring that some functions and parameters of a RMS are configurable by the system administrator.

RMS Interfaces: Functionality to exchange and transfer data from RMS to other systems. See *Information Exchange Package Documentation.*

RMS Reports: Documents officer and agency-wide activity or performance in a given area.

RMS Table Management: The ability of the user agency to define and maintain codes and associated literals for as many data elements as possible.

Scheduling: Portion of module that allows for the creation and maintenance of schedule patterns (e.g., days on, days off, and assigned hours).

Security: Protection or guard against unwanted intrusion, crime, sabotage etc.

Seize Pawn Property: Taking pawned property that has been identified as stolen into custody for evidentiary or safekeeping purposes.

Seized Property: The process and action of seizing personal property, based on a court order presented to a law enforcement officer.

Serve Orders: Process of serving orders (based on court order or subpoenas, and also includes evictions) to an individual, organizations, or other justice officials.

Standard Operating Procedure (SOP): Set of defined standards that are used to perform a given task.

Standardized Reporting: A set of standardized reports contained in each of module of an RMS.

State Identification Number (SID): A unique numeric or alpha-numeric identifier that is assigned to a person by a state's central criminal history repository upon receipt of the subject's first arrest fingerprint card. All subsequent arrest fingerprint cards received by the repository for that subject (as verified by the fingerprint searching of, and matching by, an Automated Fingerprint Identification System (AFIS) or by the comparison of the subsequent prints with the original prints by a fingerprint technician) will be associated with that unique SID.

State Interfaces: Functionality that allows a RMS to query, add, or modify information store in state systems (e.g., updates for wanted persons, missing persons, stolen vehicles/property, and state sex offender registries).

State Pawn Reporting: An external repository maintaining pawn data to which local pawn modules may be transmitted electronically.

Strategic Analysis: Provides information concerning long-range crime problems (e.g., crime rate variations, geographic, economic, social, and/or other types of general information).

Subject: Person in question.

Supplemental Report: Used to add new information to the case after the initial incident report has been submitted and approved.

Suspension-Revocation: When a license or permit is taken away.

Tactical Analysis: Provides information to assist operations personnel in the identification of specific policing problems and the arrest of criminal offenders.

Traffic Crash Reporting: The documentation of facts surrounding an accident. Typically, these are incidents that involve one or more motor vehicles but may also include pedestrians, cyclists, animals, or other objects.

Training: Instruction and education

Uniform Crime Reporting (UCR): The UCR Program is a voluntary city, county, state, tribal, and federal law enforcement program that provides a nationwide view of crime based on the submission of statistics by law enforcement agencies throughout the country. www.fbi.gov

Vehicle Identification Number (VIN): Used to uniquely identify a vehicle.

Vehicle Impound: The seizing or taking into custody of a vehicle (e.g. cars, motorcycles, boats, or any other item that can be used for transportation) during the normal course of operation, as evidence or because it has been abandoned or because it was parked in a prohibited location.

Verify Warrant: A process that an officer must complete to verify that the warrant is still valid prior to serving.

Warrant: An order of a court that directs a law enforcement officer to take specific action.

End notes

[i] http://www.it.ojp.gov/topic.jsp?topic_id=43
[ii] http://www.niem.gov/
[iii] http://www.nist.gov/
[iv] http://www.it.ojp.gov/topic.jsp?topic_id=242
[v] http://www.it.ojp.gov/topic.jsp?topic_id=55
[vi] http://www.it.ojp.gov/topic.jsp?topic_id=209