IJIS Institute

STANDARD FUNCTIONAL SPECIFICATIONS FOR LAW ENFORCEMENT RECORDS MANAGEMENT SYSTEMS VERSION III

Prepared by the Joint RMS Standardization Task Force

ACKNOWLEDGEMENTS

Following a great deal of commitment and effort by multiple contributors, the Law Enforcement Records Management Systems (RMS) Functional Specifications document has been successfully updated! As a joint effort by the Integrated Justice Information Systems (IJIS) Institute Law Enforcement Advisory Committee (LEAC) and the International Association of Chiefs of Police (IACP) Criminal Justice Information Systems (CJIS) Committee, the work represents an extraordinary collaboration between both justice practitioners and industry partners. Thank you all for your commitment, time, energy, and patience.

RECORDS MANAGEMENT SYSTEMS (RMS) STANDARDS TASK FORCE

The following lists the law enforcement technology practitioners, subject matter experts, and industry representatives who volunteered their time for over 18 months to update this important document.

Catherine A. Miller, Chair
Program Manager, National Capital Region Law Enforcement Information Exchange (NCR-LInX)
Montgomery County, MD, Police Department

Todd Thompson, Co-Chair & Team Lead
Vice President, Strategic Development
Caliber Public Safety

TEAM LEADS

Jason Bussert
Captain, Information Technology
Oklahoma City Police Department

Crystal Cody
Public Safety Technology Director
City of Charlotte—Innovation and Technology

Brian Parker
Sergeant, Justice Information Bureau
New Hampshire State Police

Melissa J. Winesburg, PhD
Director of Programs
IJIS Institute
Formerly with Optimum Technology

TASK FORCE MEMBERS

Mike Bell, Houston, TX Police Department
Ben Buller, Arizona Department of Public Safety
Jana Colwell and Cher Her, Adams County, CO Sheriff's Office
Kyle W. Comer, J.D., Missouri State Highway Patrol
Jonathan Lewin (Ret.), Chicago, IL Police Department
Dan Mahoney, Northern California Regional Intelligence Center
Flor Mayr and Michael Koontz, Mark 43
Dan Murray, Arlington County, VA Police Department
Robert Oesch, Axon Enterprises
Jim Olthaus, Cincinnati, OH Police Department
Ed Posey, University of Florida Police Department
Shawn Rehill, Edmonton Police Service (Canada)
Corey Roberts, Motorola Solutions
Jed Stone, Issured (United Kingdom)

TASK FORCE LIAISONS/ADVISORS

Bonnie Locke, Chief Marketing Officer, International Justice and Public Safety Network (Nlets)
Robert Turner, President, Commsys and Chair, IJIS Institute Law Enforcement Advisory Committee
Joe Heaps, Senior Physical Scientist, DOJ National Institute of Justice (NIJ)
William Ford, Senior Science Advisor, DOJ National Institute of Justice (NIJ)

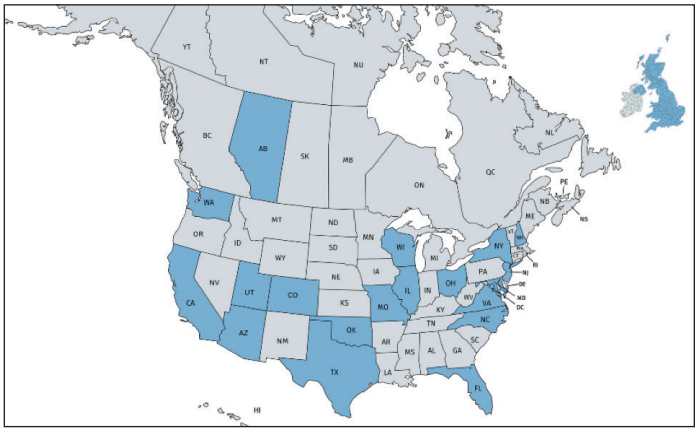
PUBLISHED APRIL 2021

SPECIAL RECOGNITION

This document represents an extraordinary collaboration between both justice practitioners and industry partners. The RMS Task Force would like to recognize both Bonnie Locke and Bob Turner for working with their respective IACP and IJIS committees to identify practitioners and industry partners who were willing to commit time to work on updating this document.

Additionally, we appreciate the leadership provided by RMS Task Force Chair, Catherine Miller and Co-Chair, Todd Thompson, who were both instrumental to the success of this effort. Further, we appreciate the support of the IJIS Institute for their contribution to underwrite the publication of this report. The IJIS team, including Executive Director Maria Cardiellos, Director of Programs Melissa Winesburg, and Communications Specialist Alex McAdoo, spent many hours managing the comments provided by the RMS Task Force teams and helping to facilitate working group sessions.

Special recognition is given to the Optimum Technology team including Melissa Winesburg and Shelby Craft for volunteering to organize the comments received from the teams for review and consolidation. Finally, the efforts of the RedFlash Group in the production of the final report contributed significantly to the realization of this valuable publication.



The RMS Task Force is comprised of law enforcement technology practitioners, subject matter experts, and industry representatives from across the country.

EXECUTIVE SUMMARY

HISTORY

The IACP CJIS Committee and the IJIS Institute Law Enforcement Advisory Committee (LEAC) has worked together to update the Law Enforcement Records Management System (RMS) Functional Specification Standards Document. Formed in the spring of 2019, the RMS Standards Task Force spent many months reviewing the Law Enforcement Information Technology Standards Council (LEITSC) RMS functional specifications documents that were produced over 10 years ago. LEITSC released Version I in June 2006 and, in 2009, an updated Version II was completed. These two versions were supported by many federal government and national organizations. LEITSC disbanded so the document had not been updated since 2009.

PURPOSE

There have been many technological advancements and changes in law enforcement record keeping practices since 2009. In 2019, the IACP CJIS Committee and the IJIS LEAC identified the need to revise previous versions of the standard functional specifications for law enforcement 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 RFPs.
- Streamline the process and lower the cost of implementing and maintaining an RMS.
- Promote information sharing and best practices.

The baseline document was developed from common elements found in RFPs, technical documentation, and other RMS-related research. These documents are still important to law enforcement and the software providers that deliver RMS solutions. However, the documents have shown their age and were in need of updating to include the latest technological advancements. The goals of the RMS Standards Task Force were to assess the state of the previous RMS standards documents, work collectively to revise the contents to become more current, and most importantly, retain their relevancy to the greater law enforcement community.

The initial objective of the task force was to provide an assessment of the state of the documents, and that has been achieved. In this assessment, the task force highlighted areas of the document that are still relevant and areas that need significant updating and improvement. Care has been taken to address compatibility with the National Crime Statistics Exchange (NCS-X); National Incident-Based Reporting System (NIBRS); local, regional, state, and federal information sharing; cloud-hosted environments; and interoperability with other platforms (i.e. citations to courts systems). Public safety records management systems are mission critical to every law enforcement agency and other stakeholders in the community.

Previous versions of the standards were compiled and published with hundreds of thousands of dollars in grant funds. This new version of the RMS standards has been developed in large part thanks to numerous volunteer hours from law enforcement and industry partners. The work was also partially funded by the IJIS Institute working with the task force to update existing content and develop new content. The IJIS Institute also worked with the RedFlash Group to complete the final editing, graphics, and layout work to publish the final product.

These specifications are intended to be generic in nature and do not favor one system 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 a substitute for an RFP. The specifications 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. Although the Standard Functional Specifications provided within this publication were not meant to replace an RFP, they can be used to supplement and guide the development of an RFP.

These specifications are intended to be used in conjunction with other technical standards such as the National Information Exchange Model (NIEM[1]) and International law enforcement technical standards such as the United Kingdom's Management of Police Information (MoPI) Standards to streamline the process of sharing information.

For questions, inquiries, training, and technical assistance, please visit IJIS.org or contact us at info@ijis.org.

INTRODUCTION

A records management system is an agency-wide system that provides for the storage, retrieval, retention, manipulation, archival, and viewing of information, records, documents, or files pertaining to law enforcement operations. It serves as the agency system of record for most policing activities.

An 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, an 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. An 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.

The 2021 Version of the Standard Functional Specifications for Law Enforcement RMS builds upon the past two versions to include necessary modifications to the business functions and adds several new features to bring this document up to date. This version has also been reorganized to address the core RMS business functions and then optional RMS business functions in the later chapters.

Chapter 1: General Recommendations

Chapter 2: Master Indices

Chapter 3: Calls for Service

Chapter 4: Incident Reporting

Chapter 5: Investigative Case Management

Chapter 6: Property and Evidence

Chapter 7: Warrant

Chapter 8: Arrest

Chapter 9: Juvenile Contact

Chapter 10: Field Contact

Chapter 11: Equipment and Asset Management

Chapter 12: Analytical Support

Chapter 13: RMS Reports

Chapter 14: RMS System Administration

Chapter 15: RMS Interfaces

OPTIONAL

Chapter 16: Booking

Chapter 17: Crash Reporting

Chapter 18: Citation

Chapter 19: Pawn

Chapter 20: Civil Process

Chapter 21: Protection Orders and Restraints

Chapter 22: Permits and Licenses

Chapter 23: Fleet Management

Chapter 24: Personnel

Chapter 25: Internal Affairs

Chapter 26: Registrations

Chapter 27: Conclusions

[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 the Global Justice XML Data Model (GJXDM) to become one of the many domains incorporated into NIEM. In October 2010, the U.S. Department of Health and Human Services joined as the third steward of NIEM. In 2019, the FBI initiated the development of the Next Generation NCIC (N3G), which will improve, modernize, and expand this cornerstone technology.*

TABLE OF CONTENTS

TABLE OF CONTENTS
CONTINUED

TABLE OF CONTENTS
CONTINUED

TABLE OF CONTENTS
CONTINUED

CHAPTER 1 | GENERAL RECOMMENDATIONS

A Records Management System is critical to law enforcement operations. It serves as the system of record for documenting, managing, and retrieving records of daily activities. The RMS and the data contained within the system provide critical analytical information about crime and agency operations that is used for decision-making, resource allocation, and crime prevention. An RMS is important for all law enforcement agencies—urban, suburban, and rural regardless of size or type of organization.

This document serves to provoke thought and careful consideration of law enforcement needs and requirements for an RMS. Local, state, tribal, and national standards and policies should be considered when implementing a system. It is important that both law enforcement and RMS service providers understand the impact these policies may have on the RMS as they vary from agency to agency. All chapters are organized by "core" and "optional" modules. Core modules are those that are necessary for most law enforcement agencies to manage day-to-day operations. Optional modules may be required based on functionality that is specific to certain types of law enforcement organizations. However, it is important to remember that each agency may have different needs based upon size, functional responsibility and jurisdiction type.

***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
- 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.
- All exchanges generated by an RMS should be in conformance with NIEM standards.

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 2019, The FBI initiated the development of the Next Generation NCIC (N3G), which will improve, modernize, and expand the 50-plus-year-old NCIC system.

In addition, an 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 criminal justice standards, using NIEM[i], NIBRS, NCIC, and those developed by the National Institute of Standards and Technology (NIST)[ii], including the Electronic Fingerprint Transmission Specification (EFTS) and facial recognition collection standards.

Open Architectures

When considering an RMS, it is important to understand the required interfaces whether internal or external and to evaluate the capability of the RMS to connect with other systems in a secure, reliable, and repeatable way. Open architectures are critical to facilitating the sharing of information across systems and become very important when considering the number of different systems an RMS should connect to (i.e. CAD, jail management systems, other local, regional, state and national systems). Service-oriented architectures (SOA) and Application Programming Interfaces (APIs) support the need for this digital transformation and data sharing. Service-oriented architecture (SOA) is a best practice that supports de-coupling of applications and reuse of common services so that systems can operate independently where appropriate. SOA typically uses SOAP and XML services. APIs are considered more open and mobile friendly and they are typically associated with REST/JSON. Regardless of the option chosen, it is important to remember that resources have to be allocated to manage and audit both approaches.

The Global Justice Reference Architecture (JRA)[iii] provides a framework that defines the most relevant aspects of a highly adaptive justice system SOA. 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 service providers should consider the architecture in their own software development efforts to understand where their RMS solutions fit into this bigger picture. The RMS service providers should address how they might expose functionality currently embedded within their RMS to facilitate implementation of a JRA-based architecture in a jurisdiction.

Implementation Models

Overall, there are two primary implementation models for an RMS. These include on-premises solutions and software as a service (SaaS) solutions. The principles of each are described below. Regardless of the model chosen, the law enforcement agency should ensure that the data is owned by the agency and that the RMS contract includes a transition plan should the agency decide to switch service providers. Law enforcement agencies should consider requiring source code to be placed in escrow or another secure location in the event the service provider decides to no longer conduct business.

On-Premises Solutions

On-premises solutions can be defined by the following principles:

- The software is hosted on an organization's own server, desktop, and network infrastructure.
- The organization is responsible for the daily operation of the system. This includes software updates, patches and security fixes, database maintenance, etc.
- The organization is responsible for the storage of data held within the system, including back-ups and disaster recovery.
- The software can only be accessed with devices that are approved to connect with the organization's network infrastructure.
- Agencies have full access to their back-end data and can connect other reporting tools or conduct analysis as required.

On-premises software solutions, depending on the scale of the system, can take longer to implement. Due to the nature of the on-premises solution, an organization must consider the skillset and cost of specialized information technology staff to support and maintain the solution. Feature and function updates to an on-premises system can be slower to deploy and adopt due to the nature of the system being more isolated within an organization as opposed to a SaaS model.

While on-premises solutions are often preferred within government, due to the perception that data is more secure, they can often be prone to higher levels of risk as the organization itself is responsible for keeping pace with emerging cyber threats and security vulnerabilities through patching and applying security fixes. On occasion, these can be missed if the IT support services within the organization do not have sufficient resources or skills to properly identify all threats and apply the appropriate counter measures. However, on premises solutions allow the organization to apply their own controls.

Software as a Service (SaaS)

Software as a Service can be defined by the following principles:

- The software allows data to be accessed from any device with an Internet connection and web browser.
- Service Providers host and maintain the servers, databases, and code that makes up the application
- SaaS solutions usually provide just one version of code, but the solution is customizable to accommodate an organization's required branding, etc.

A core principle of SaaS solutions is that the solution will be cloud hosted. Cloud hosting of the application and its data can provide the benefit of greater remote accessibility and a greater opportunity to share information with other organizations.

Where data is hosted within the cloud, any SaaS solutions should meet the standards defined within the FBI Criminal Justice Information Services (CJIS) Security Policy. International organizations will also have their own policies and standards such as the UK's National Industrial Security Programme (NISP).

SaaS solutions offer the ability for 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. These systems also make deployments simpler and eliminate the agency cost for hardware upgrades that are often required to maintain production systems. This type of implementation is beneficial to those agencies that do not have information technology trained staff to devote to issues of systems and network management.

SaaS-enabled RMS applications are typically hosted in a cloud environment or on the servers of the RMS service provider. The local agency then connects to the software application through a secured internet connection. The service typically involves a minimal up-front setup fee and an annual subscription fee.

Consideration should be given to potential challenges related to interfaces to a cloud solution. Interfaces from a cloud to on-premise solution need to consider security requirements of the agency and systems being

connected. Agencies that plan to conduct in-depth crime analysis should consider replicating the data in a local data warehouse given that back-end access to a cloud-hosted solution may not be permitted.

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 – Conditionally shared. System should provide the capability for data contributors to indicate specific elements or records types that may be shared.

Level 3 – Not shared. Silent hit sends back notice to originating agency that a record exists, but the 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 confidential informant, then data tagged as PII is not sharable."

Additional functionality that an 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[iv], Chapter 8 of the Fusion Center Guidelines[v] and the Automated Regional Justice Information System (ARJIS) site that includes useful privacy-related tools (www.arjis.org).

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. Also, as systems become more regional in nature, agency data sharing agreements will be key to the protection and security of information.

Data Quality

Ensuring data quality within an RMS becomes increasingly important as jurisdictions seek to electronically share 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. An RMS should leverage NCIC and NIBRS standardized code lists to the maximum extent possible. Furthermore, an RMS should implement some data quality validations based on context-sensitive business rules. NIBRS validations must be included within the application so that the report can be complete prior to submission for supervisor review. Other quality checks are necessary. For example, an arrest report might be required to contain an arrest identification number, arrest date, and arrest subject information. An interface that allows each service provider 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.

Mobile Technology

The RMS should provide the ability to capture reports anywhere in the field. If the RMS is not accessed directly from the field, mobile field reporting for certain modules should have direct access to the RMS. Service providers could even consider smart-phone applications (apps) that directly interface with the RMS. Minimally, technology should be device-responsive and allow users to enter data from any size screen. Mobile field reporting should allow multiple users to create reports and supplements at the same time. Simultaneous submission of supplements is critical to ensure rapid completion of reports.

Cross-Module Functionalities

There are certain functionalities that the RMS should support regardless of the module. Some of these functions are described below.

Configurability

As RMS continue to evolve, there are more opportunities to make features configurable so that agencies can customize the application to meet specific needs. The ability to hide fields, add additional data fields, and build output forms is highly desirable. The ability to configure incident and case numbering formats, determine how supplements will be used, setup property room locations, and add agency-specific domain values will be

considered as standard RMS requirements over time.

Attachments

Multiple types of attachments should be supported across all modules. These may include victim and witness statements, financial receipts, video, recordings, drawings, or other scanned documents. The RMS should allow the agency to clearly define document categories and ensure that documents can be clearly labeled to make them easy to find within the RMS. Minimally, attachment titles should be searchable.

Automated Notifications

Given the workload of law enforcement officers, the RMS should support multiple notification systems. Officers should be able to subscribe to certain events so that they can be notified when a specific location, individual, or vehicle is involved in an incident. Specific units such as the sexual assault unit should be notified when a sex offense occurs. The law enforcement administrator should have the ability to define notification types and recipients. Recipients may include law enforcement personnel, community residents, victims, etc.

Searchability

The information that law enforcement enters into the RMS should be searchable. The agency should be able to search on every data field entered and conduct cascading searches for information. Additionally, narratives should be searchable by keywords and phrases. The more flexibility that can be provided to search information contained in the agency's system of record, agency efficiencies will be improved.

Redaction/Printing

Printable reports should be available for all RMS modules. These reports should print with "unapproved" and "official copy" watermarks. In addition to the report, the RMS should provide the agency with the ability to print all corresponding supplements. Ideally, these supplements will print automatically in batch without the user being required to open each individual document. The RMS should generate both an official agency report version and a public report. The public version should be saved within the RMS and include a record of dissemination. Reports should also be available in a printable document format (PDF).

Auditing

Every action within the RMS should be audited. The system administrators must have the ability to review audit logs with ease. The audit log should include the action taken, the user who took action, date, time, and the specific action taken. If a change is made to a data field, the audit log should record the specific modification. Audit alerts may also be established for administrators to be notified for certain thresholds that may predict potential data misuse or the need for personnel training. The audit logs must be preserved in the database and users should not be able to delete information on the audit log. Permission for access to audit logs should be limited to administrators and key executives. Audit functions should ensure compliance with the FBI's Criminal Justice Information Services (CJIS) security policy as well as state and local information security policies.

Data Security

The RMS should meet local, state, and national security and compliance standards. All modules housed within a single product should be integrated with security rights defining access. Minimally, the RMS should adhere to the most recent version of the FBI CJIS Security Policy regarding user authentication, data access and dissemination, and data security in transit and at rest. Each state also has a state-level CJIS Security Officer (CSO) who may develop additional policy related to criminal justice data. The law enforcement agency should understand these policies as they relate to an RMS and ensure they are implemented in the RMS. The solution must also follow other security protocols such as the Driver's Privacy Protection Act (DPPA), 28 CFR Part 20, and 28 CFR Part 23, and any state-level laws related to PII and Criminal History Record Information (CHRI), and the Health Insurance Portability and Accountability Act (HIPAA). As new laws and regulations arise, it is important for law enforcement and RMS service providers to be aware of these requirements. There are other standards that exist on an international level such as the the MoPI guidance, the Data Protection Act (DPA), and the General Data Protection Regulation (GDPR).

As technology evolves, RMS continue to enhance efficiency in law enforcement recordkeeping, voice recognition, and agency-designed forms that allow for notifications, reports, and printing will soon become a standard for RMS solutions. These systems continue to become more flexible, allowing law enforcement to independently manage more functions, which result in increased efficiencies, enhanced data quality, and more cost-effective solutions.

[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.*

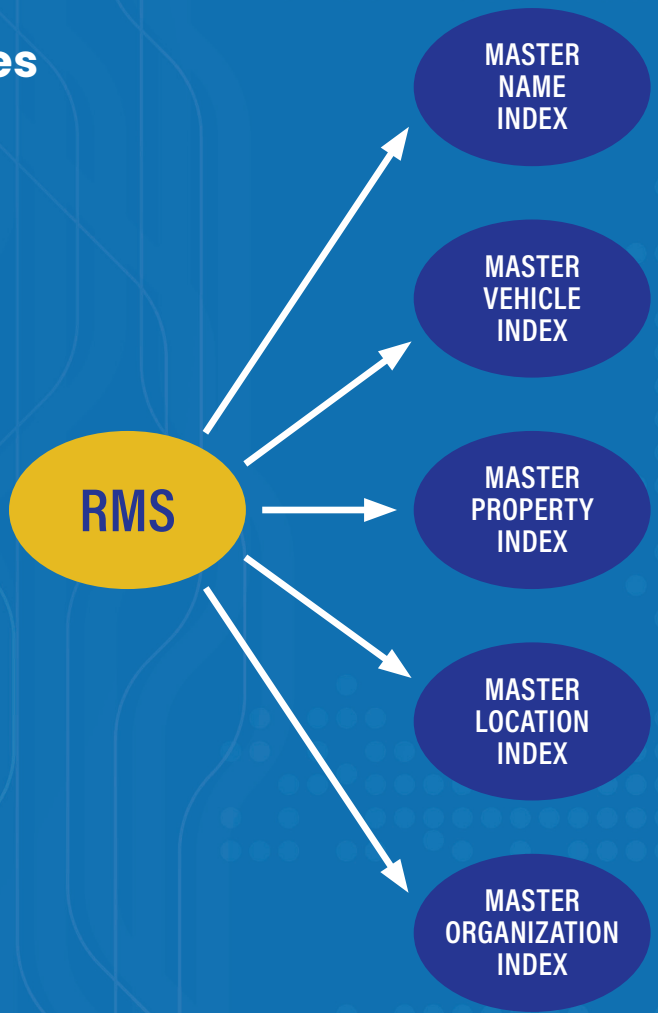
CHAPTER 2 | MASTER INDICES

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 should maintain a history of all items entered into the RMS on a subject, location, vehicle, or organization. This is an important consideration for tracking movements or changes in characteristics over time. The following are examples of items which may change over time: an individual's hair color, weight, eye color (contacts), or other physical characteristics and contact/location characteristics such as addresses and phone numbers, email addresses, social media handles, and business locations. Finally, license plate owners, vehicle owners, and colors may change on a vehicle. These are all important characteristics that a master index must have the ability to track over time.

Master indices' information is 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 give the user the option of determining whether there is a match based on existing

2.1 Master Indices Diagram



data. However, master indices should not allow updates from external systems. While it is critical to maintain master indices history, law enforcement agencies should be cautious of solutions that automatically combine master index information. There are many common names and an RMS may inadvertently combine unrelated information.

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 the RMS.

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

Additionally, a notification 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. For example, Trespass Warnings, prior Domestic Violence History and Violent or Mental Health History may be included in the RMS as notifications.

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., ARJIS, Law Enforcement Information Exchange Program (LInX), Texas Data Exchange (TDEx), Ohio Law Enforcement Gateway (OHLEG), and National Data Exchange (N-DEx))
- NCIC
- Nlets
- Computer-aided dispatch (CAD) system

Standard Internal Data Exchanges:

- Existing RMS data
- CAD system

2.2 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. The system should present possible matches to the user so that they can assess the need to create a new record, link to an existing record, and avoid the potential duplication of existing records. 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, gender, 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. Automatic matching should not replace the need of the user to assess possible matches and the user should only match one record to another when confident that they are the same entity.

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
- Contact details including: Landline, mobile, email, and social media handles
- 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 number, driver's license number, 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 historical information should be maintained, view-

able, and searchable.

Contact information (telephone numbers, email addresses, etc.) for a subject can be maintained within the MNI, but due to the prolific use of the internet and social media, consideration should be given to the creation of a Master Communication Index record type that can be linked to one or many locations or people. This can support the identification of contacts between subjects and aid in the ongoing investigations through identifying the user of a communication type, those subjects communicating with others through a communication type, or where the communication type is used by multiple subjects, etc.

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. Un-merge functionality should also provide the ability to unlink two records if it is determined the records should not have been linked.

2.3 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. Like Master Names, vehicle owners should be tracked over time. The MVI should provide a history of owners linked to a vehicle as well as license plate numbers and year and state of issue.

The RMS should provide the capability to search on:

- Vehicle Identification Number (VIN) or Owner Applied Number (OAN)
- License plate numbers
- License plate states
- License plate years
- Registered owners
- 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 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 and NIBRS property codes, should be used during the entry of property records into the 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 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. A master address file can be used to populate this index, which is often maintained by the city or county planning agency. 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).

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 the MLI.

2.6 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) as well as organizational floor plans.

All calls for service (CFS) are recorded in a structured records environment in a computer-aided dispatch system (CAD), 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. Some law enforcement agencies may utilize different CAD and RMS service providers. In this case, the systems should interface to ensure data is not reentered and seamlessly shared across the two systems.

Typically, data in this module cannot be modified after the call is closed because it serves 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, officer information, officer's assigned detail, reporting address, texts, pictures, videos, phone number, involved persons information, and associated

3.1 Calls for Service Diagram

incident number from the CAD system. It is important to make sure that all responding officers are transferred from CAD to RMS. This helps to ensure there is a record of all officers at the scene for quality checks related to completion of statements and evidence gathering. If the call does not originate from a CAD system, the 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.

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 date 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, en-route and 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

Standard Internal Data Exchanges:

- MNI
- Incident Reporting Module

3.2 NG911

NG911 allows 911 centers to receive, process and store text, pictures, and videos from citizens and should relay this information to first responders. It allows officers in the field to have live video feeds from the call for bank robberies or a picture of a missing child before they arrive on the scene.

3.3 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, and as the call data is updated in CAD.

3.4 TRANSFER RMS DATA TO CAD

CAD systems should be capable of receiving information from the RMS such as addresses of known gang members, wanted suspects, and recent violent arrest or domestic incidents to alert first responders who are dispatched to those addresses.

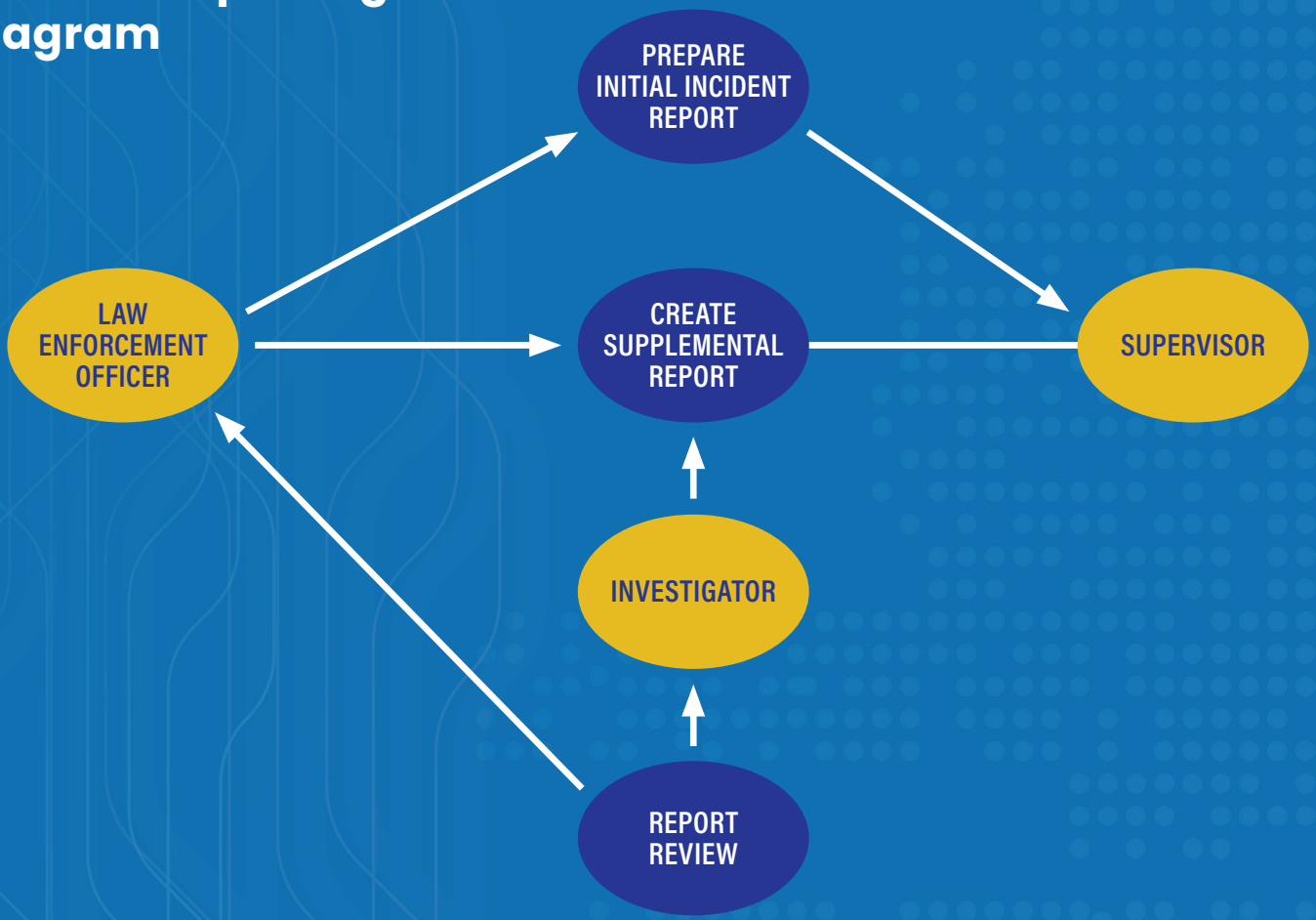
[3] *Workload is the metric or metrics that accurately describe the amount of work performed by, or within, a process in a specific period of time. For example, the CFS module contains information about the number of calls received and the length of time needed to process those calls. The data on time 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.*

CHAPTER 4 | INCIDENT REPORTING

Incident reporting is the function of capturing, processing, and storing detailed information on law enforcement-related events handled by the law enforcement agency, including both criminal and non-criminal events. The incident reporting function collects sufficient information to satisfy existing local, tribal, county, or state reporting requirements. The CFS record in the RMS or external CAD should be linked to the incident and easily accessible from the incident report.

Reporting standards such as the FBI Uniform Crime Reporting (UCR) Program's National Incident-Based Reporting System (NIBRS) must be implemented as a standard in the RMS. Consideration should be given to the incident-based reporting standards of each state UCR/ Incident-Based Reporting System (IBRS) Program. Every state maintains a state level incident-based reporting program, which forwards NIBRS data to the FBI. All state repositories should be compliant with the most recent version of the FBI's NIBRS XML Information Exchange Package Document (IEPd) and Web Services Specifications. The FBI's N-DEx program is another standard that should be considered within the RMS. N-DEx is an information sharing system that can be used for investigative purposes allowing agencies to search, link, and analyze data. There are regional and state information sharing systems (e.g. LInX, ARJIS, TDEx, OHLEG) that submit data to the FBI N-DEx program on behalf of multiple law enforcement agencies. These local and state standards should be considered for RMS implementation. It should be noted that international organizations will adhere to standards within their own countries/regions.

4.1 Incident Reporting Diagram



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 must provide the capability for a user to identify and mark sensitive information within an incident report or other RMS output. Marking the data in this way will trigger the system to redact the chosen information within the public copy that is either printed or published via the web. The public copy should be clearly marked as such and saved within the RMS. The information to be shared in a public report is determined by local, county, state, tribal and federal policy.

The RMS must provide sealing and expungement of records based upon the laws of each state. Generally, sealed records may be accessible to certain persons within an agency or organization. However, an expunged record is typically deleted. It is critical to consider that only one offense, suspect, or arrestee may be sealed or expunged in a multiple event incident. Redacting of information in the narrative must also be considered.

Certain reports may need to be locked or remain private and made accessible only to select individuals in an organization. These locked reports should not display in any search results for persons other than those with access to the report. The report must not be shared with external systems until such time that it is made accessible to the entire law enforcement agency.

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:

- 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
- State UCR NIBRS program
- Prosecutor
- Courts
- Jail management system
- State, regional, and national information sharing systems and networks [e.g., NIets, ARJIS, LInX, TDEx, OHLEG, Regional Information Sharing Systems (RISS), N-DEx, Information Sharing Environment (ISE)]
- Amber alert
- Mobile computing system
- Public facing website for reporting and viewing of crime statistics/reports

Standard Internal Data Exchanges:

- Investigative Case Management module
- Property and Evidence Management module

4.2 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.

An incident report contains factual information pertaining to the incident, including administrative information, offense information, property information, suspect information, and case status, as well as information pertaining to witnesses, victims, and complainants. Attachments such as photos, documents, and videos should be supported. These may include financial statements, witness statements, photos of victims and/or offenders, handwritten notes, etc.

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 sys-

tem 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. The RMS should automate the review process such that it routes the report through proper supervisor channels automatically. The RMS must allow the supervisor to reject the report and route it back to the reporting officer with notes explaining the reason for rejection. Records personnel may also reject a report and send it back to an officer for completion. Circumstances may also require an approved report to be reopened, corrected and resubmitted (i.e. an incorrect year on the report). All report activity should be tracked and audited.

4.3 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. The supplement process must support the ability to track changes in specific data elements in the original report and the addition of supplemental narratives. If supplemental information changes NIBRS required data, a process should be in place to update the information submitted to the state and FBI UCR Program. Law enforcement personnel shall electronically submit the supplement report to a supervisor for review and approval.

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 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. Locking of the initial incident report typically occurs upon supervisor approval. Any information added thereafter is provided as a supplement.

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 should provide the capability for a user to control whether the report can be shared with other law enforcement agencies (LEAs) or services. This will allow a department to control the dissemination of sensitive information outside of their control.

State and local data retention policies should be considered. Where possible, the RMS should produce reports of potential records that can be purged based upon the agency data retention policy.

The RMS should 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 before the report is finalized in the system. The RMS should support all required reviews and corrections prior to locking down the incident report.

Where possible, the RMS should provide an interface to allow the ingestion of incident/crime reports submitted through a public-facing website. The RMS should allow the submitted information to be automatically created as an incident report for authorized users to review the submission and allocate actions accordingly. Submission of volume crime reports will enable the public to transact with LEAs without placing additional demand on contact centers.

National Incident-Based Reporting System (NIBRS)

The Federal Bureau of Investigation sunsetted the Uniform Crime Reporting (UCR) Summary Reporting System (SRS) in January of 2021. All law enforcement agencies reporting crime data to the FBI UCR Program will submit the data in the National Incident-Based Reporting System (NIBRS) format. The traditional SRS program tallied data on crimes only in a summary format. NIBRS provides a detailed picture of administrative information, offenses, victims, offenders, property, suspects, and arrestees for each incident reported to law enforcement.

The RMS service provider and law enforcement must be aware of each states' requirements for NIBRS or incident-based reporting. Each state has established a state-level repository for collection of data and the state UCR/IBRS Program is responsible for submitting data from all law enforcement agencies within the state to the FBI. Law enforcement agencies and vendors should understand state level requirements and the version of the FBI NIBRS specification that is supported by the state program. Law enforcement agencies should consider adding language to contracts requiring NIBRS implementation and support. This support should require the service provider to upgrade to the new versions of State Program requirements at regular specified intervals.

NIBRS provides greater analytical capability for crime. Offenses and offense characteristics are reported with greater specificity and detail like property descriptions, expanded victim characteristics, relationships of victims to offenders, location details, and suspected drug and gang activity. The analytical capabilities are far superior to SRS reporting.

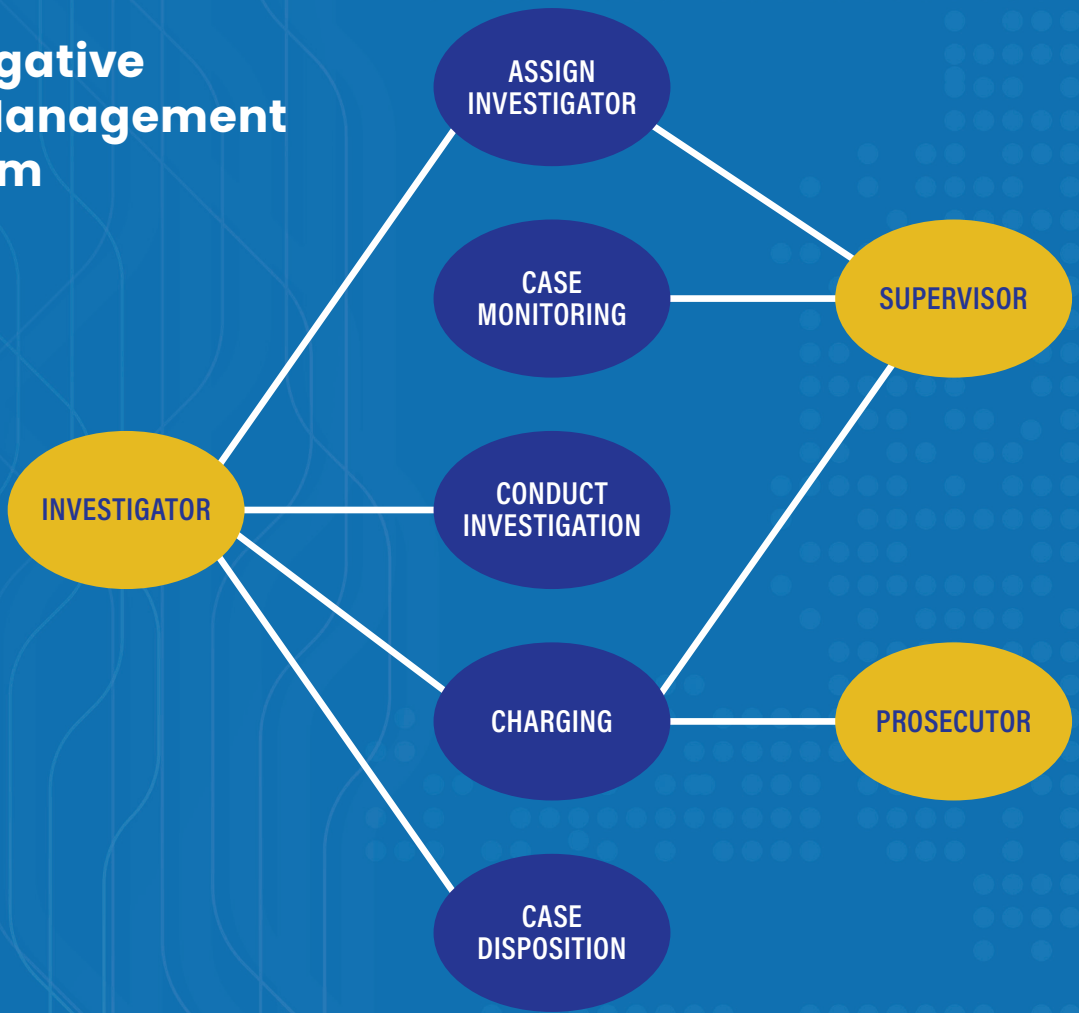
One of the key attributes to successful NIBRS reporting within the RMS is the data validations. The RMS must include all state and FBI validations and data warnings to ensure accurate reporting. NIBRS requires multiple levels of validation including validation at the screen level via mandatory field validations, pick list confirmations, and conditional mandatory fields. A conditional mandatory field occurs for example, when a property offense is entered. In this instance, property data becomes mandatory. There are also certain cross segment validations that must be included in the validation logic. For example, if an offense is an offense against society, the RMS must ensure that a Victim Type of society is collected. The RMS should validate incidents real-time and pre-submission to the state program. Records clerks and administrative personnel should have the ability to make data corrections prior to submission of the data to the state program.

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 RMS system should be able to assign case responsibility and task responsibility.

The RMS should be configurable to allow cases to be assigned to a specific unit based upon prescribed business rules such as offense type, victim age, etc. For example, homicide offenses should automatically route to a homicide unit or the assigned homicide detective. Typically, cases will be assigned at the unit level and then to an individual detective. The Case Management module should also include the ability to assign individual tasks for completion. The Case Management functions should include automated task reminders with due dates and follow-up tasks such as victim interviews, evidence collection, leads collection, expense tracking, preparation of case for prosecution, and other required tasks. Leads should be easily manageable and submitted electronically. A large case may involve hundreds of leads that need to be reviewed, followed up on, and cleared quickly.

Case investigations often involve multiple incidents. The Case Management module must allow for linking of multiple incidents to a single case. Additionally, when an arrest is made, the arrest of one individual should

5.1 Investigative Case Management Diagram



transfer to multiple incident reports to avoid duplication of effort and ensure data consistency.

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 notifications to both the assigned investigator and the supervisor.

The ability to assign, accept, and work on cases needs to be able to be completed by all officers, not just detectives. Minor crimes can be sent back to the original officer to work, or to a detective.

Key products of the process are producing information for the prosecutor, assisting in managing case materials (including evidence), and preparing cases for prosecution. Case dispositions are maintained by the prosecutor. This information will need to be manually entered by the law enforcement agency or automatically sent to the RMS case via an interface between the prosecutor case management system and the RMS Case Management module.

Standard Outputs:

Note: The following outputs should be available as reports or provided in a dashboard view to provide for effective management of cases.

- 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)
- Activity follow-up
- Notifications (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)
- Case Status
- Prosecutor charging documents/Application for Criminal Complaint
- Narrative – Rich text in a full-page mode
- Support third-party dictation integration
- An area for Public and Private narratives
- The ability for the system to automatically send the victim notifications of updates on the case and notifications to detectives regarding case assignments or task status for a case

Standard External Data Exchanges:

- Prosecutor (case submission)
- Court (disposition exchanges)
- State, regional, and national information sharing systems and networks [e.g., RISS, Nlets, N-DEx, ARJIS, LInX, TDEx, OHLEG, Suspicious Activity Report (SAR)]
- Jail management system

Standard Internal Data Exchanges:

- Incident Reporting module
- Property and Evidence Management module
- Warrant module
- Hyperlinks to other systems such as video management systems, evidence, and lab management systems

Other Optional External Data Exchanges:

- Financial management system

5.2 ASSIGN INVESTIGATOR

The supervisor must be able to access and review unassigned cases. The supervisor will assign case responsibility to a primary investigator. The RMS should allow for cases to be assigned to a secondary unit/and or investigator for situations where more than one specialized unit is required for the case. 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 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 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 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 RMS should support the creation of a case package that can be forwarded to the Prosecutor. The case package will include the original and supplemental incident report, investigator notes, photos, videos, recorded phone calls, victim and witness statements, confessions, and any other documents or files pertinent to the case. The system should support the development of charging recommendations and their electronic approval prior to 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. The detective may file charges or apply for a warrant without making an arrest. Cases may be sent to the prosecutor for a decision prior to an actual arrest. The system should allow this process to be documented. When a warrant for arrest is issued, the status should be tracked.

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 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.

5.7 NOTIFICATIONS

When evidence, reports, property, or any other item is added to the case, a notification is sent to the investigator when the case is still open. When the case is closed and an item is added, a notification will be sent to the assigned investigator and the current unit supervisor.

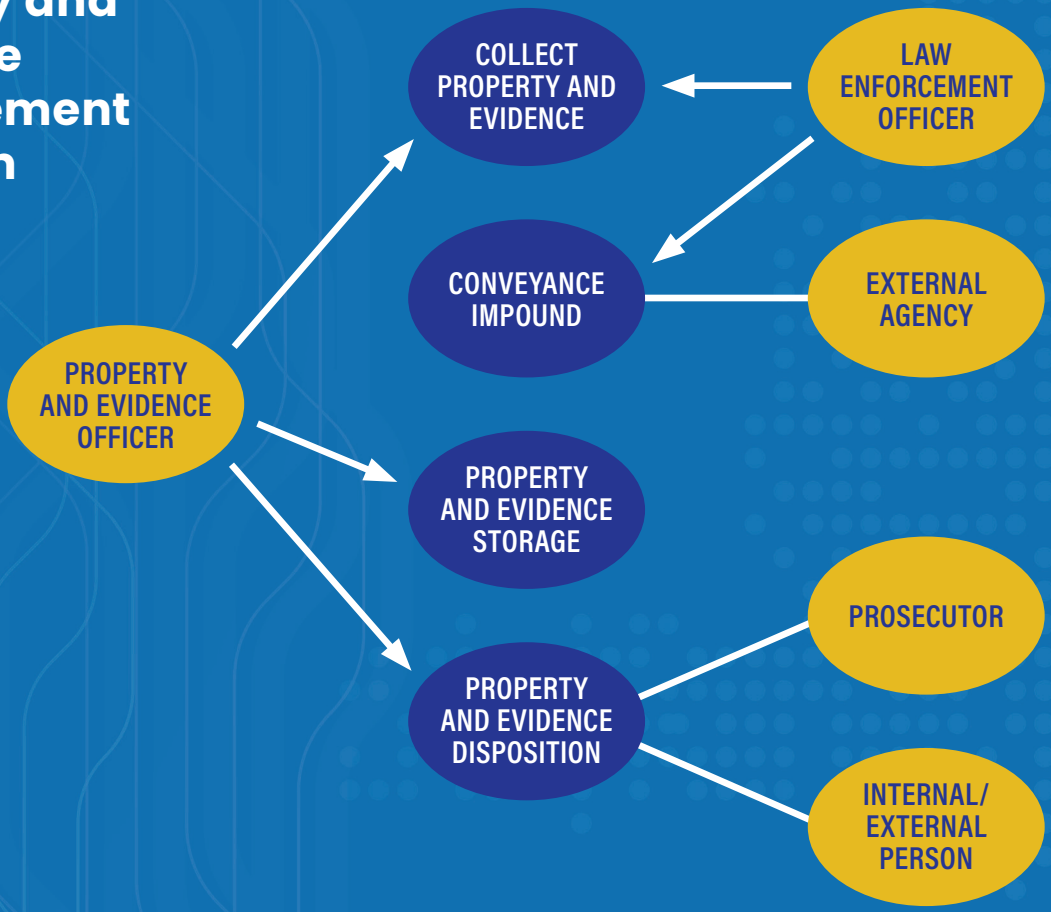
CHAPTER 6 | PROPERTY AND EVIDENCE MANAGEMENT

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. The RMS should provide the ability for the property custodian to configure lockers, shelves, rooms, and other such storage facilities per agency policy. Entry into the Property and Evidence Management Module must be able to be done from the field.

The Property Module should track the complete chain of custody of each property item. Property captured as part of the incident report should seamlessly transfer to the Property Custody module without duplicate entry. Some law enforcement agencies will store property in temporary lockers prior to final check in by the property custodian. This must be recorded as part of the chain of custody process. The location of every property item that is seized, impounded or given to the property room for another purpose should be searchable at all times.

6.1 Property and Evidence Management Diagram



These search results should minimally show the current status or location of the item, item description, date received, and reason for receipt. Personnel also can follow links to related property items tracked in the system. 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. The system should allow the use of digital signatures or other biometrics to record the release or transfer of property.

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:

- Barcode/radio-frequency identification (RFID) system
- Financial Management Systems
- Third-party property management systems, including laboratory evidence processing systems, pawn shops, prosecutor, coroner's office, and courts.

Standard Forms and Reports:

- 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 reports
- ATF gun trace form
- Other commonly used forms

Standard External Data Exchanges:

- State, regional, and federal information sharing systems and networks (e.g., RISS, NIets, ARJIS, LInX, TDEx, OHLEG, N-DEx, ISE) based on state and national standards such as NIEM and NCIC
- Prosecutor
- Courts
- Crime lab
- Coroner's office

Standard Internal Data Exchanges:

- Incident Reporting module
- Fleet Management module

6.2 COLLECT PROPERTY AND EVIDENCE

Property and evidence items are collected and processed into a physical location with established process and security controls. Many agencies require a User ID and PIN to ensure secure property check-in and checkout. 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. Property and evidence items are typically labeled with a barcode to facilitate check-in, checkout, and movement of the item to ensure accurate chain of custody. A single item or multiple items (batch) may be moved in one transaction.

6.3 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 is also 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 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. Barcodes 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 PROPERTY AUDIT AND INVENTORY

Property room inventory needs to be audited on a regular basis and when changes are made with the property and evidence officer. The inventory will ensure an accounting of all property and evidence. If a complete inventory of the property and evidence room is not possible, the agency should consider an inventory of the items required to be maintained in high value areas such as drugs and currency. The system should include the capability of managing audits, including tracking what was audited, who completed the audit, and the date of the audit. Audit capabilities should support full audits of all items in a particular location or audit of a randomly selected group of items. Auditing features should support the ability to confirm the item via barcode scanner. Law enforcement agencies should ensure that property audits conform with local and state mandates. If an agency is accredited or pursuing accreditation through the Commission on Accreditation for Law Enforcement Agencies (CALEA) property audits should conform to these requirements.

6.6 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 to 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 or disposed.

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

6.7 DIGITAL EVIDENCE MANAGEMENT

Digital evidence refers to information and data stored, received, or transmitted by an electronic device. There are many forms of digital evidence including digital images, audio recordings, forensic images, and video. It can be found on a computer hard drive, mobile phone, CD, USB, or DVD, as well as on a flash card in a digital camera or on police camera systems, surveillance videos, and many other devices. Law enforcement agencies can make exact digital copies of the evidence during the investigation of cases and preserve it for use at trial. A hash value is recorded at the time the digital evidence is received to ensure that the digital evidence remains unchanged. It is important to have a reliable digital evidence management system to preserve chain of custody. As a result, proper procedures, processes, and most importantly, technology need to be in place to manage a large amount of data.

Many jurisdictions are using stand-alone software programs to support digital evidence. 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 digital evidence record is uploaded. The RMS should minimally include a tag that allows the agency to easily identify the related digital evidence. Digital evidence collection can be done by officers in the field, investigators, or by citizens uploading or emailing it to the department. It can also be pulled from surveillance and security cameras. Given the large amount of digital data provided to law enforcement today, it is important to have a system that stores, catalogs, secures, and manages the exchange of digital assets.

The RMS should store all digital file types, including video surveillance, interviews, documents, etc. The system should automatically ingest metadata available with each evidence item and allow for manual entry of additional metadata. All access to digital evidence is treated the same as physical evidence. Only authorized personnel should have access and a complete chain of custody should be maintained.

Preservation of digital evidence is essential to a successful case. Forensic specialists must detail the steps taken to capture, examine, analyze, and report the findings. The findings are typically reported as a statement that explains the entire process used to capture, examine, and analyze the evidence. The chain of custody must preserve the digital evidence in the original form from the time it is collected until the digital evidence is provided to the court. The storage servers should be treated as physical property rooms. A complete audit trail should be kept for every case. The RMS should allow for easy sharing of digital evidence with prosecutors and defense attorneys with controlled, secure, and read-only access.

It is critical that the RMS have the ability to link incidents and cases to the digital evidence management system. The metadata captured from the digital evidence management system can be linked to the RMS case or incident. This allows the agency to sort and catalog files with the ultimate goal of providing a mechanism to easily search for required data. Finally, just like any other evidence, the system used should provide the same security, access levels, and auditing capabilities as provided for the RMS property room module.

CHAPTER 7 | 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), location of attempted contact, the date of the activity, and the result of the activity.

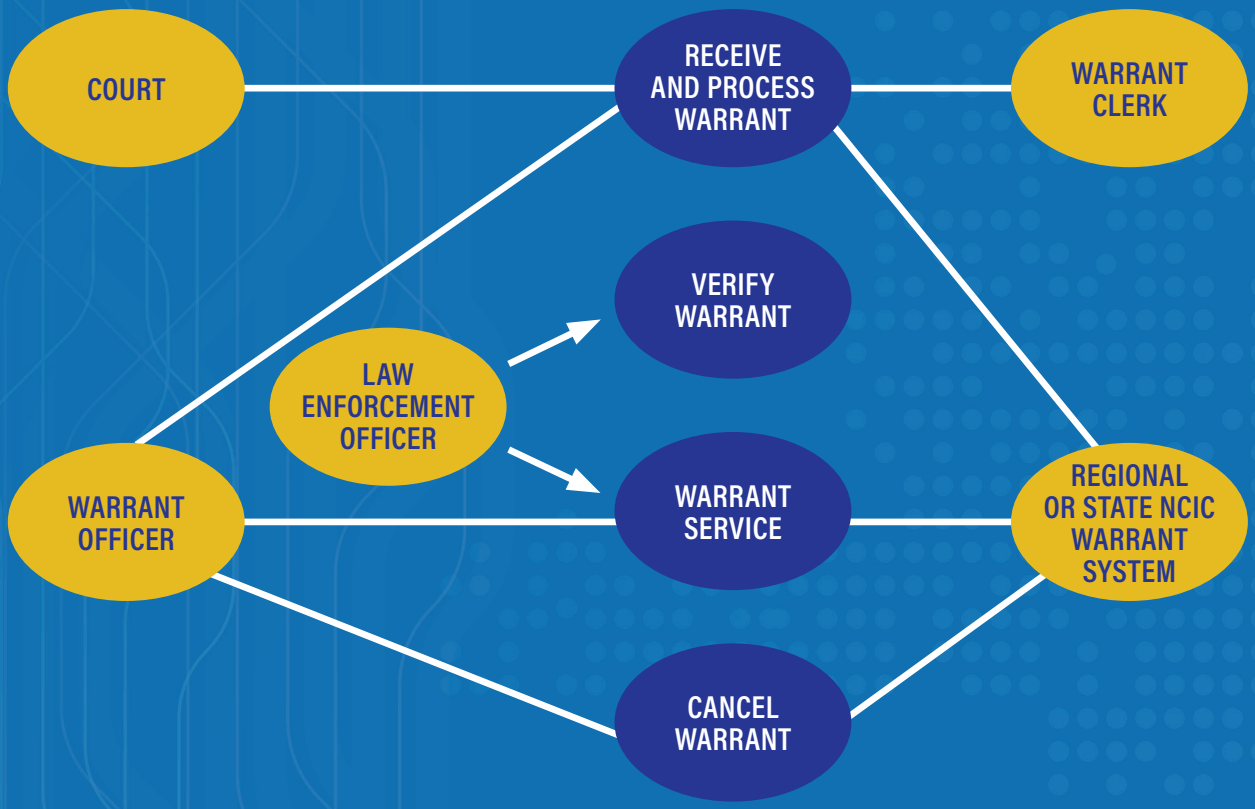
In many departments, other documents (e.g., criminal summons) may be tracked and stored using the same process identified in the Warrant module.

The Warrant module should be able to create a warrant affidavit requesting that the court issue a warrant. This application for warrant is not an arrest until a physical arrest is made. The warrant request must first be approved by the court, and then the individual served and arrested prior to recording the arrest in the RMS.

Standard Outputs:

- Warrants issued

7.1 Warrant Diagram



- 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 and networks (e.g., RISS, Nlets, ARJIS, LInX, TDEx, OHLEG, N-DEx, ISE)
- Jail management system
- Corrections
- Mobile computing systems

Standard Internal Data Exchanges:

- Booking
- Master Name Index
- Master Vehicle Index
- Master Property Index

7.2 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 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. It is critical to verify whether the warrant has been cancelled (dismissed or recalled by the court) or served by another external agency. 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 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), service of the warrant by an external agency, the date of the activity, and the result of the activity. Once the warrant is served, the module is updated and the warrant is cleared in other appropriate warrant systems. Clearing of a warrant occurs when the wanted person is apprehended.

7.5 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.

CHAPTER 8 | 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 must be linked to the original incident or case with a single click and can then be used by the Booking module, the jail management system, the prosecutor, and the court. The incident and arrest modules are often separated but should be tightly integrated to avoid duplicate entry and to ensure that the arrest and corresponding incident are clearly identified and linked.

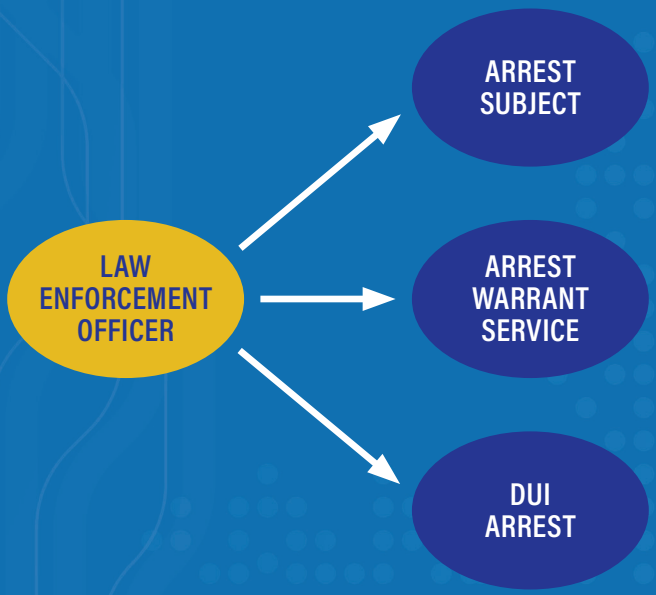
Standard Outputs:

- Daily arrests, by day and time, and date range
- Arrest report and/or affidavit
- Arrests by location
- Arrest log
- Subject's arrest history

Standard External Data Exchanges:

- Jail management system

8.1 Arrest Diagram



- Court
- Prosecutor
- State computerized criminal history system
- State, regional, and federal information sharing systems and networks (e.g., RISS, Nlets, ARJIS, LInX, OHLEG, N-DEx, ISE)
- Mobile computing systems
- LiveScan/AFIS/mugshot

Standard Internal Data Exchanges:

- Incident Reporting module
- Case Management module
- Booking module
- Master Name Index
- Master Vehicle Index
- Master Property Index
- Property and Evidence Management module

8.2 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 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 jail management system is desirable.

8.3 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 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. The terminology used for driving under the influence varies from state to state. Other terms used include Driving While Intoxicated (DWI) and Driving While Impaired (DWI). Similar terms are used for impairment while boating such as Boating While Impaired (BWI).

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.

CHAPTER 9 | JUVENILE CONTACT

The juvenile justice system requires special handling of information about juveniles. Paramount is the handling of their records, which must conform to legal requirements that specifically define privacy protections. Regulations for the handling of juveniles vary from state to state. These rules will need to be implemented based upon the specific state requirements to ensure proper handling of juvenile subjects.

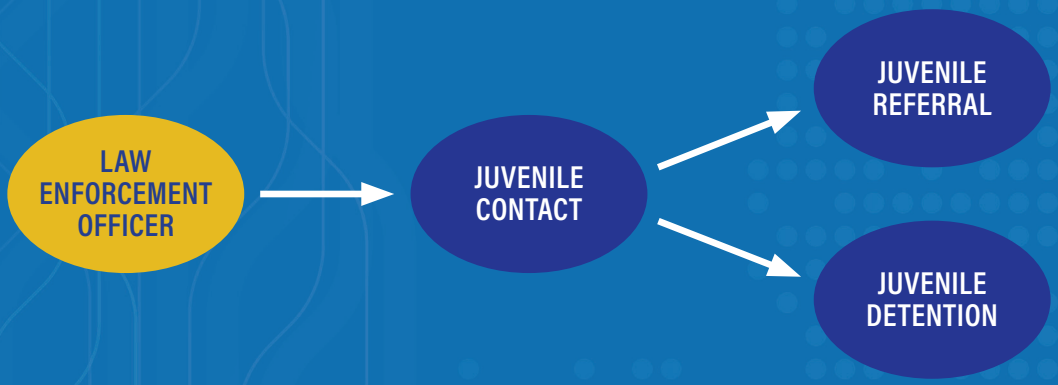
The RMS must accommodate the need to access juvenile data distinctly from adult information.

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 archive and/or restrict 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).

9.1 Juvenile Contact Diagram



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
- Jail management system
- Mobile computing system
- State, regional, and federal information sharing systems and networks (e.g., RISS, Nlets, ARJIS, LInX, OHLEG, N-DEx, ISE)

Standard Internal Data Exchanges:
- Master Name Index
- Master Vehicle Index

Other Optional External Data Exchanges:
- Social service
- Court
- Schools

9.2 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 should have 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, associates, gang affiliation) information, physical description, gender, and name of the school they attend, contact information such as cell phone and email addresses, as well as information about the incident are examples of information that may be entered into an RMS.

9.3 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.

9.4 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 should have a mechanism that allows for timed alert notices if follow-up contact or information is necessary. Juvenile Diversion tracking may be included to track the outcomes and success of diversion programs.

CHAPTER 10 | 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 can also 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 SAR standard to the ISE.

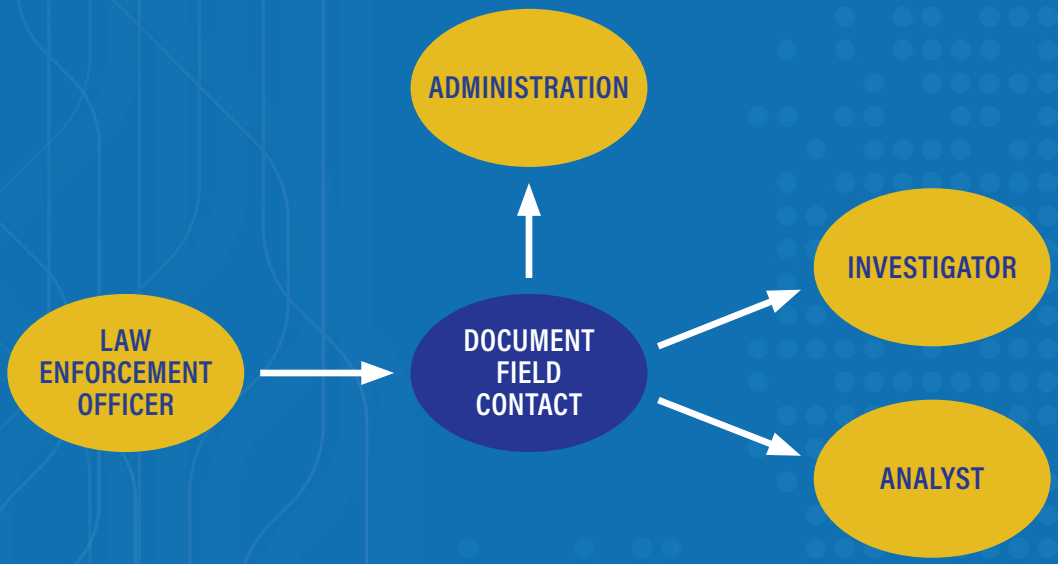
Standard Outputs:

- Field contact summary, based on varying search criteria

Standard External Data Exchanges:

- State, regional, and national information sharing systems (e.g., RISS, ARJIS, LInX, TDEx, OHLEG, N-DEx, ISE)
- Mug shot repository
- Electronic Fingerprinting Device
- Mobile computing system

10.1 Field Contact Diagram



Standard Internal Data Exchanges:

- Master Name Index
- Master Property Index
- Master Vehicle Index
- Arrest module
- Booking module
- Warrant module
- Case Management module

10.2 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.

CHAPTER 11 | EQUIPMENT AND ASSET MANAGEMENT

Law enforcement equipment and assets refers to items that are owned or leased by the department that are necessary for the agency to carry out its mission. The Equipment and Asset Management module tracks all equipment assigned to officers and departments and maintains a record of any maintenance performed on the assets. Given the critical nature of the equipment assigned to law enforcement officers, such as firearms, computers, portable radios, etc., it may ultimately impact officer and public safety if equipment is not tracked and maintained properly.

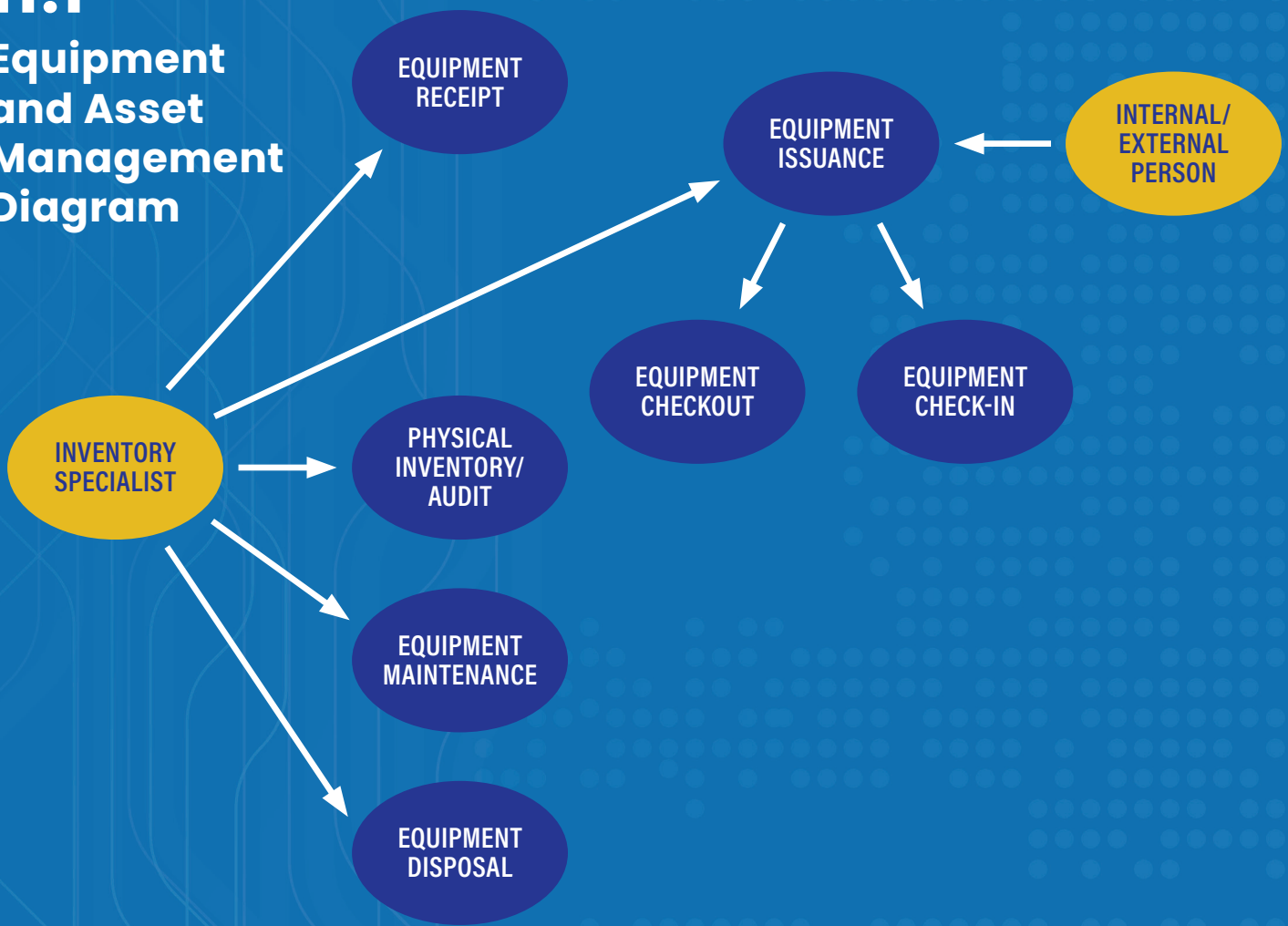
Equipment management describes the processes that the law enforcement agency uses to:

- Record the receipt of equipment
- Record the source of the equipment, including the source of funding used to procure equipment (e.g. grant)
- 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 barcoding 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.

11.1 Equipment and Asset Management Diagram



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, expiration date, unit, and location)
- Physical inventory exception report
- Check-in/checkout log
- Barcode labels
- Receipts
- Equipment history

Standard External Data Exchanges:

- Regulating authority (e.g., general services, facility services)
- Barcoding system
- Inventory control system

Other Optional External Exchanges:

- Financial management system
- Purchasing

11.2 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, funding source used to purchase the equipment, date purchased, and expiration date to assist in replacement schedules.

11.3 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.

11.4 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 barcode or RFID equipment.

11.5 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.

11.6 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.

11.7 EQUIPMENT MAINTENANCE

The system should 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.

11.8 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.

CHAPTER 12 | ANALYTICAL SUPPORT

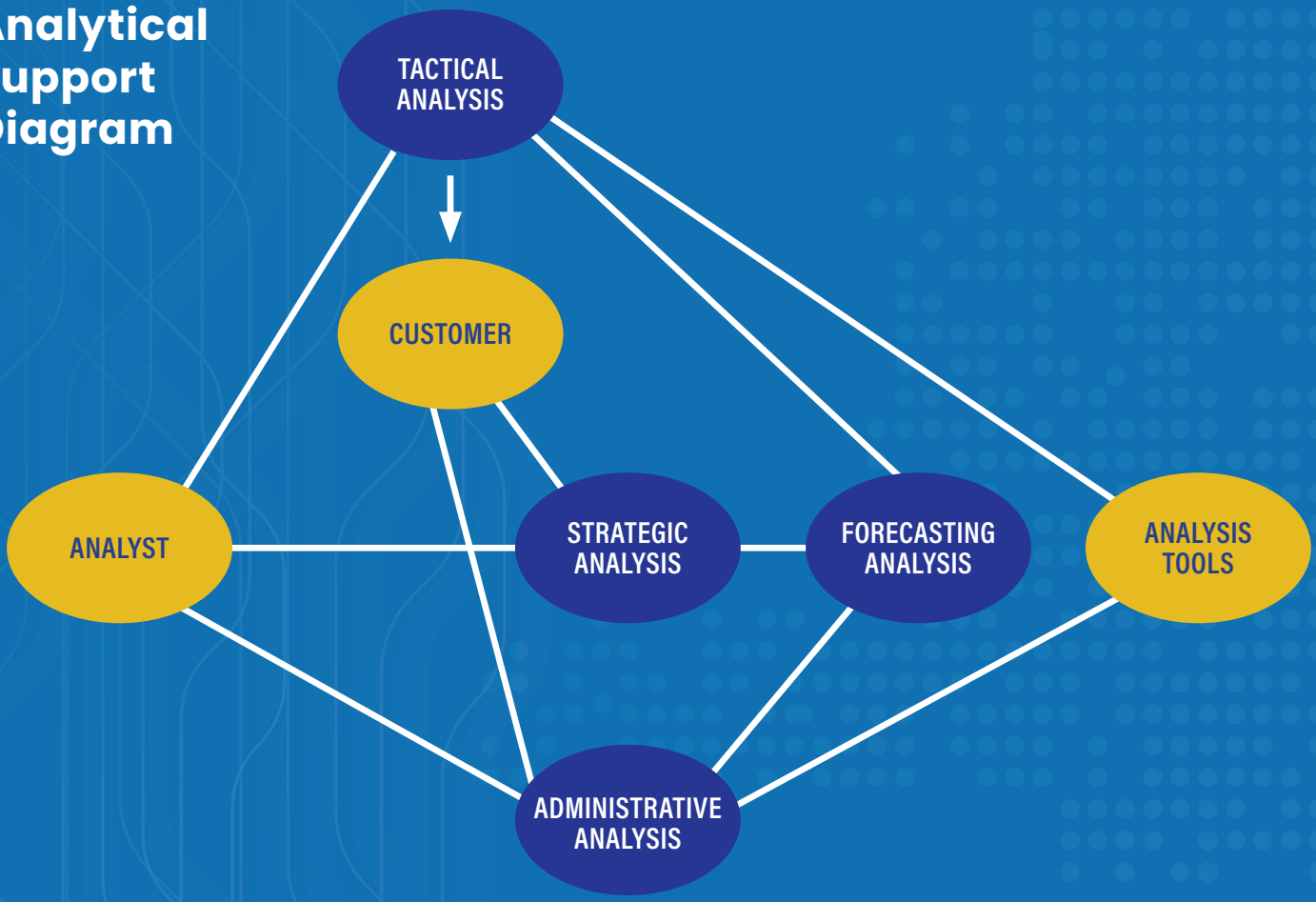
Analytics are critical to understanding the activity within a law enforcement agency. They provide the data necessary to understand the occurrence of crime, determine patrol allocations, prevent crime, and engage in predictive policing. Analytical support is the systematic process of collecting, collating, analyzing, and disseminating timely, accurate, and useful information that describes patterns, trends, problems, and potential suspects in criminal activity. The RMS should either support the tools used by the analyst in this work or provide external interfaces to connect with analytical tools. Analytical tools have matured significantly allowing for agencies to develop Dashboards, which provide real-time crime statistics, early warning systems, CAD calls, and crime maps that depict crime by precinct, district or geocode and exporting RMS data to third-party statistical analysis packages. Crime maps should support layering of other data sets and should be able to gather new maps/layers to get updates from the source data.

Analytical support can be subdivided into four main types:

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

2. 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.

12.1 Analytical Support Diagram



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

4. 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 and crime mapping. 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 crime analyst must be able to create reports that compare data over specified time-periods. The analyst should have the ability to define the time period, whether it is the last 30 days, last six months, last fiscal year, or last five years. The RMS should allow the analyst to choose the time period for analysis in an ad hoc manner.

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 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
- Victim, offender, and arrestee demographics
- Methods of operation
- Property

Standard External Data Exchanges:

- Third-party mapping, analysis, and graphing tools
- State, regional, and national information sharing systems and networks (e.g., RISS, Nlets, ARJIS, LInX, TDEx, OHLEG, N-DEx)

12.2 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.

12.3 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 and gaining and understanding business intelligence. It results in the ability to accomplish the agency mission more effectively and efficiently.

12.4 FORECASTING ANALYSIS

The purpose of forecasting analysis is to preempt crime by analyzing information collected in the RMS and correlating it with external sources. It can involve the application of advanced analytical methods and 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.

12.5 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.

12.6 REPORT OUTPUT

Once the report is completed, the RMS should allow the agency to save the report in various formats including as a Microsoft Word Document, Excel document, PDF file, or in a format that can be easily published to an agency website. The RMS should provide the ability to schedule reports to run at specified intervals. It should also provide the user the ability to email reports to others within and outside the law enforcement agency.

CHAPTER 13 | RMS REPORTS

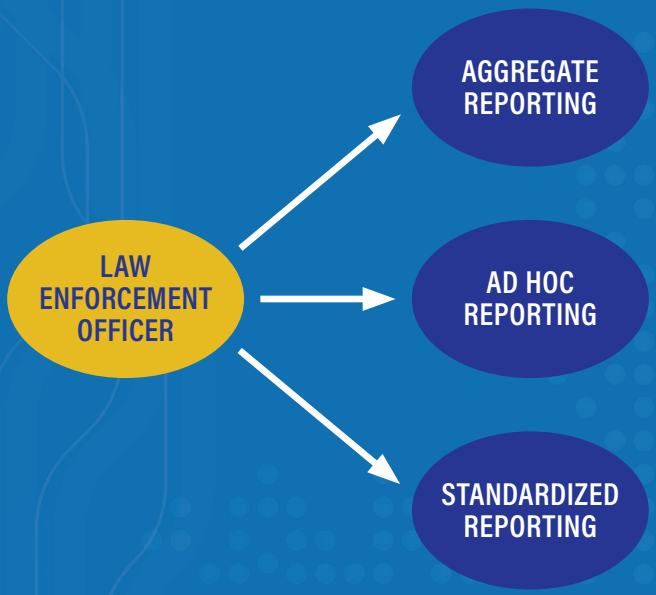
Robust reporting is a core requirement of an RMS. The law enforcement agency enters data into the solution for the purpose of an official recording of events and they must be able to retrieve information easily and in multiple forms. The RMS Reports module documents officer and agency-wide activity or 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. An RMS should provide the ability to create and save report templates. This allows the law enforcement agency to generate customized reports to meet their exact needs.

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

13.1 RMS Reports Diagram



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

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

13.2 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 calls for service, 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, groups of passwords, or by role.

13.3 PRINTED REPORTS

The RMS should provide report printing capabilities in draft form, official approved copies, and public versions. Draft reports should be marked as such. Public report versions must follow local, state, and federal dissemination rules. Law enforcement agencies should have the ability to redact public reports and save a copy of the redacted report.

13.4 STANDARDIZED REPORTING

Each module includes its own set of standardized reports, which also are available through the RMS Reporting module. Agencies should be able to run these standardized reports by date, officer, time of day, weeks or months.

13.5 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.

13.6 DATA QUERIES

Individuals at all levels of the law enforcement agency should have the ability to perform ad hoc data queries based upon permission. These queries should allow the agency to search all data elements in the solution. The RMS should allow the user to cascade searches to refine information of interest. The RMS should also provide the ability to search all narrative fields.

13.7 CLERY ACT

Colleges and Universities are required to report Campus Crime Statistics under the Clery Act. This reporting does not replace reporting of NIBRS statistics to the FBI. The RMS should have the capability to produce reports for the offenses related to dating violence, domestic violence, sexual assault, and stalking along with the data elements required under the Clery Act.

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. Configurable aspects may include roles and security, domain values, use of supplements, approval workflows, and data management and solution access. The RMS should allow an agency the freedom to configure the solution to meet agency requirements with as little service provider intervention as possible.

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.

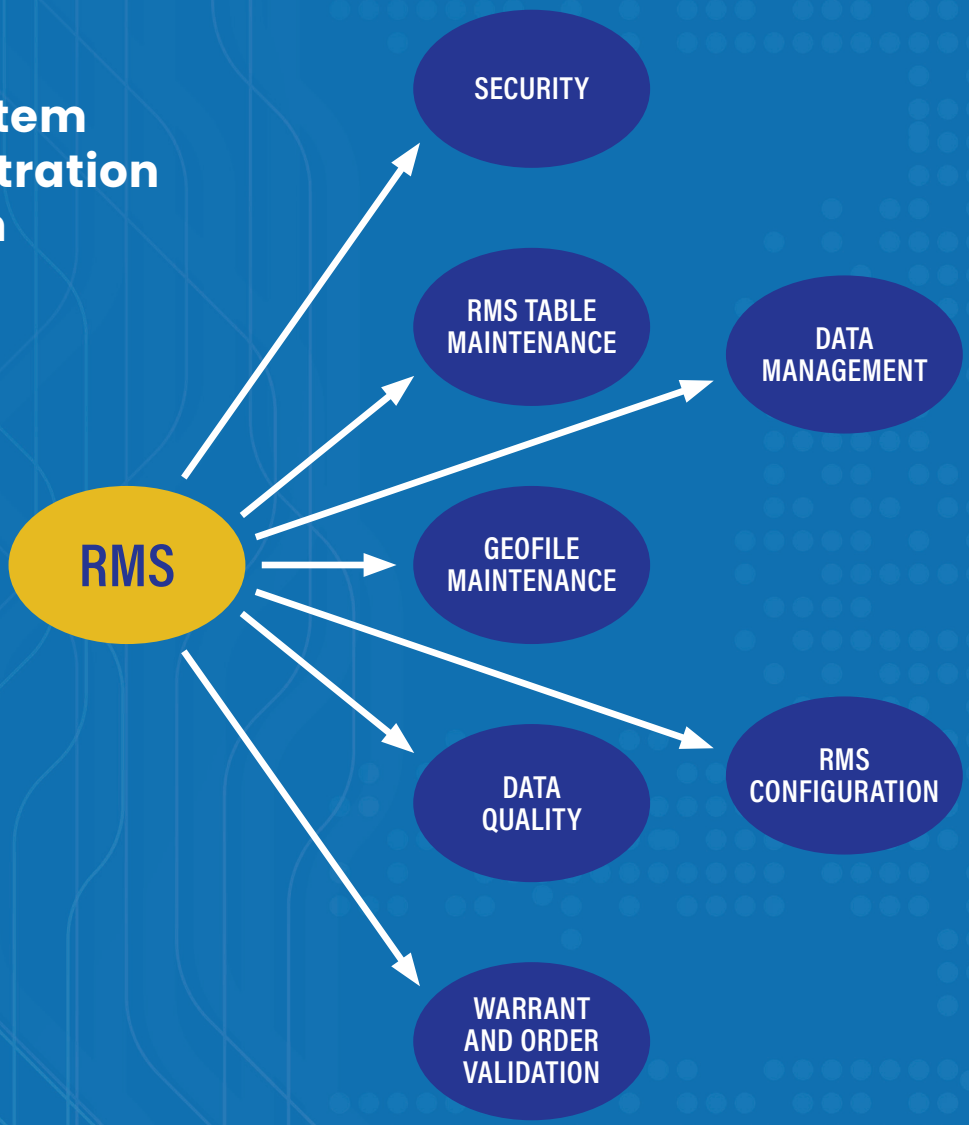
Examples of administrative functions include:

- 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

14.1 RMS System Administration Diagram



- 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 and agency-definable security violations, which generate an external message to a predefined location
- Email system for alerts

Standard Internal Data Exchanges:

- Agency network operating system

14.2 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 currently exist for identification technologies such as identification cards and security tokens. Advanced authentication should follow FBI CJIS Security Policy.

Security groups are often assigned based upon the individual's role in the law enforcement agency. Access to the RMS may be granted via a secure private directory service such as Active Directory. The solution should have the ability to grant access to the individual user level for certain modules such as Case Management and Confidential Informants.

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).

14.3 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 NIEM, NIBRS, and NCIC. The RMS should maintain up to date offense code tables for the agency. These tables should include state and local offenses and provide a mapping to the equivalent NIBRS and NCIC offense codes. Additionally, offense code tables must record applicable repeal dates to ensure that repealed offenses cannot be entered if the incident occurred after the offense was repealed.

14.4 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, 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 relevant database structures to allow the end user to access the database tables through third-party, ad hoc query 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

14.5 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. Geofiles are typically a data file that is accessed from a third-party system for address verification. This system is integrated with the RMS to validate all address entries.

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.

14.6 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.

14.7 SINGLE SIGN-ON

Many organizations use secure external directory services for access to all agency applications. The RMS should have the capability to integrate with such systems so that users sign-on once and have access to all applications that they are required to utilize. These advanced authentication methods allow users to access systems via the agency's Virtual Private Network (VPN). These methods need to be encrypted per security policy and will alleviate the need for users to remember multiple usernames and passwords.

14.8 AUDIT LOGS

Audit logs should be readily available to the agency system administrator. Audit logs should track every action taken in the RMS including log-in and log-off activity and the records accessed by a distinct individual. Any changes to data including additions, deletions, or edits should also be tracked. In addition, the system should track printed reports and, ideally, who prints reports and the reason for printing.

CHAPTER 15 | RMS INTERFACES

As the requirements for law enforcement become more complex, it is critical that the RMS use open standards to facilitate interfacing with multiple systems. Data sharing should be a core component of RMS functionality. Support of open interfaces for importing and exporting data will improve data accuracy, efficiency, and case outcomes.

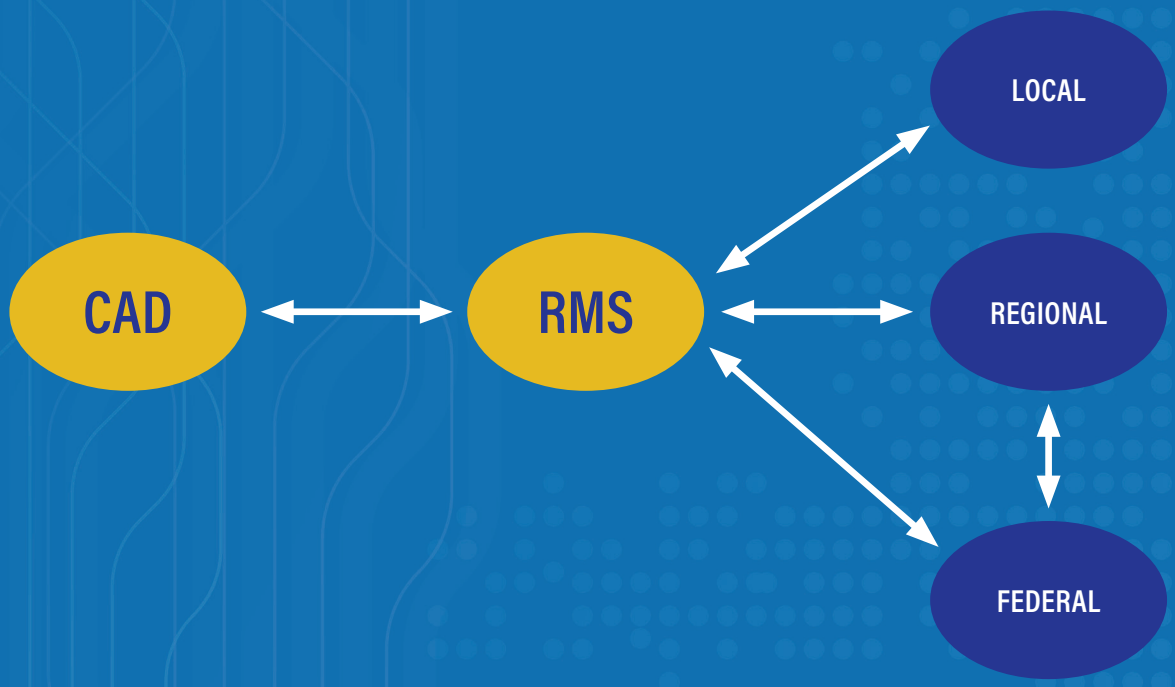
The RMS requires functionality to exchange data with other systems. The exact nature of those exchanges will, in large part, be determined by local business practices and local agency work flows. All interfaces need to comply with national standards. Each business function includes examples of data exchanges. Interfaces should be based upon open standards and be repeatable across multiple agencies. The NIEM should be utilized when possible for the exchange of data between systems. The RMS and agency should refer to the most recent published version of this standard.

Sections 15.3 – 15.4 describe exchanges between local and state or federal Interfaces.

RMS users need to access, and possibly update, a variety of local and regional systems. Examples include court systems, prosecutor systems, financial systems, jail management system, 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 stan-

15.1
RMS Interfaces Diagram



dards, such as NIEM and NCIC.

15.2 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. Caller names, incident locations, phone numbers, and narrative information may be transferred from CAD to the RMS. CAD users require the ability to retrieve information from the RMS based on phone number, name, location, and vehicle descriptors.

Data may also be transferred from the RMS to the CAD solution. Examples may include the transfer of alert data such as gang information, wanted persons, recent arrests at a specific location, and known registered weapons at a location. The CAD should be capable of receiving information from the RMS for addresses of known gang members, wanted persons, as well as notifications regarding recent violent arrests, domestic violence incidents, or mental health-related information to alert first responders dispatched to an address.

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.

The CAD may also interface to multiple systems including gunshot and other locator systems, gang tracking systems, mapping technology, ballistics tracking, automatic portable radio identification, and others.

15.3 LOCAL/REGIONAL INTERFACES

The RMS needs to have the ability to interface with regional and local systems. These may include regional information sharing systems such as LInX, ARJIS, or regional jail management systems (JMSs). Local interfaces might include court, prosecutor, e-citations, towed vehicle, pawn shop, gang tracking, permits and licenses, and laboratory management systems. Where possible, NIEM standards should be used in developing these interfaces. Finally, many organizations are integrating RMS with text, email, and messaging systems to improve organizational efficiency and communication.

As new technologies continue to emerge, additional interfaces will be required. For example, voice-to-text and text-to-voice technologies have rapidly enhanced and may soon be a common technology for law enforcement. The law enforcement agency should weigh the costs and benefits to each interface identified to determine the value proposition for inclusion in the RMS. Evaluation of whether each interface should be a one- or two-way interface is important and where possible open APIs should be utilized.

15.4 STATE/FEDERAL INTERFACES

The RMS needs to interface to state and federal information sharing systems and networks (e.g., TDEx, OHLEG, RISS, N-DEx, Nlets, ISE, and NCIC). These interfaces should be based on national standards, such as NIEM and NCIC where possible. Some interfaces will merely involve development of a web service to pull data from a state system such as the Bureau of Motor Vehicles for driver information. Access to and the ability to copy information to and from the state and NCIC system will improve officer efficiencies and data accuracy.

N-DEx is one example of a federal system that agencies may interface with. N-DEx provides law enforcement agencies with investigative tools to search, link, analyze, and share criminal justice information. N-DEx collects a copy of a law enforcement agency's incident, arrest, and booking data for investigative purposes. N-DEx submissions are based upon the NIEM Standard. The most current versions of these standards should be used at implementation. It should be noted that agencies may send data to N-DEx via a regional or state information sharing system such as LInX, ARJIS, TDEx, or OHLEG.

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. 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.

CHAPTER 16 | BOOKING

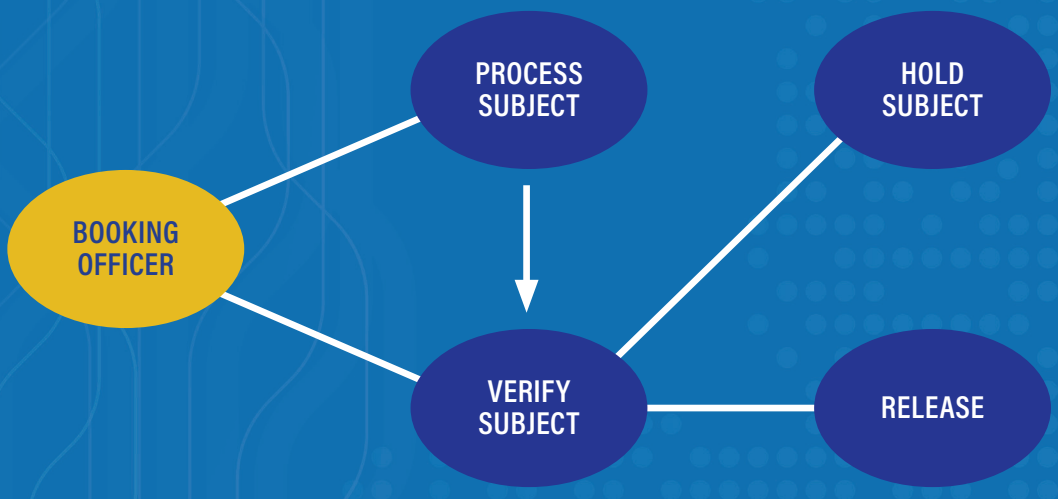
Booking data captured in a law enforcement RMS are ultimately linked to the arrest report. The data to be captured include the personal information of the subject and the official charges for which the subject was arrested. After completion of the booking process an individual may be issued a citation indicating when they should return to court or placed in a holding cell until they are transferred to jail or released at a later time.

The personal identification information provided by the subject will be checked against the Master Name Index 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 such as cell phone number; 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

16.1 Booking Diagram



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

Standard External Data Exchanges:

- Jail management system
- Arrest
- Regional and state warrant and computerized criminal history repositories, following NCIC standards
- State, regional, and federal information sharing systems (e.g., RISS, ARJIS, LInX, TDEx, OHLEG, N-DEx, ISE)
- Automated fingerprint identification system
- Mug shot system
- Victim notification systems

Standard Internal Data Exchanges:

- Master Name Index
- Master Vehicle Index
- Master Property Index
- Property and Evidence Management module
- Arrest module

16.2 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. Physical and mental health needs should be assessed by administering a medical questionnaire that provides a review of the subject's health. Alternatively, health-related notes may need to be attached to the booking record. Examples may include whether the subject was exposed to taser or mace, or any indication of use of force required to apprehend the individual. A medical clearance may be required prior to release or transfer to jail.

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 Master Name Index 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 jail management system.

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.

16.3 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, and biometric identifiers such as iris number where available, 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 Master Name Index plus state, regional, and federal databases for any information. The State Identification Number (SID), Universal Control Number (UCN)[4] and any other information returned from AFIS/IAFIS will be added to the report as they are received.

16.4 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.

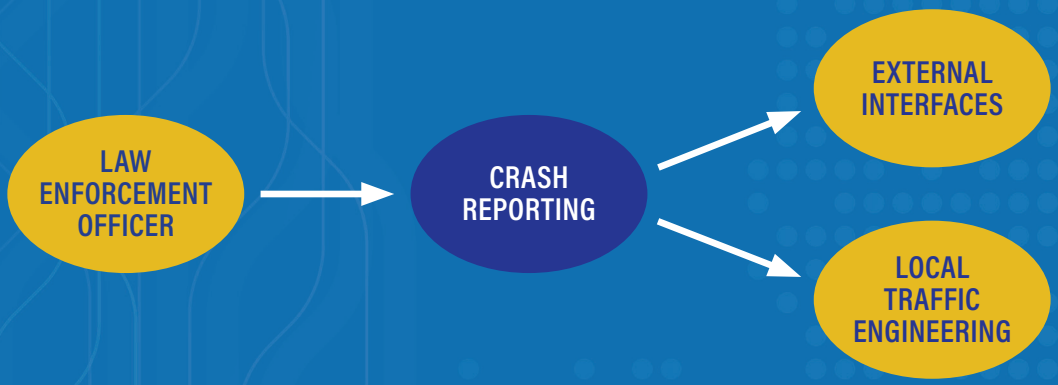
[4] *The Universal Control Number (UCN) was formerly referenced by the FBI as the FBI Number.*

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." Crash reporting is dictated by the Model Minimum Uniform Crash Criteria (MMUCC) reporting standards, however many states alter the standard to meet the specific needs of the state. Each state typically has a standard crash report form that must be used for all traffic crashes.

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. In some instances, the agency may use the state crash reporting system and require an interface to the system or the RMS to store a copy of the report captured in the state system.

17.1
Crash Reporting Diagram



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., RISS, ARJIS, LInX, TDEx, OHLEG, N-DEx, ISE)

Standard Internal Data Exchanges:

- Citation module
- Master Name Index
- Master Vehicle Index
- Master Property Index
- Arrest module
- Booking module
- Property and Evidence Management module
- Fleet Management module

17.2 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. The system should also support driver information exchange sheets that can be printed, texted, or emailed. Crash reports may be subjected to multiple levels of approval wherein the workflow should be automated.

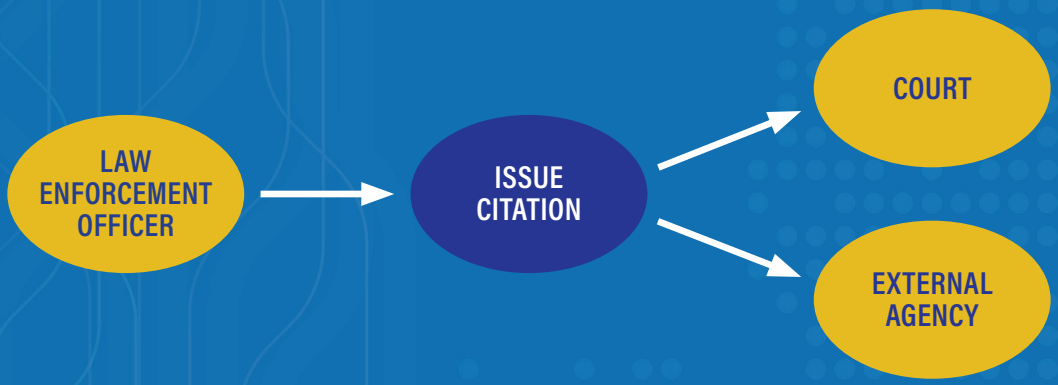
CHAPTER 18 | CITATION

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 for traffic violations and misdemeanor offenses. The user should select whether they are issuing a traffic or offense citation to generate the appropriate form for completion. The traffic citation is often a state standardized form that will vary by state. It is common for law enforcement agencies to utilize third party e-citation systems. In this case, the RMS may need to interface with the solution and integrate with the Master Name and Master Vehicle Index.

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. The citation module should support electronic signatures for both the subject and officer. The officer must have the ability to print and/or email the citation at roadside.

In many jurisdictions, a uniform citation form is used by

18.1 Citation Diagram



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.

Citations may be issued in paper form or printed from the RMS. The RMS should track paper citations utilized by the officer. If the subject is not issued a citation from a citation book, the application must be able to print the citation. If a paper citation is issued, the RMS should support entry of the citation at a later date.

Standard Outputs:
- Printed copy of e-citation
- 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
- Jail management system
- Warrant module
- Prosecutor
- Department of Motor Vehicles (DMV)
- State, regional, and federal information sharing systems (e.g., RISS, ARJIS, LInX, TDEx, OHLEG, N-DEx, ISE)
- Mobile computing system

Standard Internal Data Exchanges:
- Crash Reporting module
- Incident Reporting module (e.g., misdemeanor citations)
- Master Name Index
- Master Vehicle Index
- Master Property Index
- Arrest module
- Booking module
- Juvenile Contact module

18.2 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. Citation types may include traffic citations, local ordinance, or other types of civil citations or warnings.

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.

CHAPTER 19 | PAWN

Pawn modules in RMS help law enforcement representatives identify and recover personal property that has been reported stolen. Collection and reconciliation of pawn information is important whether it occurs within the RMS or through a third-party system that can be interfaced with the RMS. Many jurisdictions require pawn shops to register the items they receive and sell to facilitate this tracking process. The Pawn module should continually cross-reference the agency's Property Room module and other pawn-related systems for missing, found, and stolen property.

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

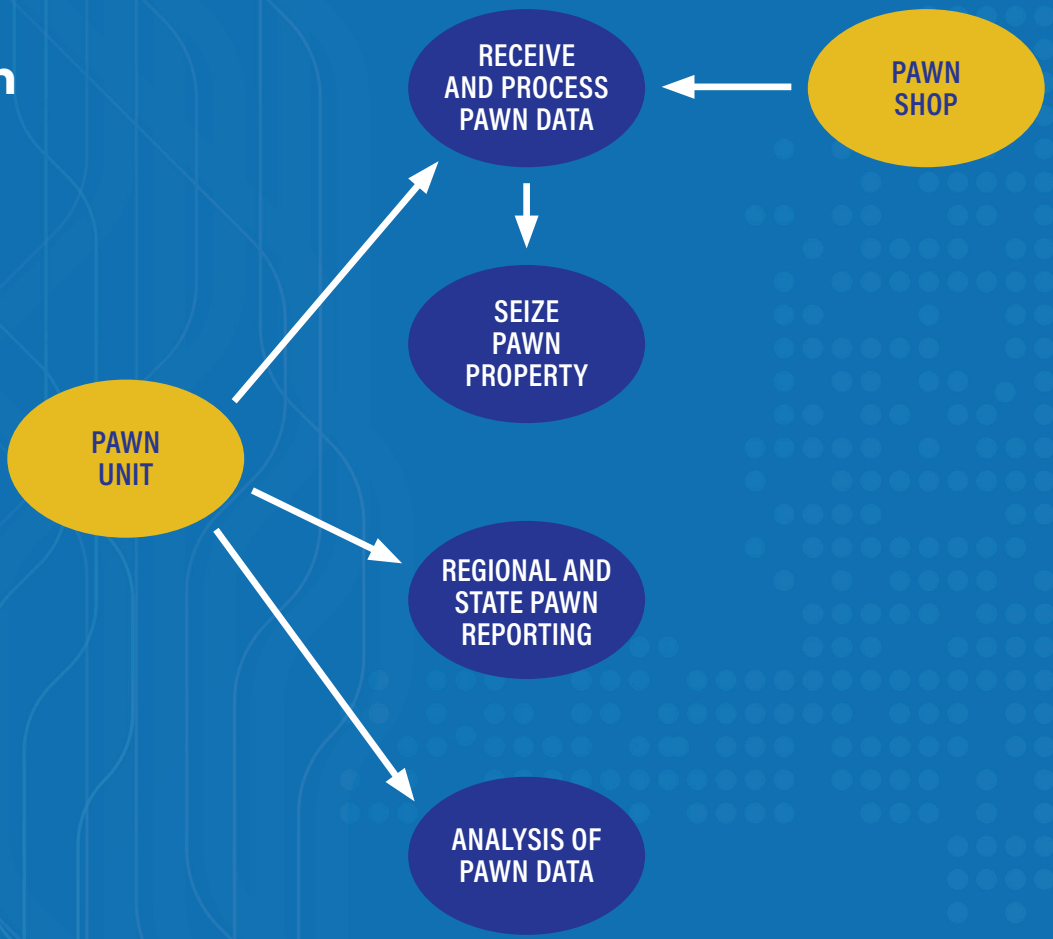
Standard Outputs:

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

Standard External Data Exchange:

- Pawn shops
- eBay
- Craig's List
- ECOATM

19.1 Pawn Diagram



- Frequent pawner list
- State and regional pawn systems following NCIC property standards
- State and national stolen property files
- Local pawn shop computer systems following NCIC property standards
- State and/or regional information sharing systems that allow the sharing of pawn records (e.g., ARJIS, LInX, TDEx, OHLEG)

Standard Internal Data Exchanges:

- Permits and Licenses module
- Master Property Index
- Property and Evidence Management module

19.2 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 or officer assigned this responsibility. This follow-up could include seizing property or further investigation.

19.3 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.

19.4 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.

19.5 REGIONAL AND STATE PAWN REPORTING

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

CHAPTER 20 | CIVIL PROCESS

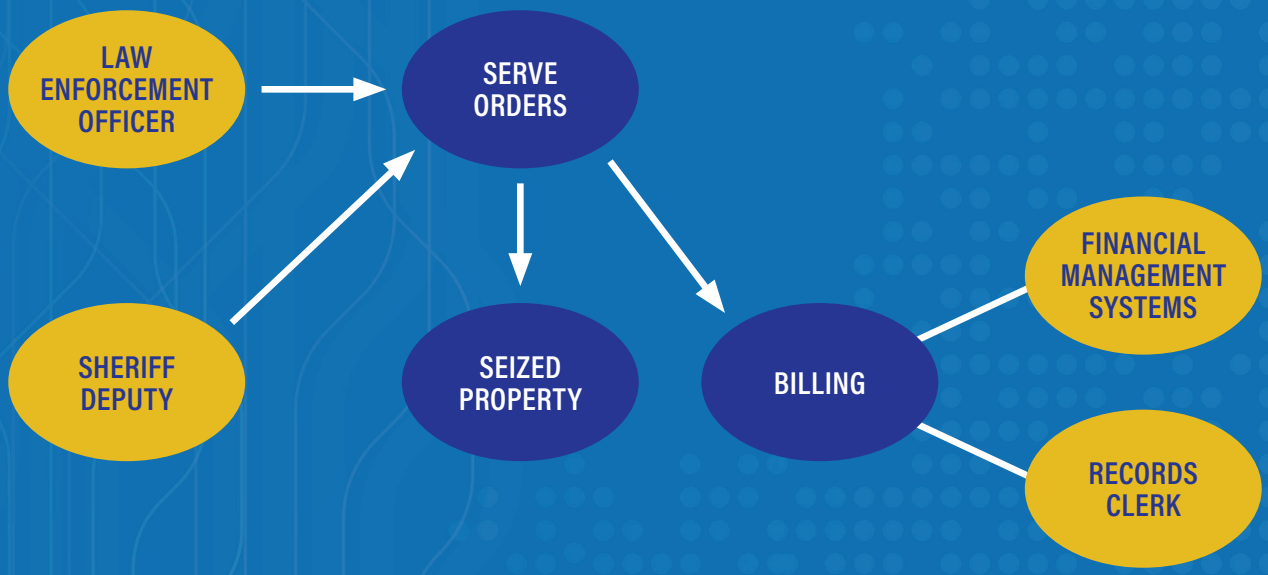
Civil process describes the law enforcement agency responsibility to serve legal papers and execute legal processes as required to facilitate due process through the judicial system. These functions are commonly performed by the county sheriff and may be entitled to compensation by private parties for such service. The 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

20.1 Civil Process Diagram



Standard External Data Exchanges:

- Accounting system
- Court
- Jail management system

Standard Internal Data Exchanges:

- Master Name Index
- Master Vehicle Index
- Master Location Index
- Master Property Index
- Master Organization Index
- Warrant module

20.2 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.

20.3 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.

20.4 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.

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. Many states have a state-level Protection Order Registry. The RMS should interface with this system, if possible.

Many agencies may utilize only the state Protection Order Registry and choose not to capture this information in their RMS.

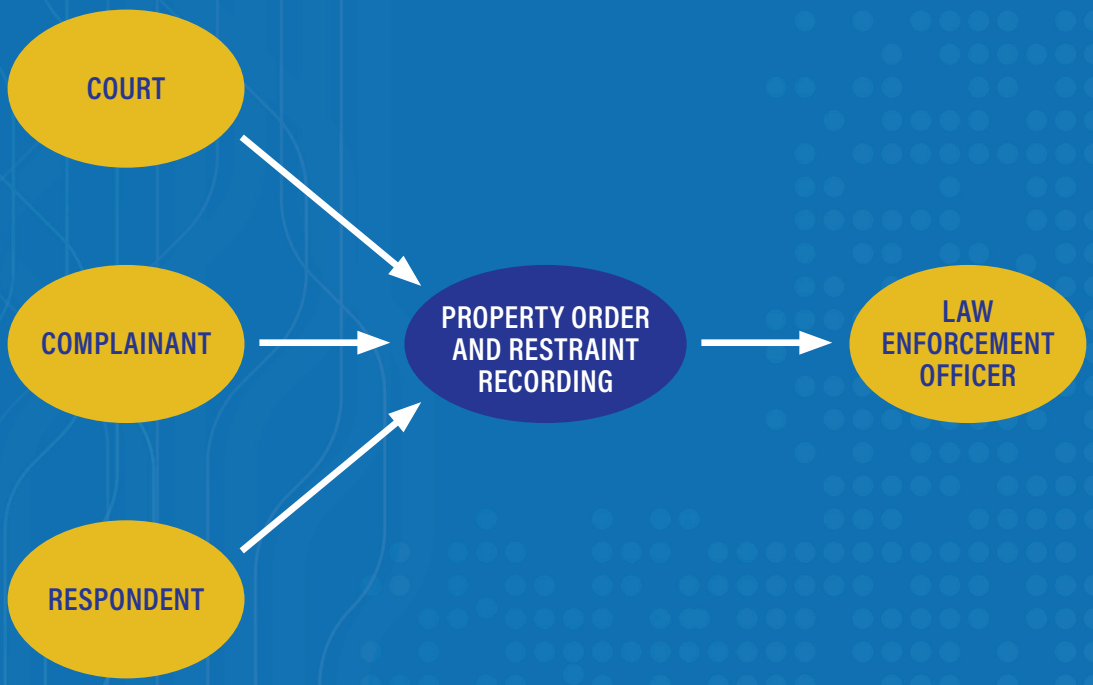
Standard Outputs:

- 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 NCIC Protection Order File

21.1
Protection Orders and Restraints Diagram



- Jail management system

Standard Internal Data Exchanges:

- Master Name Index
- Master Location Index
- Master Vehicle Index
- Master Organization Index
- Master Property Index

21.2 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 2020, 53 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 UCN, 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.

CHAPTER 22 | PERMITS AND LICENSES

The Permits and Licenses module records and tracks the issuance of permits and licenses by the department. Some law enforcement agencies may require the RMS to interface with a stand-alone Permits and Licenses System. 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.

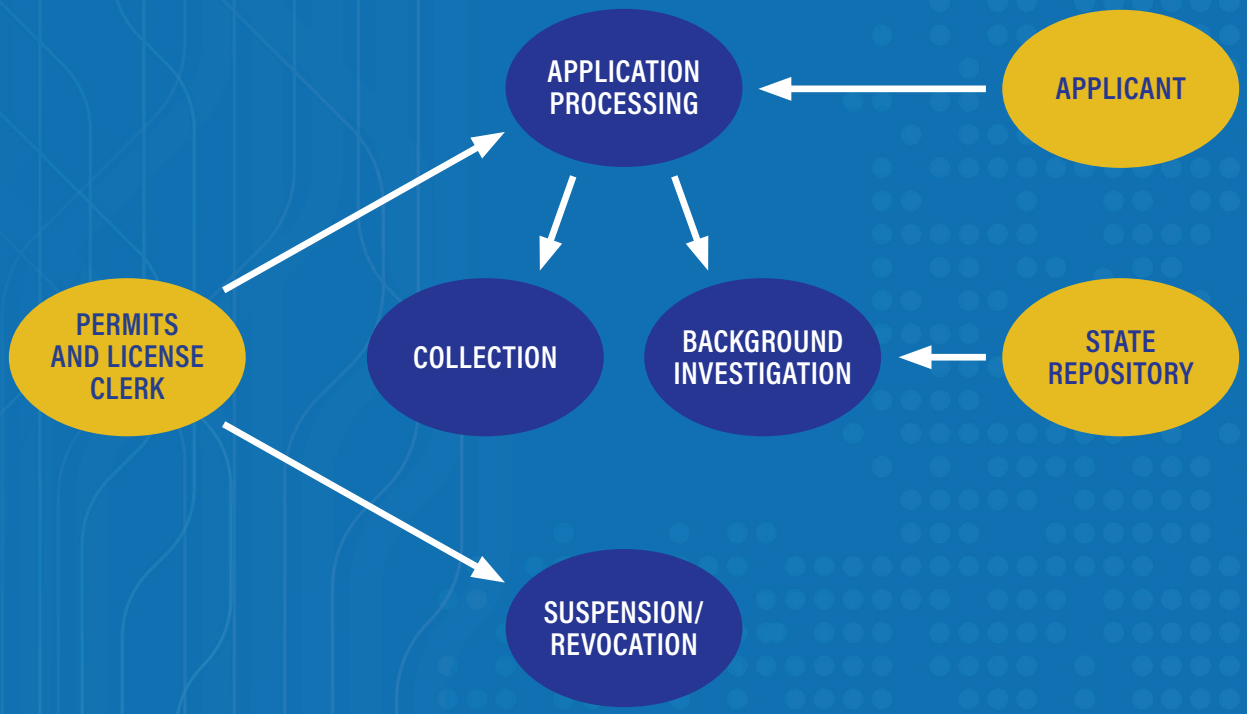
The status of licenses and permits including application, granting, denial, revocation, and expiration is tracked in the RMS. A change of status or an upcoming expiration date generates appropriate alerts and notifications.

As part of the processing, applicant names may be checked against the system Master Name Index. 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

22.1
Permits and Licenses Diagram



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:
- Master Name Index
- Master Organization Index

Other Optional External Data Exchanges:
- Financial management system

22.2 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.

22.3 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.

22.4 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. The law enforcement agency must follow state and federal guidelines for performing a background check for purposes of obtaining a permit.

22.5 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.

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

- Issuance of fleet assets
- Service and maintenance schedules and history
- Crashes involving fleet vehicles
- Vehicle inspections
- 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
- Fleet crash log
- Fluid consumption/cost
- Vehicle repair cost
- Fleet equipment list

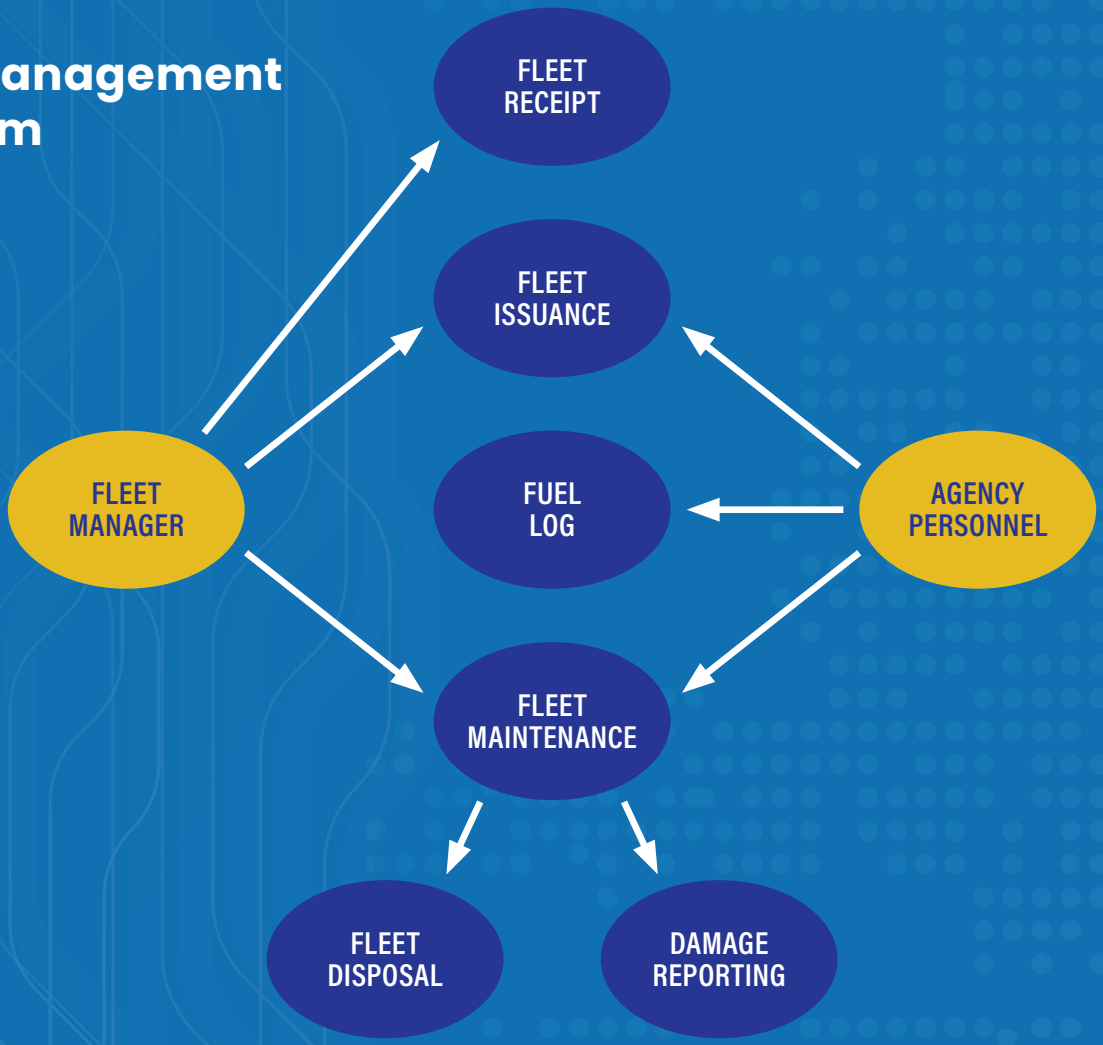
External Data Exchanges:

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

Other Optional External Data Exchanges:

- Real-time vehicle monitoring

23.1 Fleet Management Diagram



- Integrated with the vehicles on board computer to track maintenance, performance, and driving behavior
- External fleet management system managed by city, county, or agency
- City/county financial management systems
- Fuel card system
- Personnel module (for tracking vehicle and related damage/accidents)

23.2 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.

23.3 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.

23.4 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, and person completing fueling. 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.

23.5 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.

23.6 DAMAGE/CRASH REPORTING

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

Crashes involving fleet vehicles should capture the factors of the crash and employee assigned to the vehicle.

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

23.7 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.

CHAPTER 24 | 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 agencies, 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.

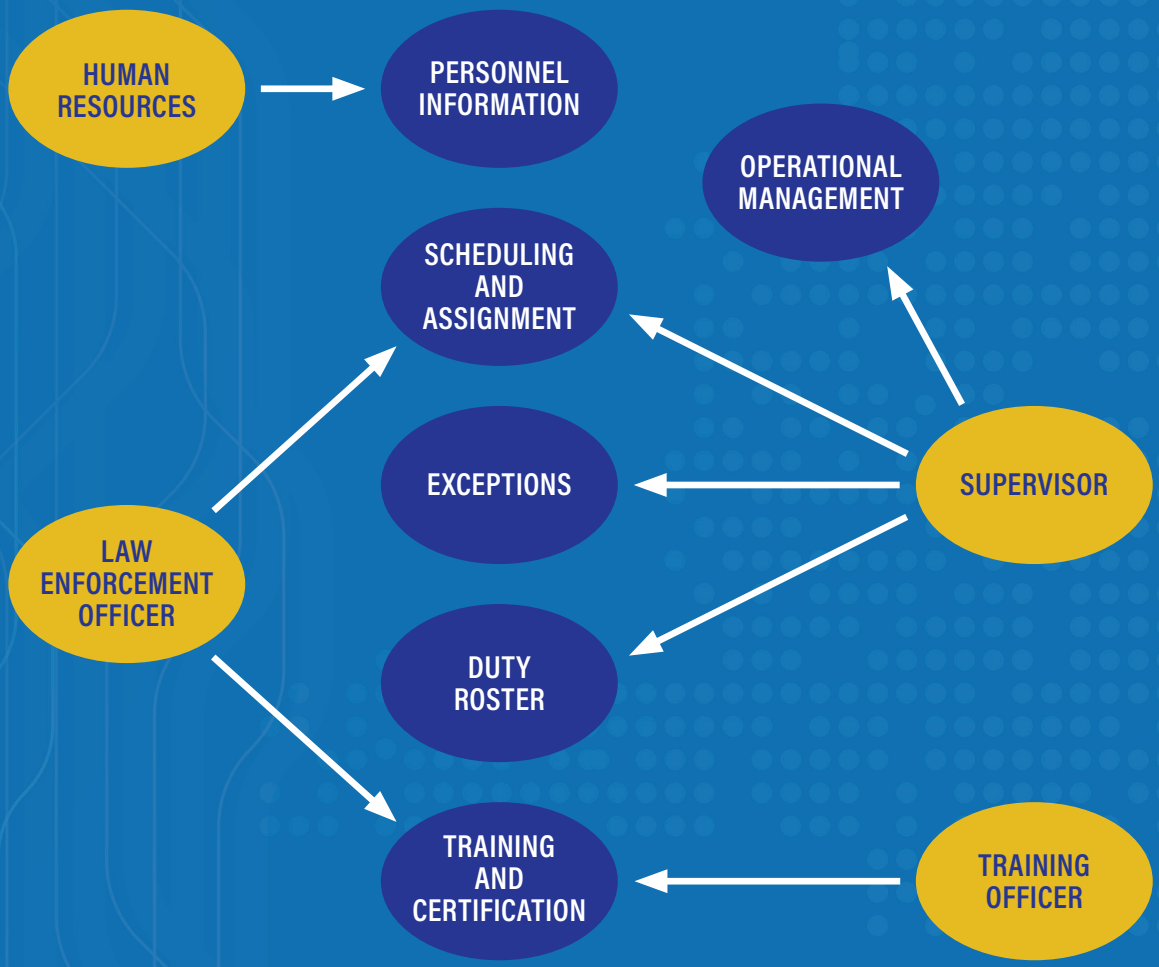
This module addresses those functions that are unique to a law enforcement agency and/or are typically not found in a stand-alone human resources software program.

The regulations under the Health Insurance Portability and Privacy Act (HIPAA) 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

24.1 Personnel Diagram



- 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

24.2 PERFORMANCE EVALUATIONS

The system should include the ability to track performance evaluations of employees. This includes upcoming due dates for the evaluations and the ability to track performance in each of the categories over time. It should include the ability to track the training done to address any deficient categories for the employee and the employee's responses to the evaluations.

24.3 PERSONNEL INFORMATION

The system must allow for the gathering and maintenance of basic information for all personnel working for the department or be updated through an API with a separate human resource system. Information may include names and addresses, physical characteristics, assigned equipment, emergency contact information, special skills, classifications (e.g. sworn/non-sworn), and rank histories.

The system should allow for tracking of background check information. Information should include when the background was completed, what information sources were used for the background check, and renewal dates for rechecking information sources.

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.

24.4 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 is 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.

24.5 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).

24.6 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.

24.7 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. All training records including certificates and qualifications such as Firearms, Driving, Laser, Radar, Taser, Spray, etc. should be tracked. The system should produce a report of any training expirations.

Background checks results may be recorded in the Training Section. Law enforcement agencies should follow state and local requirements for criminal background checks that are used for criminal justice and non-criminal justice personnel hiring purposes.

24.8 OVERTIME AND SECONDARY EMPLOYMENT

The system needs the ability to track overtime and secondary employment assignments. This should include the workflow for approval for the assignment, the address and business name, days and hours to be worked, and the duration of the assignment. There needs to be the ability to set expiration dates and required renewal dates to each assignment. It should be able to send an alert if this assignment conflicts with the employee's regularly scheduled duty times.

24.9 COMMENDATIONS AND AWARDS

The system should be able to include awards, commendations, citizen letters, and recommendations from supervisors for each employee. This should include the dates received and who submitted the information.

24.10 EARLY INTERVENTION PROGRAM

The system should have the ability to identify employees who are experiencing or potentially experiencing performance or personal difficulties and who may need assistance or training. It should enable custom configuration for the factors used to determine which employees may need help. For the indicators stored in an internal affairs module or system, a secure interface may be required.

CHAPTER 25 | INTERNAL AFFAIRS

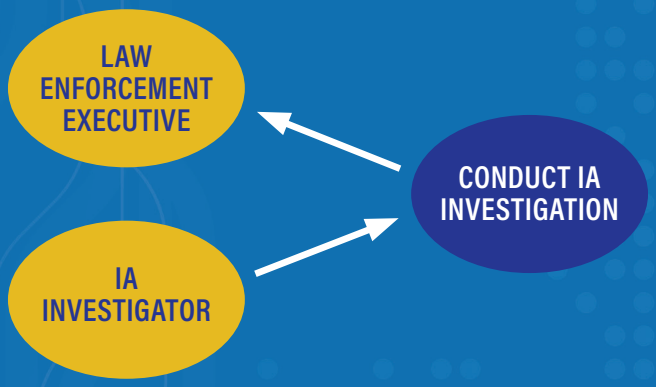
A law enforcement agency's internal affairs (IA) Division investigates department personnel for incidents and possible suspicions of violations of law and professional misconduct.

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. The system should be permission based only giving permissions to those who need access to the information with the proper rights to either read, read and write or read, write and delete. Due to the sensitivity of the information collected in IA functions, the data should be encrypted. It must also include detailed auditing of the users showing both the before value and after value for any changes and tracking view, print, and export actions.

The system should be able to track use of force investigations, administrative investigations, accidents, pursuits, citizen complaints, and civil and criminal actions. It should interface with the RMS to identify potential personnel and organizational issues. The interface should be able to include citations, contact reports, field interviews, and arrest reports for each employee. Management should have the ability to conduct analysis as well as ad hoc reports on these parameters.

The RMS will store all information related to the internal affairs investigation or have the ability to be connected to a third-party Internal Affairs system.

25.1
Internal Affairs Diagram



25.2 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.

25.3 REPORTING

The system should be able to report the following:

- Internal Use of Force Reports
- FBI National Use of Force Reporting System
- Firearm discharges
- Less-lethal incidents
- Monthly and yearly comparisons
- Vehicle pursuits
- Allegation-based discipline
- Allegations
- Demographics
- Disciplinary actions taken
- CALEA reporting

CHAPTER 26 | REGISTRATIONS

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

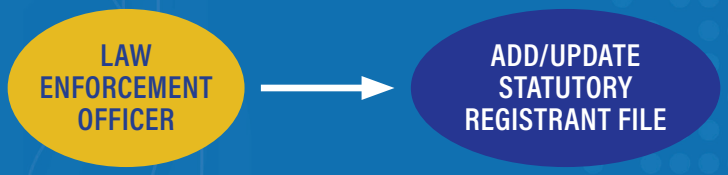
The RMS should provide a mechanism to add and update any type of mandatory registration. Registries should follow state and federal laws that govern the registration requirements, publication and mapping of registration data, personal privacy, and open records policies.

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.

Standard External Data Exchanges:

- State, regional, and federal information sharing systems (e.g., RISS, ARJIS, LInX, TDEx, N-DEx, ISE)

26.1 Registrations Diagram



CHAPTER 27 | CONCLUSION

This functional specifications document provides a general understanding of what should be included in a records management system. It can also be used to support agency policy, RFPs, and training development and delivery. Persons new to law enforcement records management systems will find this an invaluable resource.

Historically, the lifespan of a law enforcement records management system is 10 to 20 years. Given the implementation cycle, including requirements definition, procurement, data migration, and training, it is important to plan carefully. As society demands more of our officers and law enforcement organizations, it is crucial that they have up-to-date technology that promotes efficiency and reduces duplicative effort.

When considering a new RMS, or an upgrade to an RMS, it is critical to understand how local, state, and national policies impact both the requirements definition and procurement process. Also, it is just as critical to consider that crime has no boundaries. While the necessity of information sharing across jurisdictional boundaries has been a topic for the last 20 years, there is still much progress to be made. We cannot achieve this without the implementation of solutions that are based on open standards that promote sharing of information with adjoining agencies and at the state, national, and international levels.

Security and privacy is of the utmost importance. At the same time, the public demands transparency. The information that is entered into the RMS must be available to law enforcement for reporting and analysis. The balance between security, privacy, and transparency can sometimes be difficult to attain, but it is not insurmountable. The RMS must allow for reporting and analysis that gives the agency quick access to data and reporting methodologies.

Readers should consider this publication as a baseline from which agencies can develop software requirements to include in an RFP. Successful procurements typically occur when requirements are detailed, clear, and documented in a manner that is easy to understand. This document is intended to provide an overview of core and optional functions that should be included in a law enforcement RMS to ensure proper recordkeeping, transparency, and efficiency for law enforcement.

Finally, when using this document, consideration should be given to technology advancements. We need to push our solutions to work smarter and more efficient for law enforcement. Much has changed in the last 20 years in the RMS world and it continues to advance. In the future, completion of reports through voice recognition technology, full adoption of RMS apps that can be used on any device, and the ability for law enforcement agencies to build database-driven forms will be the norm. Most importantly, as a community, we must continue to push the envelope on the adoption of open standards to facilitate information sharing. This will accomplish the end goal of understanding, preventing, and reducing crime.

For more information, please contact the IJIS Institute at info@ijis.org

APPENDIXES | LIST OF ACRONYMS

AFIS	Automated Fingerprint Identification System
API	Application Programming Interface
ARJIS	Automated Regional Justice Information System
BJA	Bureau of Justice Assistance
BJS	Bureau of Justice Statistics
BWI	Boating While Intoxicated
CAD	Computer Aided Dispatch system
CALEA	Commission on Accreditation for Law Enforcement Agencies
CFS	Calls for Service
CHRI	Criminal History Record Information
CJIS	Criminal Justice Information System
CSO	CJIS Security Officer
DMV	Department of Motor Vehicles
DNA	Deoxyribonucleic Acid
DOJ	United States Department of Justice
DOT	United States Department of Transportation
DPA	Data Protection Act (UK)
DPPA	Driver's Protection and Privacy Act
DUI	Driving Under the Influence
DWI	Driving While Intoxicated
DWI	Driving While Impaired
EFTS	Electronic Fingerprint Transmission Specification
FBI	Federal Bureau of Investigation
GDPR	General Data Protection Regulation (UK)
GIS	Geographical Information System
HIPAA	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
IBRS	Incident-Based Reporting 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
JSON	JavaScript Object Notation
LEA	Law Enforcement Agency
LEITSC	Law Enforcement Information Technology Standards Council
LEO	Law Enforcement Online, a FBI system
LInX	Law Enforcement Information Exchange, an NCIS System
MLI	Master Location Index
MMUCC	Model Minimum Uniform Crash Criteria
MNI	Master Name Index
MOI	Master Organization Index
MOPI	Management of Police Information (UK)
MPI	Master Property Index
MVI	Master Vehicle Index
N3G	Next Generation NCIC
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
NISP	National Industrial Security Programme (UK)
NIST	National Institute of Standards and Technology
Nlets	International Justice and Public Safety Information Sharing Network

APPENDIXES | LIST OF ACRONYMS

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
OHLEG	Ohio Law Enforcement Gateway
OJP	Office of Justice Programs
ORI	Originating Agency Identifier
PDF	Portable Document Format
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
SRS	Summary Reporting System
TDEx	Texas Data Exchange
UCN	Universal Control Number
UCR	Uniform Crime Reporting
VIN	Vehicle Identification Number
XML	ieXtensible Markup Language

GLOSSARY

CRASH REPORTING: Module within an 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.

AUTOMATED REGIONAL JUSTICE INFORMATION SYSTEM (ARJIS): A joint powers agency sharing justice information throughout San Diego and Imperial Counties and referenced in this document to provide an example of regional information sharing.

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.

GLOSSARY

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.

ECOATM: A kiosk that allows you to deposit cell phones, MP3 players, and tablets to receive funds for the device at the time of deposit.

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 that 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: The 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: The 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: The 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.

GLOSSARY

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 that are spatially referenced to the earth.

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 SHARING: The sharing of law enforcement and justice information has proven to be a critical component of law enforcement investigations and statistical reporting.

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 (10 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: The 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 EXCHANGE PROGRAM (LINX): Consists of 15 regional information sharing programs sponsored by the Naval Criminal Investigative Service and governed by its member law enforcement agencies. Referenced in this document to show examples of regional information sharing.

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

GLOSSARY

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.

NEXT GENERATION NCIC (N3G): A nationwide; computerized information system under development to replace the 50-plus-year-old NCIC system that is a service to all criminal justice agencies—local, state, and federal.

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.

NATIONAL LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM (NLETS): An International Justice and Public Safety Information Sharing Network—a state-of-the-art secure information sharing system for state and local law enforcement agencies.

OHIO LAW ENFORCEMENT GATEWAY (OHLEG): An electronic information network that allows Ohio criminal justice agencies to share criminal justice data efficiently and securely. Referenced in the document as an example of state level interfaces.

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.

GLOSSARY

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 an 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

GLOSSARY

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 an 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.

TDEX: The State of Texas Integrated Justice Information Systems and referenced in this document to show an example of a state interface.

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. NIEM (https://www.niem.gov)

ii. NIST (https://www.nist.gov)

iii. Global Justice Reference Architecture (https://it.ojp.gov/initiatives/gra)

iv. Global Privacy Guidelines (https://it.ojp.gov/privacy)

v. Fusion Center Guidelines (https://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf)

HELPFUL RESOURCES

The following resources have been compiled to aid agencies transitioning to a new RMS and/or industry solution providers tracking updates to standards and requirements at the local, state, federal, and international levels.

United States National Resources:

APCO International:
https://www.apcointl.org
APCO is The Association of Public-Safety Communications Officials (APCO) is an international leader committed to providing complete public safety communications expertise, professional development, technical assistance, advocacy and outreach to benefit our members and the public.

Arrest-Related Deaths (ARD):
https://www.bjs.gov/index.cfm?tid=82&ty=tp.
The ARD program is an annual national census of persons who died either during the process of arrest or while in custody of state or local law enforcement personnel. The ARD program collects data on civilian deaths caused any use of force by state or local law enforcement personnel.

CJIS Security Policy Resource Center:
https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center
The Criminal Justice Information Systems (CJIS) Security Policy contains information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI)

Cloud Fundamentals Whitepaper:
https://cdn.ymaws.com/www.ijis.org/resource/collection/93F7DF36-8973-4B78-A190-0E786D87F74F/IJIS__Cloud_Fundamentals_White_Paper_.pdf.
This paper describes the basics of cloud computing and the role that the cloud can play in public safety. It will also provide a brief introduction on critical security and compliance considerations.

Defense Counterintelligence and Security Agency (DCSA):
https://www.dcsa.mil/mc/ctp/nisp/.
DCSA is the security agency in the federal government dedicated to protecting America's trusted workforce and trusted workspaces—real or virtual.

Drivers Privacy Protection Act:
https://www.govinfo.gov/content/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap123-sec2721.pdf
Prohibition on release and use of certain personal information from State motor vehicle records

Electronic Code of Federal Regulations- CFR 28-Part 20:
https://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title28/28cfr20_main_02.tpl
It is the purpose of these regulations to assure that criminal history record information wherever it appears is collected, stored, and disseminated in a manner to ensure the accuracy, completeness, currency, integrity, and security of such information and to protect individual privacy.

Electronic Code of Federal Regulations- CFR 28-Part 23:
https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=6f7d4bd0341ac10ad72b9375f4afb345&h=L&mc=true&r=PART&n=pt28.1.23
The purpose of this regulation is to assure that all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647), are utilized in conformance with the privacy and constitutional rights of individuals.

Fusion Center Guidelines:
https://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf
Chapter 8 specifically speaks to Privacy and Civil Liberties related to data sharing.

Health Insurance Portability and Privacy Act (HIPAA):
https://www.hhs.gov/ocr/hipaa/
HIPAA applies to those agencies that provide health care. To determine whether your system falls under the purview of HIPAA.

International Association of Crime Analysts (IACA):
https://iaca.net/.
The IACA was formed in 1990 to help crime analysts around the world improve their skills and make valuable contacts, to help law enforcement agencies make the best use of crime analysis, and to advocate for

HELPFUL RESOURCES

standards of performance and technique within the profession itself.

National Incident-Based Reporting System (NIBRS):
https://www.fbi.gov/services/cjis/ucr/nibrs.
NIBRS is an incident-based reporting system used by law enforcement agencies in the United States for collecting and reporting data on crimes.

National Data Exchange (N-DEx) System:
https://www.fbi.gov/services/cjis/ndex.
The N-DEx System provides criminal justice agencies with an online tool for sharing, searching, linking, and analyzing information across jurisdictional boundaries.

National Information Exchange Model (NIEM):
https://www.niem.gov/.
NIEM is a common vocabulary that enables efficient information exchange across diverse public and private organizations. NIEM can save time and money by providing consistent, reusable data terms and definitions, and repeatable processes.

National Use of Force Data Collection:
https://www.fbi.gov/services/cjis/ucr/use-of-force
The FBI created the National Use of Force Data Collection in 2015, in partnership with law enforcement agencies, to provide nationwide statistics on law enforcement use-of-force incidents.

The Nationwide Suspicious Activity Reporting (SAR) Initiative:
https://www.dhs.gov/nsi.
The Nationwide SAR Initiative (NSI) is a joint collaborative effort by the U.S. Department of Homeland Security, the Federal Bureau of Investigation, and state, local, and territorial law enforcement partners. This initiative provides law enforcement with another tool to prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information.

National Crime Information Center (NCIC):
https://www.fbi.gov/services/cjis/ncic.
The National Crime Information Center, or NCIC, has been called the lifeline of law enforcement. It's an electronic clearinghouse of crime data available to virtually every criminal justice agency nationwide. NCIC helps: apprehend fugitives, locate missing people, recover stolen property, identify terrorists, and perform other duties more safely.

NENA The 911 Association:
https://www.nena.org/
NENA is a 9-1-1 Association that improves 9-1-1 through research, standards development, training, education, outreach, and advocacy.

United Kingdom Resources:

Data Protection Act:
https://www.app.college.police.uk/app-content/information-management/data-protection/.

General Data Protection Regulation (GDPR):
https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation.
This guide explains the General Data Protection Regulation (GDPR) to help organizations comply with its requirements.

Management of Police Information (MoPI):
https://www.app.college.police.uk/app-content/information-management/management-of-police-information/.
The principles of management of police information (MoPI) provide a way of balancing proportionality and necessity that are at the heart of effective police information management. They also highlight the issues that need to be considered in order to comply with the law and manage risk associated with police information.